



VÝKLADOVÝ SLOVNÍK KYBERNETICKÉ BEZPEČNOSTI

Petr Jirásek

Luděk Novák

Josef Požár

CYBER SECURITY GLOSSARY

Policejní akademie ČR v Praze
Česká pobočka AFCEA

Praha

2013

Policejní akademie ČR v Praze a Česká pobočka AFCEA



Výkladový slovník kybernetické bezpečnosti

Petr Jirásek, Luděk Novák, Josef Požár

Cyber Security Glossary

*Druhé aktualizované vydání
vydané pod záštitou
Národního centra kybernetické bezpečnosti České republiky a
Národního bezpečnostního úřadu České republiky.*

*The second updated edition
is published under the auspices of
National Cyber Security Centre of the Czech Republic and
National Security Authority of the Czech Republic.*



Na přípravě slovníku rovněž spolupracovali:
členové meziresortní Rady pro kybernetickou bezpečnost,
pracovníci Národního bezpečnostního úřadu,
členové pracovní skupiny AFCEA – Kybernetická bezpečnost,
členové AFCEA,
členové AOBP,
zástupci akademické obce,
zástupci CZ.NIC a CESNET
a další odborníci z oblasti kybernetické bezpečnosti

Tato publikace není určena k prodeji.

Publikace bude distribuována zdarma v tištěné podobě výhradně autory a převážně v elektronické podobě, a to především autory a spolupracujícími organizacemi.

© Jirásek, Novák, Požár, Praha 2013

Žádná část této publikace nesmí být kopírována a rozmnožována za účelem rozšiřování v jakékoli formě či jakýmkoli způsobem bez písemného souhlasu autorů.

Also cooperating in the preparation of the Glossary:

Members of Interdepartmental Council for Cyber Security,

Experts of the National Security Authority,

Experts of AFCEA Working Group – Cyber Security,

AFCEA members,

Members of AOBP,

Representatives of the academia,

Representatives of CZ.NIC and CESNET

and other professionals from the area of cyber security

This publication is not for sale.

The publication will be distributed free of charge in a printed form exclusively by the authors and predominantly in the electronic form by authors and cooperating organizations.

© Jirásek, Novák, Požár, Praha 2013

No part of this publication may be copied or duplicated for distribution in any form or in any way without the written permission of the authors.

Obsah / Summary

Obsah / Summary	5
Úvodní slovo	7
Introduction	9
Česko – anglický slovník / Czech – English Glossary	11
Poznámky:	119
Anglicko – český slovník / English – Czech Glossary	121
Notes:.....	187
Použité zkratky / Abbreviations used	191
Použité zdroje / Sources used	195

Úvodní slovo

Pojmosloví je v každém oboru významným prostředkem k racionálnímu dorozumívání a shodnému chápání sdělovaných obsahů. Vzhledem k tomu, že obory se vzájemně prolínají a doplňují, také speciální odborný jazyk nemá přesné hranice, navíc se mezioborově obohacuje.

Sestavit v dnešní době slovník z oblastí spojených s informační a komunikační technologií (ICT) je úkol značně složitý a současně velmi naléhavý. Nesnadnost spočívá v tom, že se tento obor stále ještě velmi rychle rozvíjí, což se sebou nese terminologickou explozí, doprovázenou zákonitě mnohonásobně duplicitním pojmenováním stejných jevů, a to přímo v dominantním jazyku oboru, angličtině. Nutnost pokusit se kodifikovat vyjadřovací prostředky v tomto oboru pak vyplývá ze skutečnosti, že s ICT pracuje stále větší množství pracovníků i manažerů na různém stupni znalostí a dovedností, kteří nutně potřebují komunikovat pomocí pokud možno jednotné české slovní zásoby.

Proměny současné společnosti, v níž stále významnější úlohu zaujímá věda, moderní technologie, ICT se pochopitelně odrážejí i v rozsahu a terminologii slovní zásoby v oblasti kybernetické bezpečnosti. Významným výsledkem tohoto vlivu se stává ze strany uživatelů jazyka často velice kriticky a vnímavě posuzovaný proces přejímání slov z cizích jazyků, jehož nedlouhou součástí je i vznik nových slovních spojení a utváření nových nebo dříve jen okrajově zaznamenávaných slovních významů. Všechny tyto změny podnecují potřebu moderního člověka slovům cizího původu dobře rozumět a přesně a výstižně je používat.

Výkladový slovník kybernetické bezpečnosti navazuje na výsledky již dlouhodobého zkoumání a zpracování této problematiky. Rozšiřuje a aktualizuje materiál předchozího Výkladového slovníku kybernetické bezpečnosti, který byl vydán za přispění České pobočky AFCEA. Slovník se brzy po svém uvedení na knižní trh i v elektronické verzi stal vyhledávanou příručkou, kterou široká veřejnost přijala s opravdovým zájmem. Tento Překladový slovník vznikl předkladem české terminologie a pojmosloví z kybernetické bezpečnosti do anglického jazyka. Je tedy odlišného pojetí předcházejících verzí. Autoři pojali tuto

filozofii proto, aby i čtenáři, kteří rozumí anglicky, pochopili český význam pojmu, termínu. Jsme si vědomi, že tento proces je v podstatě nekonečný a je tomu tak proto, že terminologie kybernetické bezpečnosti a nadále rozšiřuje a vyvíjí.

Snažili jsme se vytvořit slovník, který by zahrnoval jak základní slovní zásobu oboru, tak perspektivní výrazy. Vybírali jsme z kartotéky obsahující více než 700 výrazů z kybernetické bezpečnosti, kterou hodláme průběžně doplňovat z nejnovějších zahraničních pramenů.

Největší nesnází bylo, že jsme neustále naráželi na slovní spojení a termíny nové i v angličtině, a vyžadující tudíž tvorbu odpovídající české podoby. Návrh českých ekvivalentů jsme prováděli po prostudování různých odborných publikací a po konzultacích s odborníky příslušných oborů. Tam, kde se nám nepodařilo vytvořit vyhovující termín, uvádíme sousloví, které charakterizuje obsah daného pojmu.

Snažili jsme se dát uživatelům dílo z oblasti kybernetické bezpečnosti co nejobsáhlejší a doufáme, že se nám to podařilo, neboť tento slovník je jedním z prvních Česko – anglických slovníků v oboru. Nedostatky slovníku se nejlépe mohou projevit až v praktickém užívání. Protože naší snahou je nedostatky soustavně odstraňovat, uvítáme veškeré připomínky uživatelů a budeme je odpovědně posuzovat.

Tento dvojjazyčný výkladový slovník obsahuje i mnoho výrazů z českého jazyka do angličtiny nepřeložených, jakož i výrazy se kterými lze polemizovat, neboť jsou využívány v okrajových oblastech anebo na ně mohou dvě či více odborných skupin odlišný názor. Autoři předpokládají, že tato verze výkladového slovníku otevře další ještě širší diskusi.

Autoři zároveň děkují všem, kteří se aktivně podíleli na přípravě této verze slovníku, jeho připomínkování, jakož i všem autorům původních termínů, které posloužily jako zdroj informací.

V Praze dne 21. května 2013

Autoři

Introduction

Compilation of a glossary, in particular from the areas related with the information and communication technology (ICT), is a task which is both rather complicated and highly necessary, and more so in our time. The difficulty rests in the fact that the area has been rapidly developing which results in a terminological explosion accompanied as a rule by a multiplicity of names for the same phenomena even in the dominant language of the area, the English language. The necessity for a codification of the means of communication in this area then follows directly from the fact that more and more employees and managers are active here who have different levels of knowledge and skills and share a need to communicate, if possible, in a uniform Czech vocabulary.

Recent transformations in society, with science, modern technology and ICT growing in importance, naturally find their reflection in scope and terminology in the cyber security area. As a result, users of language are highly critical and sensitive about the process of taking over words from foreign languages as well as about the creation of jargon and new word meanings or word meanings formerly only marginally recorded. All these changes stimulate the need of a modern human being to understand foreign words quite well and use these precisely and aptly.

The glossary of computer security connects with the results of research and processing of these issues over a rather long period of time. It expands and updates the material of the previous Glossary of Computer Security, which was published with a contribution of the Czech AFCEA Chapter. This Glossary has become, from the very publication of both the printed version and the electronic version, a sought-after handbook accepted by the general public with real interest. The new bilingual Glossary came into being by translating Czech terminology and lexical meanings into English. In this, it differs from the philosophy of the previous versions. The authors have adopted this philosophy so that even the readers who understand only English may comprehend the Czech meaning. We are aware that this process is practically endless, the reason being that cyber security terminology keeps expanding and developing.

We have tried to compile a glossary which would contain both the basic vocabulary and the vocabulary just at the horizon. We have been selecting from card indexes containing more than 700 expressions of cyber security, and we intend to supplement the indexes continuously from recent foreign sources.

The biggest issue is the fact that we have been encountering vocabulary and terms new even in English and thus have been forced to find the appropriate Czech counterpart. We have made proposals for Czech equivalents after studies of various professional publications and upon consultations with experts from the relevant area. Where we have been unable to find a suitable term, we give an explanation characterizing the idea behind the term.

We have endeavoured to present to our users a piece of work as compendious as possible in the area of cyber security, and we hope it will be a success as this Glossary is one of the first Czech-English glossaries in our line of expertise. The deficiencies are best found out during a practical use. Because we aim at removing the deficiencies rather consistently, we welcome any comments of users and will consider these very seriously.

This encyclopaedic and bilingual Glossary contains also many expressions with no translations from Czech into English, and also some debatable expressions whose use is either marginal or where two or more groups of professionals differ. The authors assume that this version of the bilingual glossary opens an even wider discussion.

The authors at the same time want to thank all those who took an active role in preparing this edition of the Glossary and for their comments, as well as all authors of the original terms which served as a source of information.

Prague, 21 May 2013

Authors

Česko – anglický slovník / Czech – English Glossary

Administrativní / procedurální bezpečnost

Administrativní opatření pro zajištění počítačové bezpečnosti. Tato opatření mohou být operační postupy nebo postupy týkající se odpovědnosti, postupy zkoumání narušení bezpečnosti a revize auditních záznamů.

Administrative measures to ensure computer security. These measures can be operational procedures or procedures related to responsibility, procedures for examining security incidents and revision of audit records.

Administrátor

Osoba odpovědná za správu části systému (např. informačního systému), pro kterou má zpravidla nejvyšší privilegia přístupu (práva supervizora).

Person responsible for the management of a part of a system (e.g. information system) for which he/she usually has the highest access privileges (supervisor rights).

Adresový / adresní prostor

V **ICT** označení pro souvislý rozsah adres. Adresní prostor je tvořen sadou jedinečných identifikátorů (**IP adres**). V prostředí Internetu je správcem jeho adresového rozsahu organizace **IANA**.

ICT denotation for a continuous range of addresses. Address space is made up of a set of unique identifiers (IP addresses). In the Internet environment, IANA organization is the administrator of the address range.

Advertising supported software

Typ softwarové licence, jejíž užívání je zdarma, v programu se objevuje reklama, ze které je financován jeho vývoj.

Type of software licence whose use is free, a commercial appears in the programme, which is used to finance programme development.

Agentura pro elektronickou a informační bezpečnost

Agentura založená Evropskou unií jako kooperativní centrum v oblasti sítové a informační bezpečnosti v roce 2004. Jejím úkolem je tvořit informační platformu pro výměnu informací, znalostí a „best practices“, a tím pomáhat EU, jejím členským státům, soukromému sektoru a veřejnosti při prevenci a řešení bezpečnostních problémů.

Agency founded in 2004 by the European Union as a cooperative centre in the area of network and information security. Its role is to create an information

Administrative / procedural security

Administrator

Address space

Adware

platform for the exchange of information, knowledge and "best practices" and thus help EU, its member states, private sector and the public in the prevention and solutions of security problems.

Agregace

Řízená ztráta či omezení informace nebo prostředků, obvykle slučováním, spojením, či statistickými metodami.

Controlled loss or limitation of information or equipment, usually by aggregation, merge, or statistical methods.

Aktivní hrozba

Jakákoliv hrozba úmyslné změny stavu systému zpracování dat nebo počítačové sítě. Hrozba, která by měla za následek modifikaci zpráv, vložení falešných zpráv, vydávání se někoho jiného nebo odmítnutí služby.

Any threat of an intentional change in the state of a data processing system or computer network. Threat which would result in messages modification, inclusion of false messages, false representation, or service denial.

Aktivum

Cokoliv, co má hodnotu pro jednotlivce, organizaci nebo veřejnou správu.

Anything that has value to an individual, company or public administration.

Aktualizační balík

Souhrn (balík) více aktualizací, který lze instalovat najednou.

Collection (pack) of several updates which could all be installed at the same time.

Algoritmus

Konečná uspořádaná množina úplně definovaných pravidel pro vyřešení nějakého problému.

Finite ordered set of completely defined rules in order to solve some problem.

Analýza hrozeb

Zkoumání činností a událostí, které by mohly negativně ovlivnit kvalitu služby IT (systém zpracování a přenosu dat) i / nebo data samotná.

Analysis of activities and events which could negatively affect IT service quality (system of data processing and transfer) and/or data proper.

Aggregation**Active threat****Asset****Service pack****Algorithm****Threat analysis**

**Analýza komunikace / datových
přenosů****Traffic analysis**

Jednoduché i pokročilé matematické a vizualizační metody sloužící k analýze datového provozu TCP/IP v počítačové sítí. Více *Analysis*.

Simple and advanced mathematical and visual methods for the analysis of data traffic TCP/IP in a computer network. See Analysis.

Analýza počítačového viru**Virus analysis**

Komplexní činnost zahrnující analýzu chování počítačového viru (způsob šíření, skrývání, škody působené virem), analýzu kódu viru, nalezení způsobu vyhledání viru a jeho odstranění ze souborů, resp. nalezení postupu pro nápravu škod virem způsobených. Více též disasemblování, debugger, trasování, emulace kódu.

Complex activity including the analysis of computer virus behaviour (how it spreads, hides, damage caused by the virus), analysis of virus code, finding of the virus and its removal from files, or rectification of damage caused by the virus. More also in disassembly, debugger, tracing, code emulation.

Analýza rizik**Risk analysis**

Proces pochopení povahy rizika a stanovení úrovně rizika.

Process of understanding the nature of risks and establishing a risk level.

Analýza zranitelnosti**Vulnerability analysis**

Systematické zkoumání systému a provozovaných služeb vzhledem k bezpečnostním slabinám a efektivitě bezpečnostních opatření.

Systematic analysis of a system and operating services in view of security weaknesses and the efficiency of security measures.

Anonymní přihlášení**Anonymous login**

Přihlášení do sítě a zpřístupnění jejích zdrojů bez autentizace účastníka.

Login into network and access to its resources without authentication of the party.

Antispamový filtr**Antispam**

Sofistikovaný software, který každý email porovnává s množstvím definovaných pravidel a pokud email pravidlu vyhovuje, započítá váhu pravidla. Váhy mohou mít různou hodnotu, kladnou i zápornou. Pokud součet vah emailu překročí určitou hodnotu, je označen jako spam.

Sophisticated software comparing each email with a number of defined rules and if the email satisfies a rule, counts in the weight of the rule. The weights can

vary in value, positive and negative. When the total of weights exceeds a certain value, it is labelled as spam.

Anti-stealth technika

Schopnost antivirového programu detekovat i stealth viry (sub-stealth viry), které jsou aktivní v paměti, například pomocí přímého čtení dat z disku bez použití služeb operačního systému.

Ability of an antivirus programme to detect even stealth-viruses (sub-stealth-viruses) which are active in memory, for example by using direct disc reading bypassing the operating system.

Antivir

Více *Antivirus Program*.

See Antivirus Program.

Antivirový program

Jednoúčelový nebo vícefunkční program plnící jednu nebo několik následujících funkcí: vyhledávání počítačových virů (jednou nebo několika různými technikami, často s možností jejich výběru nebo nastavení režimu vyhledávání – scanování, heuristická analýza, metoda kontrolních součtů, monitorování podezřelých činností), léčení napadených souborů, zálohování a obnova systémových oblastí na disku, ukládání kontrolních informací o souborech na disku, poskytování informací o virech aj.

Single-purpose or multipurpose programme doing one or more of the following functions: searching for computer viruses (by a single or several different techniques, often with a possibility of their selection or setting mode for search – scanning, heuristic analysis, methods of checksums, monitoring of suspicious activities), healing of infected files, backup and recovery of system sectors on the disc, storing control information on files on disc, providing information on viruses, etc.

Asymetrická kryptografie

Asymetrická kryptografie (nebo také kryptografie s veřejným klíčem) je skupina kryptografických metod, ve kterých se pro šifrování a dešifrování používají odlišné klíče – přesněji pár matematicky svázaných klíčů. Pár klíčů tvoří klíč veřejný a klíč soukromý. Veřejný klíč je klíč šifrovací, majitel klíče ho volně uveřejní, a kdokoli jím může šifrovat jemu určené zprávy; dešifrovací klíč je soukromý, majitel jej drží v tajnosti a pomocí něj může tyto zprávy dešifrovat. Kromě utajení obsahu komunikace se asymetrická kryptografie používá také pro elektronický (digitální) podpis, tzn. možnost u dat prokázat jejich autora.

Anti-stealth technique**Antivirus****Antivirus program****Asymmetric cryptography**

Asymmetric cryptography (also public-key cryptography) is a group of cryptographic methods where different keys are used for encrypting and decrypting – more precisely a pair of mathematically-bound keys. The pair is made up of a public key and a private key. Public key is the encryption key, key owner makes it public, and anyone can encrypt messages for the owner; decryption key is private, the owner holds it in secrecy and uses it to decrypt messages. In addition to making the content of communication secret, asymmetric communication is used also for the electronic (digital) signature that is the possibility to verify the author of data.

Attack surface

Kód v počítačovém systému, který může být spuštěn neautorizovanými uživateli.

Code within a computer system that can be run by unauthorized users.

Attack surface**Audit**

Systematický proces objektivního získávání a vyhodnocování auditních záznamů, jehož cílem je stanovit, zda činnosti systému jsou v souladu se stanovenou bezpečnostní politikou a provozními procedurami.

Systematic process of unbiased obtaining and evaluation of audit records, whose objective is to determine whether system activities are in accordance with defined security policies and operational procedures.

Audit**Audit počítačové bezpečnosti**

Nezávislé ověření implementace opatření a jejich účinnosti vzhledem k dosažení počítačové bezpečnosti.

Independent verification of measures implementation and their efficiency with the view of attaining computer security.

Computer security audit**Audit počítačového systému**

Zkoumání postupů používaných v systému zpracování dat s cílem zhodnotit jejich účinnost a správnost, a doporučit zlepšení.

Analysis of procedures used in data processing in order to evaluate their efficiency and correctness, and to recommend improvements.

Computer system audit**Auditní záznam**

Chronologický zápis aktivit v systému, které jsou dostatečné pro rekonstrukci, zpětné sledování a vyhodnocení sekvence stavu prostředí a aktivit souvisejících s operacemi a procedurami od jejich počátku ke konečnému výsledku.

Chronological record of those system activities which suffice for restoring, backtracking and evaluation of the sequence of states in the environment as well as activities related to operations and procedures from their inception to the

Audit trail

final result.

Auditovaná událost

Systémem detekovaná akce, která vyvolá spuštění a zápis auditu.

Event detected by the system and resulting in triggering and recording the audit.

Autenticita

Vlastnost, že entita je tím, za co se prohlašuje.

Attribute confirming that the entity is what it claims to be.

Autentizace

Proces ověření identity subjektu.

Process of verification of subject identity.

Autentizace dat

Proces používaný k ověření integrity dat (např. ověření, že přijatá data jsou identická s odeslanými daty, ověření, že program není infikován virem).

Process used to verify data integrity (verification that received and sent data are identical, verification that programme is not infected by a virus, for example).

Autentizace entity / identity

Provedení testů, umožňujících systému zpracování dat rozpoznání a potvrzení entity.

Execution of tests making it possible for a data processing system to recognize and authenticate the entity.

Autentizace klíče

Proces ověření, že veřejný klíč osoby skutečně patří této osobě.

Process of verification that the public key truly belongs to that person.

Autentizace zprávy

Ověření, že zpráva byla odeslána údajným původcem zamýšlenému příjemci a že tato zpráva nebyla při přenosu změněna. Ověření identity zdroje informací – odesílatele zprávy. Častým způsobem se stává využití digitálního podpisu.

Verification that message was sent by the alleged originator to the intended

Audit event**Authenticity****Authentication****Data authentication****Entity / identity Authentication****Key authentication****Message authentication / data origin authentication**

receiver and that this message was not changed in transmission. Verification of the identity of information source-sender of the message. Frequently, digital signature is used.

Autentizační výměna

Mechanismus, jehož cílem je zjistit identitu entity (subjektu) pomocí výměny informací.

Mechanism whose objective is to find out the identity of an entity (subject) by way of information exchange.

Automatické monitorování výskytu bezpečnostního incidentu

Automatické monitorování provozu sítě s detekcí neautorizovaných aktivit a nežádoucích událostí.

Automatic monitoring of network operations with the detection of non-authorized activities and undesirable events.

Autorizace

Udelení práv, které zahrnuje udelení přístupu na základě přístupových práv. Proces udelení práv subjektu pro vykonávání určených aktivit v informačním systému.

Granting rights including granting access on the basis of access rights. Process of rights granting to a subject to perform defined activities in the information system.

Autorizační údaje

Data, která jsou přenášena k ustavení prohlašované identity dané entity, pověření.

Data transferred in order to establish proclaimed identity of a given entity, credentials.

Autorizovaný uživatel

Uživatel, který má určité právo nebo povolení pracovat v Informačním systému a s aplikacemi podle stanovených zásad přístupu.

User having certain right or permission to work in the information system and with the applications in accordance with defined access guidelines.

Bezpečnost

Vlastnost prvku (např. informační systém), který je na určité úrovni chráněn proti ztrátám, nebo také stav ochrany (na určité úrovni) proti ztrátám. Bezpečnost IT zahrnuje ochranu důvěrnosti, integrity a dosažitelnosti při zpracování, úschově, distribuci a prezentaci informací.

Property of an element (e.g. an information system) which is at a certain level

Authentication exchange**Automated security incident measurement (ASIM)**

Automatické monitorování provozu sítě s detekcí neautorizovaných aktivit a nežádoucích událostí.

Automatic monitoring of network operations with the detection of non-authorized activities and undesirable events.

Authorization**Credentials****Accredited user****Security**

protected against losses, or also a state of protection (at a certain level) against losses. IT security covers protection of confidentiality, integrity and availability during processing, storage, distribution and presentation of information.

Bezpečnost dat**Data security**

Počítačová bezpečnost aplikovaná na data. Zahrnuje například řízení přístupů, definování politik a procesů a zajištění integrity dat.

Computer security applied to data. Includes for example control of access, definition of policies and ensuring data integrity.

Bezpečnost informací**Information security**

Zajištění (ochrana) důvěrnosti, integrity a dostupnosti informací.

Security (protection) of confidentiality, integrity and availability of information.

Bezpečnost informací / informačních systémů**Information security (INFOSEC)**

Uplatnění obecných bezpečnostních opatření a postupů sloužících: (1) k ochraně informací před jejich ztrátou nebo kompromitací (ztráta důvěrnosti, integrity, a dalších vlastností jako např. autentičnost, odpovědnost, nepopíratelnost a spolehlivost), případně k jejich zjištění a přijetí nápravných opatření. (2) k zachování dostupnosti informací a schopnosti s nimi pracovat v rozsahu přidělených oprávnění. Opatření INFOSEC zahrnují bezpečnost počítačů, přenosu, emisí a šifrovací bezpečnost a odhalování ohrožení skutečností a systémů a jeho předcházení.

Implementation of general security measures and procedures for: (1) protection of information against loss or compromise (loss of confidentiality, integrity and reliability), or as the case may be for their detection and adoption of remedial actions. (2) Continuation of information accessibility and ability to work with them within the scope of functional rights. Measures INFOSEC cover security of computers, transmission, emissions and encryption security and exposing threats to facts and systems and prevention thereof.

Bezpečnost internetu**Internet security**

Ochrana důvěrnosti, integrity a dostupnosti informací v síti internet.

Protection of confidentiality, integrity and accessibility of information in the Internet network.

Bezpečnost komunikací**Communication security (COMSEC)**

Použití bezpečnostních opatření v komunikacích, které znemožní neoprávněným osobám získat informace, které lze získat z přístupu ke komunikačnímu provozu a z jeho vyhodnocení, nebo které zajistí autentičnost komunikačního provozu.

Počítáčová bezpečnost aplikovaná na datovou komunikaci – přenos dat.

Use of such security measures in communications which prohibit unauthorized persons to obtain information which could be gained from access to communication traffic and its evaluation, or which ensure the authenticity of the communication process. Computer security as applied to data communications – data transfer.

Bezpečnost transportní vrstvy

Transport layer security (TLS)

Kryptografický protokol, který poskytuje komunikační bezpečnost pro Internet. Používá se asymetrické šifrování pro výměnu klíčů, symetrické šifrování pro důvěrnost a kody pro ověřování celistvosti zpráv. Široce se používá několik verzí těchto protokolů v aplikacích jako prohlížení na webu, elektronická pošta, faxování přes internet, instantní zprávy and voice-over-IP (**VoIP**).

A cryptographic protocol that provide communication security over the Internet. They use asymmetric cryptography for authentication of key exchange, symmetric encryption for confidentiality and message authentication codes for message integrity. Several versions of the protocols are in widespread use in applications such as web browsing, electronic mail, Internet faxing, instant messaging and voice-over-IP (VoIP).

Bezpečnostní audit

Security audit

Nezávislá revize a zkoumání záznamu systému zpracování dat a činností pro testování adekvátnosti systémových kontrol, k zjištění shody s přijatou bezpečnostní politikou a operačními postupy, k detekování narušení bezpečnosti a doporučení jakýchkoliv indikovaných změn v řízení, bezpečnostní politice a postupech. Nezávislé testování činnosti informačního systému a záznamů o této činnosti. Cílem je určení, zda kontroly jsou odpovídající, zda existuje shoda s bezpečnostní politikou, doporučení případných změn v systému protiopatření. Je zpravidla prováděn externím, nebo interním auditorem.

Independent revision and analysis of records in the data processing system as well as activities for testing of the suitability of system controls, checking compliance with accepted security policy and operational procedures, detection of security infringements and recommendation for any indicated changes in the control, security policy and procedures. Independent testing of the information system activity and records thereof. The objective is to determine if checks are appropriate, if there is compliance with security policy, recommendation of eventual changes in the system of countermeasures. As rule is, it is done by an external or an internal auditor.

Bezpečnostní autorita**Security authority**

Entita odpovědná za správu bezpečnostní politiky v rámci bezpečnostní domény.

Entity responsible for the administration of security policy within the security domain.

Bezpečnostní cíle**Security aims**

Stav bezpečnosti, který má daný systém nebo produkt dosáhnout.

State of security which the given system or product has to reach.

Bezpečnostní doména**Security domain**

Skupina uživatelů a systémů podléhající společné bezpečnostní politice.

Group of users and systems subject to common security policy.

Bezpečnostní filtr**Security filter**

Důvěryhodný počítačový systém, který prosazuje bezpečnostní politiku u dat procházejících systémem.

Trusted computer system enabling security policy for data passing through the system.

Bezpečnostní hrozba**Information security threat**

Potenciální příčina nežádoucí události, která může mít za následek poškození systému a jeho aktiv, např. zničení, nežádoucí zpřístupnění (kompromitaci), modifikaci dat nebo nedostupnost služeb.

Potential cause of an undesirable event which may result in a damage to system and its assets, e.g. destroying, undesired accessing (compromising), data modification or inaccessibility of services.

Bezpečnostní incident**Security incident**

Porušení nebo bezprostřední hrozba porušení bezpečnostních politik, bezpečnostních zásad nebo standardních bezpečnostních pravidel provozu Informační a komunikační technologie.

Infringement or an imminent threat of infringement, of security policies, security principles or standard security rules of operation for the information and communication technologies.

Bezpečnostní kategorie**Security category**

Seskupení citlivých informací používaných k řízení přístupu k datům.

Grouping of sensitive information used when controlling data access.

Bezpečnostní klasifikace**Security classification**

Určení, jaký specifický stupeň ochrany před přístupem data nebo informace vyžadují, spolu s vyznačením tohoto stupně ochrany.

Determination which level of protection for data or information is required before access, together with noting this level of protection.

Bezpečnostní manažer**Security manager**

Zaměstnanecká role pro výkon odpovědnosti gestora IS za bezpečnost s definováním odpovědností a pravomocí.

Employee role to act as a guarantee for IT security with the definition of responsibility and authority.

Bezpečnostní opatření**Security safeguards**

Ochranná opatření pro zajištění bezpečnostních požadavků kladených na systém. Mohou mít různý charakter (fyzická ochrana zařízení a informace, personální bezpečnost – kontrola pracovníků, organizační opatření – provozní předpisy apod.).

Protective measures to ensure security requirements put on the system. May vary in character (physical protection of equipment and information, personnel security – checking of employees, organizational measures – operational rules, and similar).

Bezpečnostní politika**Security policy**

(1) Na úrovni organizace základní dokument, který vymezuje strukturu bezpečnostního rizika, odpovědnost za ochranu informací v organizaci, úroveň ochrany informací. (2) Na úrovni systému soubor pravidel a praktik, které specifikují nebo regulují, jak systém (nebo organizace) poskytuje bezpečnostní služby, aby chránil citlivé nebo kritické zdroje systému.

(1) At the level of an organization, basic document which defines the structure of security risk, responsibility for information protection within an organization, level of information protection. (2) At the system level, a set of rules and practices specifying or regulating how the system (or organization) provides security services in order to protect sensitive or critical system resources.

Bezpečnostní politika informačního systému**IS security policy**

Celkový záměr vedení a směr řízení bezpečnosti informačního systému se stanovením kritérií pro hodnocení rizik.

General purpose of management and direction in the control of information system security with the definition of criteria to assess risks.

Bezpečnostní politika IT**IT security policy**

Pravidla, směrnice a praktiky, které rozhodují o tom, jak jsou aktiva včetně citlivých informací spravovány, chráněny a distribuovány uvnitř organizace a jejich systémů **ICT**.

Rules, directives and practices deciding how assets including sensitive information are administered, protected and distributed inside the organization and its ICT systems.

Bezpečnostní požadavky**Security requirements**

Požadavky kladené na informační systém, které jsou odvozeny ze zákonů, instrukcí, právních úprav, závazných norem a standardů, vnitřních předpisů organizace; prostředí, ve kterém systém působí a poslání, které plní; nutné pro zajištění důvěrnosti, dostupnosti a integrity informací, která se v systému zpracovává.

Requirements put on the information system which follow from laws, instructions, legal amendments, binding standards, internal regulations of an organization; environment where the system operates and the mission it fulfills; necessary for ensuring confidentiality, availability and integrity of information processed in the system.

Bezpečnostní prověření**Security clearance**

Povolení udělené jednotlivci pro přístup k datům nebo informacím na nebo pod specifickou bezpečnostní úrovni.

Clearance given to an individual for accessing data or information on or below the specified security level.

Bezpečnostní rada státu**National security council**

Stálý pracovní orgán vlády České republiky (ČR) pro koordinaci bezpečnosti ČR a přípravu návrhů opatření k jejímu zajištění.

Permanent working body of the government of the Czech Republic (CZE) for the coordination of security of CZE and preparation of proposals to implement them.

Bezpečnostní rozšíření systému doménových jmen (DNSSEC)**Domain name system security extensions (DNSSEC)**

Sada specifikací, které umožňují zabezpečit informace poskytované **DNS** systémem v IP sítích (např. Internet). DNSSEC používá asymetrické šifrování (jeden klíč pro zašifrování a druhý klíč na dešifrování). Držitel domény, která používá DNSSEC, vygeneruje privátní a veřejný klíč. Svým privátním klíčem pak elektronicky podepíše technické údaje, které o své doméně do **DNS** vkládá. Pomocí veřejného klíče, který je uložen u nadřazené autority jeho domény, je pak možné ověřit pravost tohoto podpisu. DNSSEC dnes používá řada velkých

serverů.

Set of specifications which enable the security of information provided to DNS by a system in IP networks (Internet, for example). DNSSEC uses asymmetric encryption (one key for encryption and the second one for decryption). The owner of the domain which uses DNSSEC generates both the private and the public key. Using its private key it then electronically signs technical data about the domain which are then input into DNS. Using the public key which is stored at an authority superior to the domain, it is possible to verify the authenticity of the signature. A number of large servers use DNSSEC at present.

Bezpečnostní standardy**Security standards**

Soubor doporučení a obecných principů pro vymezení, udržování a zlepšování bezpečnosti informací v organizaci.

Set of recommendations and general principles to define, maintain and improve information security inside an organization.

Bezpečnostní událost**Information security event**

Identifikovaný výskyt stavu systému, služby nebo sítě označující možné prolomení politiky, bezpečnosti informací nebo selhání opatření nebo předem neznámé situace, která může být pro bezpečnost závažná.

Identified occurrence of a state of the system, service or network noting a possible breaking of policy, information security or a failure of measures or of formerly unknown situation which could be important for security.

Bezpečnostní událost**Security event**

Událost, která může způsobit nebo vést k narušení informačních systémů a technologií a pravidel definovaných k jeho ochraně (bezpečnostní politika).

Event which may result in or cause the infringement of information systems and technologies and rules defined for the protection (security policy).

Bezpečnostní úroveň**Security level**

Kombinace hierarchické bezpečnostní klasifikace a bezpečnostní kategorie, reprezentující citlivost objektu nebo bezpečnostní prověření jednotlivce.

Combination of a hierachic security classification and security category, representing sensitivity of an object or security clearance of an individual.

Bezpečnostní zranitelnost**Security vulnerability**

Úmyslná chyba nebo neúmyslný nedostatek či závada v software obecně nebo ve firmware zařízení komunikační infrastruktury, která může být zneužita potenciálním útočníkem pro škodlivou činnost. Tyto zranitelnosti jsou buď známé a publikované, ale výrobcem ještě neošetřené nebo skryté a neobjevené. V případě skrytých zranitelností je důležité, zda je objeví dříve útočník,

výrobce, bezpečnostní analytik, či uživatel. Bezpečnostní zranitelnosti jsou proto potenciálními bezpečnostními hrozbami. Bezpečnostní zranitelnosti lze eliminovat důsledným bezpečnostním záplatováním systémů.

Intentional error or unintended defect or software error in general or in firmware of the communication infrastructure equipment which may be used by a potential attacker for harmful activity. These vulnerabilities are either known or published but yet untreated by the manufacturer, or hidden and undetected. In case of hidden vulnerabilities it is important whether these are detected sooner by the attacker, manufacturer, security analyst or user. Security vulnerabilities are therefore potential security threats. Security vulnerabilities can be eliminated by consequential security patches for the system.

Biometrický**Biometric**

Týkající se použití specifických atributů, které odrážejí jedinečné biofyziológické charakteristiky jako je otisk prstu nebo otisk hlasu k validaci identity osoby.

Related to the use of specific attributes reflecting the unique bio-physiological characteristics as is a fingerprint or voice record to validate personal identity.

BitTorrent**BitTorrent**

Nástroj pro peer-to-peer (**P2P**) distribuci souborů, který rozkládá zátěž datových přenosů mezi všechny klienty, kteří si data stahují.

*Tool for peer-to-peer (**P2P**) distribution of files which spreads out the load of data transfers among all clients downloading data.*

Black hat**Black hat**

Více **Cracker**.

See **Cracker**.

Bod obnovy dat**Recovery point objective (RPO)**

Místo v čase, ke kterému musí být obnovena data po havárii.

Point in time when data must be recovered after a breakdown.

Bot (Robot)**Bot**

V rámci kybernetické kriminality: programy, které ovládnou počítače v síti a používají je k provádění zločinných aktivit – např. distribuované útoky (**DDoS**) a hromadná distribuce nevyžádané komerční pošty. Individuální boty jsou základem velkých skupin robotů známých jako botnety. Počítač zcela nebo částečně ovládaný botem je známý jako "zombie".

*Within the framework of cyber criminality: programmes which take over computers in the network and use them for criminal activities – for example, distributed attacks (**DDoS**) and mass distribution of unsolicited commercial emails. Individual bots are the basis for large groups of robots known as botnets. Computer wholly or partially taken over by a bot is known as "zombie".*

Bot herder / Bot wrangler

(1) Cracker, který ovládá velké množství zkompromitovaných strojů (robotů, botů, zombie). (2) Nejvyšší počítač v hierarchii botnetu ovládající zkompromitované počítače daného botnetu.

(1) Cracker who controls a large number of compromised machines (robots, bots, zombies). (2) The topmost computer in the botnet hierarchy controlling compromised computers of the given botnet.

Botnet (síť botů)

Síť infikovaných počítačů, které ovládá jediný cracker, který tak má přístup k výpočetnímu výkonu mnoha tisíců strojů současně. Umožňuje provádět nezákonné činnosti ve velkém měřítku – zejména útoky **DDoS** a distribuci spamu.

Network of infested computers controlled by a single cracker who thus has the possibility to access the power of many thousands of machines at the same time. It allows for illegal activities on a large scale – in particular, attacks as DDoS and spam distribution.

BSD licence

Třída tolerujících licencí na volný software, která klade minimální omezení na opakování šíření takového softwaru.

A family of permissive free software licenses, imposing minimal restrictions on the redistribution of covered software

BSD licence**Completely automated public Turing test to tell computers from humans (CAPTCHA)**

Turingův test, který se na webu používá ve snaze automaticky odlišit skutečné uživatele od robotů, například při vkládání komentářů, při registraci apod. Test spočívá zpravidla v zobrazení obrázku s deformovaným textem, přičemž úkolem uživatele je zobrazený text opsat do příslušného vstupního políčka. Předpokládá se, že lidský mozek dokáže správně rozeznat i deformovaný text, ale internetový robot při použití technologie OCR ne. Nevýhodou obrázkové CAPTCHA je nepřístupnost pro zrakově postižené uživatele, proto je obvykle doplněna o možnost nechat si písmena z obrázku přečíst.

Turing test used on the web in an effort to automatically differentiate real users from robots, for example when entering comments, at registration, etc. The test

usually consists of an image with a deformed text and the task for the user is to rewrite the pictured text into the entry field. It is assumed that the human brain can properly recognize even corrupted text but an internet robot using OCR technology cannot do. Disadvantage of the image CAPTCHA is its unavailability for users with visual impairment; hence usually there is the option of having the letters from the image read aloud.

Certifikace**Certification**

- (1) V počítačové bezpečnosti postup, pomocí kterého dává třetí strana záruku, že celý systém zpracování dat nebo jeho část splňuje bezpečnostní požadavky.
(2) Proces ověřování způsobilosti komunikačních a informačních systémů k nakládání s utajovanými informacemi, schválení této způsobilosti a vydání certifikátu.

(1) Procedure in the computer security by means of which a third party gives a guarantee that the whole system or its part meets security requirements. (2) Process for verification of the competence of communication and information systems for handling classified information, approval of such competence and issuance of a certificate.

Certifikační autorita (CA)**Certification authority (CA)**

V počítačové bezpečnosti třetí strana, která vydává digitální certifikáty, tak, že svojí autoritou potvrzuje pravdivost údajů, které jsou ve volně dostupné části certifikátu.

In computer security, a third party which issues digital certificates and uses its authority to confirm the authenticity of data which exist in the freely accessible part of the certificate.

Certifikační dokument**Certification document**

Dokument označující, že systém řízení např. systém řízení bezpečnosti informací klientské organizace vyhovuje předepsaným normám a další dokumentaci vyžadované pro certifikovaný systém.

Document stating that any system of control, for example system for the control of information security, meets the required standard, and other documentation needed for a certified system.

Certifikační orgán**Certification body**

Třetí strana, která hodnotí a certifikuje systém řízení např. systém řízení bezpečnosti informací klientské organizace s ohledem na mezinárodní normy a další dokumentaci požadovanou pro certifikovaný systém.

Third party which assesses and certifies a system, for example system for the control of computer security for a client organization, with regard to

international standards and other documentation needed for a certified system.

Certifikát řízení přístupu**Access control certificate**

Bezpečnostní certifikát obsahující informaci o řízení přístupu.

Security certificate containing information on access control.

Cíle opatření**Control objective**

Tvrzení popisující, čeho se má dosáhnout jako výsledku zavedení opatření.

Statement describing what is to be achieved by introducing a measure.

Citlivá data**Sensitive data**

Chráněná data mající pro chod organizace zásadní význam. Jejich vyzrazením, zneužitím, neautorizovanou změnou nebo nedostupností by vznikla organizaci škoda, případně by organizace nemohla rádně plnit svoje poslání.

Protected data having fundamental importance for the operation of an organization. Its leakage, abuse, unauthorized alteration or unavailability would mean damage to the organization, or, as the case may be, the organization would be unable to meet its objectives.

Citlivá informace**Sensitive information**

Informace, která na základě rozhodnutí příslušné autority musí být chráněna, protože její zpřístupnění, modifikace, zničení, nebo ztráta by způsobilo někomu nebo něčemu znatelnou újmu, škodu.

Information which, on the basis of a decision by the relevant authority, must be protected, because access to it, modification, destruction, or loss would cause a substantial damage to someone or something.

Citlivost**Sensitivity**

Míra důležitosti přiřazená informacím vlastníkem těchto informací, označující potřebu jejich ochrany.

Measure of importance assigned to information by the owner of the information, describing the need for protection.

Cloud computing**Cloud computing**

Způsob využití výpočetní techniky, kde jsou škálovatelné a pružné IT funkce zpřístupněné uživatelům jako služba. Výhody cloudů: snadný upgrade softwaru, nenáročné klientské stanice a software, levný přístup k mohutnému výpočetnímu výkonu bez nutnosti investic do HW, garantovaná dostupnost. Nevýhody: k důvěrným datům má přístup i provozovatel cloutu.

Mode of utilization of computing technology whereby scalable and flexible IT functions are accessible to users as a service. The advantage of clouds: easy software upgrade, unsophisticated client stations and software, cheap access to a mighty computing power without hardware investments, guaranteed availability. Disadvantages: confidential data are available also to the cloud provider.

Cookie / HTTP cookie

Data, která může webová aplikace uložit na počítači přistupujícího uživatele. Prohlížeč potom tato data automaticky odesílá aplikaci při každém dalším přístupu. Cookie se dnes nejčastěji používá pro rozpoznání uživatele, který již aplikaci dříve navštívil, nebo pro ukládání uživatelského nastavení webové aplikace. Dnes jsou často diskutovány v souvislosti se sledováním pohybu a zvyklostí uživatelů některými weby.

Data which a web application can store in the computer of a signed-in user. The browser then sends these data automatically to the application at every future access. Cookie is at present mostly used for the recognition of a user who visited the application before, or for storing user setting of the web application. Nowadays, discussions are underway about cookies in connection to watching the movements and habits of users by some webs.

Crack

Neoprávněné narušení zabezpečení ochrany programu nebo systému, jeho integrity nebo systému jeho registrace / aktivace.

Unauthorized infringement of programme or system security protection, its integrity or system of its registration/activation.

Cracker (prolamovač)

Jednotlivec, který se pokouší získat neoprávněný přístup k počítačovému systému. Tito jednotlivci jsou často škodliví a mají prostředky, které mají k dispozici pro prolamování se do systému.

Individual trying to obtain an unauthorized access to a computer system. These individuals are often harmful and possess means for breaking into a system.

Creative commons (CC)

Nezisková organizace se sídlem v Mountain View, Kalifornie, Spojené Státy, která se věnuje rozšiřování rozsahu kreativních děl tak, aby i jiní na nich mohli legálně stavět a sdílet je. Organizace již uvolnila zdarma veřejnosti několik licencí na autorská práva, známých jako Creative commons.

A non-profit organization headquartered in Mountain View, California, United States devoted to expanding the range of creative works available for others to build upon legally and to share. The organization has released several

Cookie / HTTP cookie**Crack****Cracker****Creative commons (CC)**

copyright – licenses known as Creative commons licenses free of charge to the public.

Cross-site scripting (XSS)

Útok na webové aplikace spočívající v nalezení bezpečnostní chyby v aplikaci a jejího využití k vložení vlastního kódu. Vložený kód se obvykle snaží získat osobní informace uživatelů, obsah databáze či obejít bezpečnostní prvky aplikace.

Attack on web applications consisting in an attempt to find a security error in the application and using this for the insertion of own code. The inserted code usually tries to get personal data of users, content of database or to bypass the security elements of an application.

Cyberstalking

Nejrůznější druhy stopování a obtěžování s využitím elektronického média (zejm. prostřednictvím elektronické pošty a sociálních sítí), jejichž cílem je např. vzbudit v oběti pocit strachu. Informace o oběti pachatel získává nejčastěji z webových stránek, fór nebo jiných hromadných komunikačních nástrojů. Často je taková aktivita pouze mezistupněm k trestnému činu, který může zahrnovat výrazné omezování osobních práv oběti nebo zneužití chování oběti k provedení krádeže, podvodu, vydírání apod.

Different kinds of stalking and harassment using electronic media (especially using emails and social networks), the objective being for example to instill a feeling of fear in the victim. The culprit obtains information about the victim most often from web pages, forums, or other mass communication tools. Often such an activity is merely an intermediate step to a criminal act which may include a substantial limitation of human rights of the victim, or misuse the behaviour of the victim to steal, defraud, blackmail, etc.

Časovaná bomba

Logická bomba aktivovaná v předem určený čas.

Logical bomb activated at a predetermined time.

Časový hlídáč

Elektronický časovač, který se používá pro zjištění a obnovu po počítačových chybách. V průběhu normální činnosti počítač pravidelně spouští časovač, aby zabránil uplynutí času do konce jeho činnosti neboli jeho "vyčasování". Jakmile však z důvodů buďto technické nebo programové chyby počítač znova nespustí časovač, časovač se vypne a vydá signál o přerušení. Tento signál o přerušení se používá pro zahájení nápravy nebo náprav. Takové typické nápravy jsou uvedení počítače do bezpečného stavu a obnova normální činnosti systému.

Cross-site scripting (XSS)**Cyberstalking****Time bomb****Watchdog timer**

An electronic timer that is used to detect and recover from computer malfunctions. During normal operation, the computer regularly restarts the watchdog timer to prevent it from elapsing, or "timing out". If, due to a hardware fault or program error, the computer fails to restart the watchdog, the timer will elapse and generate a timeout signal. The timeout signal is used to initiate corrective action or actions. The corrective actions typically include placing the computer system in a safe state and restoring normal system operation.

Červ**Worm**

Autonomní program (podmnožina **Malware**), schopný vytvářet své kopie, které rozesílá do dalších počítačových systémů (sítí), kde vyvíjí další činnost, pro kterou byl naprogramován. Často slouží ke hledání bezpečnostních skulin v systémech nebo v poštovních programech.

*Autonomous programme (subset of **Malware**) capable of creating its copies which it then sends out to other computer systems (networks) where these pursue further activities they have been programmed for. Often it may serve to detect security holes in systems or mail programmes.*

Český kyberprostor**Czech cyberspace**

Kyberprostor pod jurisdikcí České republiky.

Cyberspace under the jurisdiction of the Czech Republic.

Člověk uprostřed**Man in the middle (MITM)**

Typ útoku, kdy útočník zachycuje, čte a modifikuje komunikaci mezi dvěma komunikujícími stranami, aniž by to tyto strany věděly.

Type of attack whereby the attacker intercepts, reads and modifies communication between two communicating parties without their knowledge.

Databáze**Database**

Souhrn dat uspořádaný podle pojmové struktury, v níž jsou popsány vlastnosti těchto dat a vztahy mezi odpovídajícími entitami, slouží pro jednu nebo více aplikačních oblastí.

Set of data arranged by a notional structure which describes properties of these data and relations among corresponding entities, serves one or more application areas.

Dávkové viry**Batch viruses**

Počítačové viry vytvářené pomocí dávkových souborů. Zajímavá možnost pro některé operační systémy (např. UNIX), ale existují i pro MS-DOS. Nejsou příliš rozšířené a jsou spíše raritou.

Computer viruses created using batch files. An interesting possibility for some operating systems (e.g. UNIX), exist however even for MS-DOS. They are not too widespread and are more of a rarity.

Defacement, Zkreslení webových stránek **Defacement**

Průnik do webového serveru protivníka a nahrazení jeho internetových stránek obsahem, který vytvořil útočník. Zkreslení není skrytý, naopak, usiluje o medializaci a jeho psychologická síla spočívá jednak ve vyvolání pocitu ohrožení a nedůvěry ve vlastní informační systémy napadené strany, jednak v prezentaci ideologie či postojů útočníka.

Breaking into the web server of an adversary and replacing its internet pages by the content created by the attacker. Corruption is not hidden, quite the reverse, it aims at medialization and its psychological power rests on the one hand in creating a feeling of threat and mistrust in own information systems of the infected party, on the other hand in presenting the ideology or points of view of the attacker.

Demilitarizovaná zóna (DMZ)

Demilitarized zone (DMZ)

Část síťové infrastruktury organizace, ve které jsou soustředěny služby poskytované někomu z okolí, případně celému internetu. Tyto vnější (veřejné) služby jsou obvykle nejsnazším cílem internetového útoku; úspěšný útočník se ale dostane pouze do DMZ, nikoliv přímo do vnitřní sítě organizace.

Part of the network infrastructure of an organization which concentrates services provided to someone in the neighbourhood, or to the whole internet. These external (public) services are usually the easiest target of an internet attack; a successful attacker however only gets to DMZ, not straight into the internal network of the organization.

Detekce anomálního chování sítě (NBAD)

Network behavior anomalies detection (NBAD)

Řešení pro pomoc při obraně proti útokům zero-day. NBAD je integrální částí analýzy chování sítě, která poskytuje bezpečnost kromě bezpečnosti již posypané tradičními aplikacemi proti hrozbám, jako jsou firewall, antivirový software a software pro zjišťování spyware.

A solution for helping protection against zero-day attacks on the network. NBAD is the continuous monitoring of a network for unusual events or trends. NBAD is an integral part of network behavior analysis, which offers security in addition to that provided by traditional anti-threat applications such as firewalls, antivirus software and spyware-detection software.

Detekce manipulace

Manipulation / modification detection

Postup, který je použit ke zjištění, zda data nebyla modifikována, ať už náhodně

nebo záměrně.

Procedure to ascertain whether data were modified, either by accident or by design.

Dialer

Škodlivý program, který připojuje počítač nebo chytrý telefon uživatele k Internetu komutovanou linkou prostřednictvím velmi drahého poskytovatele připojení (obvykle útočníka).

Harmful programme which connects the computer or smart phone of the user to Internet by a commuted line using a very expensive service provider (usually of the attacker).

Digitální podpis / Elektronický podpis

Data připojená ke zprávě, která příjemci zprávy umožňují ověřit zdroj této zprávy. Často se využívá asymetrické kryptografie (podpis je vytvořen pomocí soukromé části klíče a je ověřován veřejnou částí). Obvykle jde ruku v ruce i s ověřením integrity dat zprávy.

Data attached to a message which allows the receiver to verify the source of the message. Asymmetric cryptography is often used (signature is created by the private part of key and is verified by the public part). Goes usually hand in hand with the verification of data of the message.

Dispečerské řízení a sběr dat (SCADA)

Počítačový systém pro dispečerské řízení a sběr údajů. Mohou to být průmyslové řídicí systémy, nebo počítačové systémy monitorování a řízení procesů. Procesy mohou být průmyslové (např. výroba elektrické energie, výroba a rafinace PHM), infrastrukturní (např. úprava a rozvod pitné vody, odvádění a čištění odpadních vod, ropovody a plynovody, civilní systémy protivzdušné obrany – sirény, a velké komunikační systémy) a zařízení (např. letiště, železniční stanice a uzly).

Computer system for the dispatcher control and data acquisition. It could be industrial control systems, or computer systems for monitoring and process control. The processes could be industrial ones (e.g. electrical energy generation, manufacture and purification of fuel), infrastructural (e.g. treatment and distribution of drinking water, taking away and purification of sewage, oil and gas pipes, civilian systems of antiaircraft defence – sirens, and large communication systems), and facilities (e.g. airports, railway stations and hubs).

Dialer**Digital signature / electronic signature****Supervisory control and data acquisition (SCADA)**

Distribuované odmítnutí služby**Distributed denial of service (DDoS)**

Distribuované odmítnutí služby je technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a k pádu nebo nefunkčnosti a nedostupnosti systému pro ostatní uživatele a to útokem mnoha koordinovaných útočníků.

Distributed denial of service is the technique of attack by many coordinated attackers on the internet services or pages resulting in flooding by requests or breakdown or unfunctionality or unavailability of the system for other users.

Distribuované výpočetní prostředí**Distributed computing environment (DCE)**

Programový systém vyvinutý na počátku devadesátých let konsorcium zahrnujícím Apollo Computer (později část Hewlett-Packard), IBM, Digital Equipment Corporation, a jinými. DCE poskytuje rámec a soubor nástrojů pro vyvíjení aplikací klient/server.

A software system developed in the early 1990s by a consortium that included Apollo Computer (later part of Hewlett-Packard), IBM, Digital Equipment Corporation, and others. The DCE supplies a framework and toolkit for developing client/server applications.

DNS server / Jmenný server**Domain name system server (DNS server)**

Distribuovaný hierarchický jmenný systém používaný v síti Internet. Překládá názvy domén na číselné IP adresy a zpět, obsahuje informace o tom, které stroje poskytují příslušnou službu (např. přijímají elektronickou poštu či zobrazují obsah webových prezentací) atd.

Distributed hierarchical name system used in the Internet network. It translates the names of domains to numerical IP addresses and back, contains information about which machines provide the relevant service (e.g. receive emails or show content of web applications) etc.

Doba obnovy chodu**Recovery time objective (RTO)**

Časové období, během kterého musí být po havárii obnovena minimální úroveň služeb a / nebo produktů a podpůrných systémů, aplikací či funkcí.

Time period during which a minimal level of services and/or products and support systems, applications or functions, must be recovered after a disaster.

Dohoda o úrovni služeb (SLA)**Service level agreement (SLA)**

Dokumentovaná dohoda mezi poskytovatelem služeb a zákazníkem, která určuje služby a jejich parametry.

Documented agreement between the service provider and the customer which defines services and their parameters.

Dokument

Informace v čitelné podobě. Dokument může být v papírové nebo elektronické formě např. specifikace politik, dohoda o úrovni služeb, záznam incidentu nebo schéma uspořádání počítačového sálu. Více také **Záznam**.

Information in a readable form. Document may be in a paper form or an electronic form as for example specification of policies, service level agreement, incident record or diagram of the computer room arrangement. See also Record.

Doména nejvyšší úrovně**Top level domain (TLD)**

Jedná se o internetovou doménu na nejvyšší úrovni stromu internetových domén. V doménovém jméně je doména nejvyšší úrovně uvedena na konci (např. u nic.cz je doménou nejvyššího rádu cz). Domény nejvyššího rádu jsou pevně stanoveny internetovou standardizační organizací **IANA**: a) Národní **TLD** (country-code **TLD**, ccTLD) sdružující domény jednoho státu. Jejich název je dvoupísmenný, až na výjimky odpovídající kódu země podle ISO 3166-1, např. cz pro Českou republiku; b) Generické **TLD** (generic **TLD**, gTLD) společná pro daný typ subjektů (např. aero, biz, com, info, museum, org,...), nespojené s jedním konkrétním státem (až na výjimku **TLD** mil a gov, které jsou z historických důvodů vyhrazeny pro vojenské, resp. vládní počítačové sítě v USA); c) Infrastrukturní **TLD** využívané pro vnitřní mechanismy Internetu. V současné době existuje jediná taková **TLD**: arpa, používaná systémem **DNS**.

*This is the internet domain at the highest level in the tree of internet domains. In the domain name, top level domain is given at the end (e.g. in nic.cz, cz is the top level domain). Top level domains are fixed by the internet standards organization IANA: a) National **TLD** (country-code **TLD**, ccTLD) unites domains in one country. Their name has two letters, with exceptions corresponding to country code per ISO 3166-1, e.g. cz for the Czech Republic; b) Generic **TLD** (generic **TLD**, gTLD) is common for a given type of subjects (e.g. aero, biz, com, info, museum, org,...) not tied to one concrete country (with exceptions **TLD** mil and gov which out of historical reasons are assigned for military and government computer networks in the U.S.A.); c) Infrastructure **TLD** used for the internal mechanisms of the internet. At present there is just one such **TLD**: arpa, used by the DNS system.*

Doménové jméno**Domain name**

Název, který identifikuje počítač, zařízení nebo službu v síti (včetně internetu). Příklad doménového jména: www.afcea.cz.

Name to identify a computer, equipment or service in the network (including the internet). Example of a domain name: www.afcea.cz.

Doménové pirátství

Registrace doménového jména souvisejícího se jménem nebo obchodní známkou jiné společnosti za účelem následného nabízení domény této společnosti za vysokou finanční částku.

Registration of the domain name related to the name or trade mark of another company, with the purpose of subsequent offering the domain to this company at a high financial amount.

Dopad

(1) Nepříznivá změna dosaženého stupně cílů. (2) Následky určitého činu nebo události.

(1) Adverse change in the attained degree of objectives. (2) Consequenses of a certain act or event.

Dost dobré soukromí**Pretty good privacy (PGP)**

Mechanismus/program umožňující šifrování a podepisování dat. Nejtypičtěji se používá pro šifrování obsahu zpráv (e-mailů) a pro vybavení těchto zpráv elektronickým (digitálním) podpisem.

Mechanism/programme enabling encryption and signature of data. Most typically it is used for encrypting the content of messages (emails) and for providing these messages with an electronic signature.

Dostupnost**Availability**

Vlastnost přístupnosti a použitelnosti na žádost autorizované entity.

Property of availability and usability at the request of an authorized entity.

Dotaz**Request**

Žádost o informace, obecně jako formální žádost zaslaná databázi nebo do vyhledávače nebo signál z jednoho počítače do druhého, nebo na server s žádostí o konkrétní informaci nebo údaj.

Request for information, in general as a formal request sent to a database or to a browser, or a signal from one computer to another, or to a server with the request for concrete information or data item.

Důvěrnost**Confidentiality**

Vlastnost, že informace není dostupná nebo není odhalena neautorizovaným jednotlivcům, entitám nebo procesům.

Characteristic that information is not available or is not disclosed to unauthorized individuals, entities or processes.

Důvěryhodný počítačový systém**Trusted computer system**

Systém zpracování dat, který poskytuje dostatečnou počítačovou bezpečnost na to, aby umožnil souběžný přístup k datům uživatelům s odlišnými přístupovými právy a k datům s odlišnou bezpečnostní klasifikací a bezpečnostními kategoriemi.

Data processing system having sufficient computer security to allow for a concurrent access to data to users with different access rights and to data with different security classification and security categories.

Efektivnost, účinnost**Effectiveness**

Rozsah, ve kterém jsou plánované činnosti realizovány a plánované výsledky dosaženy.

Scope in which planned activities are implemented and planned results are achieved.

Elektronická obrana**Electronic defence**

Použití elektromagnetické energie k poskytnutí ochrany a k zajištění užitečného využití elektromagnetického spektra (zahrnuje ochranu sil, prostorů apod.).

Use of electromagnetic energy to provide protection and to secure useful utilization of the electromagnetic spectrum (includes protection of forces, spaces, etc.).

Elektronická pošta**Electronic mail (E-mail)**

Textová, hlasová, zvuková nebo obrazová zpráva poslaná prostřednictvím veřejné sítě elektronických komunikací, která může být uložena v síti nebo v koncovém zařízení uživatele, dokud ji uživatel nevyzvedne.

Text, voice or picture message sent using public network of electronic communications which can be stored in the network or enduser terminal until collected by the user.

Elektronické prostředky**Electronic means**

Zejména síť elektronických komunikací, elektronická komunikační zařízení, koncová zařízení, automatické volací a komunikační systémy, telekomunikační a elektronická pošta.

Primarily a network of electronic communications, electronic communication equipment, terminals, automatic call and communication systems, telecommunication and electronic mail.

Elektronický boj**Electronic warfare**

Vojenská činnost, která využívá elektromagnetické energii na podporu útočných a obranných akcí k dosažení útočné a obranné převahy. Je to vedení boje v prostředí používajícím elektromagnetické záření. Je samostatnou disciplínou,

ale jako jeden z prvků působí na podporu kybernetické obrany v rámci *NNEC*.

Military activity using electromagnetic energy in support of offensive and defensive actions in order to achieve offensive and defensive supremacy. This means engaging in fighting in the environment using electromagnetic radiation. It is a separate discipline but as one of the elements it supports cyber security within NNEC.

Elektronický podpis**Electronic signature**

Více *Digitální podpis*.

See *Digital signature*.

Elektronický útok**Electronic attack**

Použití elektromagnetické energie pro účely útoku. Zahrnuje zbraně se směrovanou energií, vysoce výkonné mikrovlnné a elektromagnetické pulsy a RF zařízení.

Use of electromagnetic energy for the purposes of an attack. Includes weapons with directed energy, high-power microwave and electromagnetic pulses and RF equipment.

Emulace**Emulation**

Použití systému zpracování dat k napodobení jiného systému zpracování dat; napodobující systém přijímá stejná data, provádí stejné programy a vykazuje stejné výsledky jako napodobovaný systém.

Use of a data processing system to emulate another data processing system; emulating system receives the same data, runs the same programmes and exhibits the same results as the emulated system.

Evropská kritická infrastruktura**European critical infrastructure**

Kritická infrastruktura na území České republiky, jejíž narušení by mělo závažný dopad i na další členský stát Evropské unie.

Critical infrastructure in the territory of the Czech Republic whose infringement would result in a serious impact also on another member of the European union.

Extranet**Extranet**

Obdoba intranetu, ovšem zpřístupněná v širším měřítku, než jen pro vnitřní potřeby organizace, stále však ne zcela veřejně – například obchodním partnerům či zahraničním pobočkám.

Analogy of the intranet, available however on a larger scale than for internal needs only but fully public – for example, for business partners or foreign

branches.

Failover

Automatické přepnutí na záložní systém či proces v okamžiku selhání předchozího pro dosažení velmi krátké doby výpadku a zvýšení spolehlivosti.
Automatic switch to a backup system or process at the instant of failure of the previous one in order to achieve a very short time of outage and increase in reliability.

File transfer protocol (FTP)

Internetový standard (RFC 959) pro přenos souborů mezi klientem a serverem.

An Internet standard (RFC 959) for transferring files between a client and a server.

Firewall

Ucelený soubor bezpečnostních opatření, která mají zabránit neoprávněnému elektronickému přístupu k počítači, či konkrétním službám v síti. Také systém zařízení nebo soubor zařízení, který lze nakonfigurovat tak, aby povoloval, zakazoval, šifroval, dešifroval nebo vystupoval v roli prostředníka (proxy) pro všechny počítačové komunikace mezi různými bezpečnostními doménami založený na souboru pravidel a dalších kritérií. Firewall může být realizován jako hardware nebo software, nebo jako kombinace obou.

Comprehensive system of security measures which should prevent unauthorized electronic access to a computer or concrete services in the network. Also, a system of devices or set of devices, which could be configured in such a way as to allow, forbid, encrypt, decrypt or act as a mediator (proxy) for all computer communications among various security domains, based on a set of rules and other criteria. Firewall can be implemented as hardware or software, or a combination of both.

Firmware

Program ovládající **hardware**.

Programme controlling hardware.

FIRST

Celosvětově působící asociace, která spojuje přibližně 200 pracovišť typu **CSIRT / CERT**.

Worldwide organization uniting about 200 workplaces of the CSIRT/CERT type.

Failover**File transfer protocol (FTP)****Firewall****Firmware****Forum for incident response and security teams (FIRST)**

Forensní analýza / vyšetřování**Forensic analysis / investigation**

Vyšetřovací postup nad digitálními daty používaný k získávání důkazů o aktivitách uživatelů (útočníků) v oblasti informačních a komunikačních technologií.

Analysis used on digital data to obtain proofs about the activities of users (attackers) in the area of information and communication technologies.

Freeware**Freeware**

Je proprietární software, který je obvykle distribuován bezplatně (či za symbolickou odměnu). Někdy hovoříme o typu softwarové licence. Podmínky bezplatného používání a šíření jsou definovány v licenční smlouvě. Autor si u freewaru zpravidla ponechává autorská práva.

Proprietary software usually distributed free (or for a symbolic reward). We speak sometimes about a kind of software licence. Conditions for the free use and distribution are defined in the licence agreement. The author of the freeware usually retains the copyright.

Fyzické aktivum**Physical asset**

Aktivum mající materiální charakter.

Asset having a material character.

Fyzické řízení přístupu**Physical access control**

Použití fyzických mechanizmů k zajištění řízení přístupu (např. umístění počítače v uzamčené místnosti). Více **Access Control**.

*Use of physical mechanisms to enable control of access (e.g. placing the computer in a locked room). See **Access Control**.*

Generické TLD**Generic TLD**

Více **TLD**.

*See **TLD**.*

GNU / GPL**GNU / GPL**

Všeobecná veřejná licence GNU – licence pro svobodný software vyžadující, aby byla odvozená díla dostupná pod stejnou licencí.

General public licence GNU – licence for free software requesting that related creations be available under the same licence.

PGP**GNU privacy guard (GPG)**

Bezplatná verze **PGP**. Více **PGP**.

Free version of PGP. See PGP.

Grey hat**Grey hat**

Osoba, která podle své činnosti je něco mezi hackerem **White hat** a **Black hat**, protože zneužívá bezpečnostní slabinu systémů nebo produktu k tomu, aby veřejně upozornila na jejich zranitelnost. Avšak zveřejnění takovýchto citlivých informací může být příležitostí k páchnání trestné činnosti osobám typu **Black hat**.

An individual who according to the activity stands between White hat and Black hat hackers, since the individual abuses security weakness of systems or a product in order to publicly draw attention to their vulnerability. However, publicizing these sensitive information may be an opportunity to persons of the Black hat character to commit criminal acts.

Hack / Hacking**Hack / Hacking**

Často se používá ve smyslu hesla **Crack**. Druhé obvyklé použití je ve smyslu podařeného, neobvyklého, nápaditého, či rychlého vyřešení programátorského či administrátorského problému.

Often used in the sense under the entry Crack. The second usual use is in the sense of a fitting, unusual, witty, or fast solution of a programming or administrative issue.

Hacker**Hacker**

Osoba: (1) která se zabývá studiem a prozkoumáváním detailů programovatelných systémů nejčastěji pro intelektuální zvídavost a tuto schopnost si neustále zdokonaluje (White hat), (2) kterou baví programování a která dobře a rychle programuje, (3) která je expertem pro určitý operační systém nebo program, např. UNIX. Pojem Hacker se často nesprávně používá pro osoby, které zneužívají svých znalostí při pronikání do informačního systému a tak porušují zákon. Více **Cracker**.

Person: (1) who engages in the study and analysis of details of programmable systems most often for an intellectual inquisitiveness and keeps on improving this ability (White hat); (2) who enjoys programming and who programs well and fast; (3) who is an expert for a certain operating system or a programme, e.g. UNIX. The idea of Hacker is often improperly used for persons who abuse their knowledge during breaking into an information system and thus break the law. See Cracker.

Hackers for hire (H4H)

Akronym pro hackery, kteří nabízejí své služby jiným kriminálním, teroristickým nebo extremistickým skupinám (najmutí hackeři).

Acronym for hackers who offer their services to other criminal, terrorist or extremist groups (hired hackers).

Hactivism

Použití hackerských dovedností a technik k dosažení politických cílů a podpoře politické ideologie.

Use of hacker skills and techniques to achieve political objectives and to support political ideology.

Havarijní plán

Plán pro záložní postupy, odezvu na nepředvídanou událost a obnovu po havárii.

Plan for backup procedures, response to an unforeseen event and recovery after a contingency.

Havarijní postup**Contingency procedure**

Postup, který je alternativou k normálnímu postupu zpracování pro případ, že nastane neobvyklá, ale předpokládaná situace.

Procedure which is an alternative to the normal procedure in case of an occurrence of an unusual but assumed situation.

Heslo**Password**

Znakový řetězec používaný jako součást autentizační informace. Obecný prostředek k autentizaci uživatele pro přihlášení k počítači, k přístupu k souborům, programům a službám.

Character string used as part of the authentication information. General instrument to authenticate a user signing up to a computer, accessing files, programmes and services.

Hodnocení rizik**Risk evaluation**

Proces porovnání výsledků analýzy rizik s kritérii rizik k určení, zda je míra rizika přijatelná (akceptovatelná).

Process to compare the results of risk analyses with risk criteria to find out if the risk level is acceptable.

Hodnocení zranitelností**Vulnerability assessment**

Proces identifikace, kvantifikace a prioritizace (nebo hodnocení) zranitelností systému.

Process of identifying, quantifying, and prioritizing (or ranking) the

vulnerabilities in a system.

Hodnocení zranitelností a řízení zranitelností (VA/VM)

Viz hodnocení zranitelností a řízení zranitelností.

Vulnerability assessment and vulnerability management (VA/VM)

See Vulnerability assessment and Vulnerability management.

Hodnota aktiv

Objektivní vyjádření obecně vnímané hodnoty nebo subjektivní ocenění důležitosti (kritičnosti) aktiva, popř. kombinace obou přístupů.

Objective expression of a generally perceived value or a subjective evaluation of the importance (criticality) of an asset, or a combination of both approaches.

Honeypot

Slouží jako návnada lákající útočníka (malware), přičemž po zachycení potenciálně nebezpečného software dochází k jeho automatizované analýze.

Serves as a bait luring the attacker (malware) and after trapping a potentially dangerous software there is an automatic analysis.

Honeypot

Horká linka

On-line (zpravidla telefonická) služba, kterou nabízí automatizovaný informační systém a prostřednictvím které mohou uživatelé získat pomoc v oblasti použití společných či specializovaných služeb systému.

Online (as a rule, telephone) service offered by an automated information system and through which users can get help for using shared or specialized services of the system.

Hromadné rozesílání nevyžádané pošty

Hromadné rozesílání nevyžádaných zpráv elektronickými prostředky – nejčastěji elektronickou poštou.

Mass distribution of unsolicited messages by electronic means – most often by electronic mail.

Spamming

Hrozba

Potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace.

Potential cause of an unwanted incident which may result in damage to a system or organization.

Threat

Hypertext transfer protocol (HTTP) Hypertext transfer protocol (HTTP)

Aplikační protokol pro distribuované, kolaborativní, multimediální informační systémy. HTTP je základem datových přenosů pro celosvětovou síť WWW.

An application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

Hypertext transfer protocol secure (HTTPS)**Hypertext transfer protocol secure (HTTPS)**

Široce používaný komunikační protokol pro bezpečnou komunikaci přes počítačovou síť, zvlášť široce používán na Internetu. Technicky se nejedná o protokol jako takový, spíše je výsledkem prostého vrstvení protokolu HTTP na protokol **SSL/TLS** a tak dodává standardní komunikaci **HTTP** ještě bezpečnostní možnosti.

A widely used communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. Technically, it is not a protocol in and of itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications.

Charakteristika viru (signatura viru)**Virus signature**

Jedinečný bitový řetězec, který dostatečným způsobem virus identifikuje, a který může být využit skenovacím programem pro detekci přítomnosti viru.

Unique bit string which sufficiently identifies the virus and which can be used by a scanning programme to detect virus presence.

Chat**Chat**

Způsob přímé (on-line) komunikace více osob prostřednictvím Internetu.

Way of direct (online) communication of several persons using the Internet.

Chyba**Bug**

V **ICT** označení pro programátorskou chybu, která v software způsobuje bezpečnostní problém. Útočník využívá takovou zranitelnost pro ovládnutí počítače, znefunkčnění nebo chybné chování běžící služby, modifikaci dat apod. *Term in ICT to denote a programming error which causes a security problem in software. The attacker utilizes such a vulnerability to control the computer, make a running service dysfunctional or running improperly, to modify data and similar.*

Chybný přístup

Neautorizovaný a obvykle neúmyslný přístup k datům v systému zpracování dat, který je výsledkem selhání hardware nebo software.

Unauthorized and usually unintentional access to data in a data processing system which is the result of hardware or software failure.

ICMP záplava

Útok využívající protokol ICMP. Nejčastěji se využívají pakety ICMP echo (Ping), které slouží ke zjišťování, zda je vzdálené (cílové) zařízení dostupné. Zasláním velkého počtu těchto ICMP zpráv (nebo velkých ICMP echo paketů) může být docíleno zahlcení vzdáleného systému a jeho zpomalení nebo úplnou nedostupnost. Jedná se o velmi lehce proveditelný útok typu **DDoS**.

An attack using the ICMP protocol. Most often used are ICMP echo (Ping) packets which serve to establish if the remote (target) equipment is available. Sending out a large number of these ICMP messages (or large ICMP echo packets) may result in clogging the remote system and its slowdown or total unavailability. This is a simply executed attack of the DDoS type.

Identifikace

Akt nebo proces, během kterého entita předloží systému nějaký identifikátor, na jehož základě systém může rozpoznat entitu a odlišit ji od jiných entit.

Act or process during which an entity submits an identifier to the system and on its basis the system can recognize the entity and differentiate it from other entities.

Identifikace / ID uživatele

Znakový řetězec nebo vzorec používaný systémem zpracování dat k identifikaci uživatele.

Character string or a formula used by a data processing system for user identification.

Identifikace rizik

Proces hledání, rozpoznávání a popisování rizik.

Process of looking for, recognizing, and describing risks.

Identifikační předmět

Předmět používaný pro zjištění a ověření (autentizaci) identity.

Token used to find out and verify (authenticate) the identity.

Failure access**ICMP flood****Identification****User identification****Risk identification****Identity token**

Identifikátor

Informace o identitě, která v dané doméně jednoznačně rozlišuje mezi entitami.

Identity information that unambiguously distinguishes one entity from another one in a given domain.

Identita

Sada vlastností, které jednoznačně určují konkrétní objekt – věc, osobu, událost.

Set of attributes which uniquely define a definite object – a thing, person, and event.

Incident

V prostředí **ICT** je incidentem myšlena událost, která je obvykle spojená s výpadkem sítě, služby nebo se zhoršením jejich kvality.

Incident in the ICT environment assumed to be an event which is usually related to the outage of a network, service, or to a deterioration of its quality.

Informace

Každý znakový projev, který má smysl pro komunikátora i příjemce.

Any sign expression which makes sense for the communicator and receiver.

Informace o autentizaci**Authentication information**

Informace použitá k ustavení validity prohlašované identity dané entity.

Information used to establish validity of proclaimed identity of a given entity.

Informace řízení přístupu**Access control information (ACI)**

Jakákoliv informace použitá pro účely řízení přístupu, včetně kontextových informací.

Any information used for the purpose of access control including context information.

Informační (kybernetická) společnost**Information (cyber) society**

Společnost schopná využívat a využívající informační a komunikační technologie. Základem je neustálá výměna znalostí a informací a práce s nimi za předpokladu schopnosti jím rozumět. Tato společnost pokládá vytváření, šíření a manipulaci s informacemi za nejvýznamnější ekonomické a kulturní aktivity.

Society capable of utilizing, and indeed utilizing, information and communication technologies. The basis is an incessant exchange of knowledge

and information and handling them under the assumption of understanding these. This society considers creation, distribution and manipulation of information as the most significant economic and cultural activity.

Informační a komunikační technologie **Information and communication technology (ICT)**

Informační a komunikační technologií se rozumí veškerá technika, která se zabývá zpracováním a přenosem informací, tj. zejména výpočetní a komunikační technika a její programové vybavení.

Under information and communication technology we understand all technology dealing with processing and transfer of information, in particular computing and communication technology and software.

Informační aktivum **Information asset**

Znalosti a data, která mají pro organizaci hodnotu (význam).

Knowledge and data of value (importance) to an organization.

Informační kriminalita **Info-crime**

Trestná činnost, pro kterou je určující vztah k software, k datům, respektive uloženým informacím, respektive veškeré aktivity, které vedou k neautorizovanému čtení, nakládání, vymazání, zneužití, změně nebo jiné interpretaci dat.

Criminal activity with a determined relation to software, data, more precisely to stored information, more precisely all activities resulting in unauthorized reading, handling, erasing, abusing, changing or other data interpreting.

Informační operace (IO) **Information operation (IO)**

Plánovaná, cílevědomá a koordinovaná činnost prováděná na podporu politických a vojenských cílů operace, k ovlivnění rozhodovacího procesu možného protivníka a jeho spojenců působením na jeho informace, informační procesy a komunikační infrastrukturu při současném využívání a ochraně vlastních informací a komunikační infrastruktury. IO jsou výhradně vojenskou aktivitou (činností), která má koordinovat vojenské informační aktivity, jejichž cílem je ovlivnit myšlení (vůli), chápání a možnosti protivníka nebo potencionálního protivníka. Veškeré informační aktivity by měly být vedeny v souladu s cíli vojenské operace, a zároveň je podporovat.

Planned, goal-oriented and coordinated activity done in support of political and military objectives of an operation, to influence the decision-making process of a possible adversary and its allies by affecting its information, information processes and communication infrastructure and at the same using information and protection for own information and communication infrastructure. IO is exclusively a military activity which has to coordinate military information

activities with the objective of influencing the thinking (will), understanding and capabilities of the adversary or potential adversary. All information activities should be conducted in line with the objectives of the military operation and to support them at the same time.

Informační systém**Information system**

(1) Je funkční celek zabezpečující cílevědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací a dat. Zahrnuje datové a informační zdroje, nosiče, technické, programové a pracovní prostředky, technologie a postupy, související normy a pracovníky; (2) komplex prvků, nacházejících se ve vzájemné interakci (L. von Bertallanfy, 1956).

(1) A functional aggregate enabling goal-oriented and systematic acquisition, processing, storage and access to information and data. Includes data and information sources, mediums, hardware, software and utilities, technologies and procedures, related standards and employees; (2) A complex of elements existing in mutual interaction (L. von Bertallanfy, 1956).

Information assurance**Information assurance**

Soubor opatření k dosažení požadované úrovně důvěry v ochranu komunikačních, informačních a jiných elektronických i ne-elektronických systémů a informací ukládaných, zpracovávaných nebo přenášených v těchto systémech s ohledem na důvěrnost, integritu, dostupnost, neodmítnutelnost a autentičnost.

Set of measures to achieve the required level of confidence in the protection of communication, information and other electronic as well non-electronic systems and information stored, processed or transferred in these systems with regard to confidentiality, integrity, availability, undeniability and authenticity.

Informatizace společnosti**Informatisation of society**

Proces prosazování nové gramotnosti ve společnosti založené na zvládnutí nových metod práce s počítačem, s informacemi a informačními technologiemi.

Process of promoting new literacy in a society focused on adopting new methods of work with computers, information and information technology.

Infoware**Infoware**

Aplikace pro informatickou podporu klasických bojových akcí, respektive jako soubor aktivit, které slouží k ochraně, vytěžení, poškození, potlačení nebo zničení informací nebo informačních zdrojů, s cílem dosáhnout významné výhody v boji nebo vítězství nad konkrétním protivníkem. Pojem Infoware nelze zaměňovat s termínem Infowar, tj. informační válka.

Application for the automatic support of classical battle events, more precisely a set of activities serving to protect, mine out, damage, suppress or destroy

information or information sources, with the objective of achieving a significant advantage in a battle or victory over a concrete adversary. The notion of Infoware must not be mistaken with the notion Infowar that is information war.

Infrastruktura veřejných klíčů**Public Key Infrastructure (PKI)**

V kryptografii se jedná o označení infrastruktury pro správu a distribuci veřejných klíčů z asymetrické kryptografie. PKI díky přenosu důvěry umožňuje používat pro ověření elektronického podpisu cizí veřejné klíče, aniž by bylo nutné každý z nich individuálně prověřovat. Přenos důvěry lze realizovat buď pomocí certifikační autority (X.509), nebo pomocí důvěrných sítí (např. PGP).

This in cryptography denotes infrastructure for the management and distribution of public keys from asymmetric cryptography. PKI, thanks to transfer of confidence, enables the use of unfamiliar public keys for the verification of electronic signature without having to verify each individually. The transfer of confidence can be implemented either by means of the certification authority (X.509) or by trusted network (e.g. PGP).

Insider**Insider**

Nebezpečný uživatel (zaměstnanec, stážista), který zneužívá svého legálního přístupu do komunikačního a informačního systému organizace zejména k neoprávněnému odcizování citlivých dat a informací.

Dangerous user (employee, intern) who abuses a legal access to the communication and information system of an organization, in particular in order to perform unauthorized pilferage of sensitive data and information.

Integrita**Integrity**

Vlastnost ochrany přesnosti a úplnosti aktiv.

Attribute of protection for accuracy and completeness of assets.

Integrita dat**Data integrity**

Jistota, že data nebyla změněna. Přeneseně označuje i platnost, konzistence a přesnost dat, např. databází nebo systémů souborů. Bývá zajišťována kontrolními součty, hašovacími funkcemi, samoopravnými kódy, redundancí, žurnálováním atd. V kryptografii a v zabezpečení informací všeobecně integrita znamená platnost dat.

Assurance that data were not changed. In the figurative sense denotes also the validity, consistency and accuracy of data, e.g. databases or file systems. It tends to be implemented by checksums, hash functions, self-correcting codes, redundancy, journalling, etc. In cryptography and information security in general, integrity means data validity.

Integrita sítě

Funkčnost a provozuschopnost propojených sítí elektronických komunikací, ochrana těchto sítí vůči poruchám způsobeným elektromagnetickým rušením nebo provozním zatížením.

Functionality and operational capability of interconnected networks of electronic communications, protection of these networks against failures caused by electromagnetic jamming or operational loading.

Integrita systému

Kvalita systému zpracování dat plnicího svůj provozní účel a zabraňující přitom neautorizovaným uživatelům provádět změny zdrojů nebo používat zdroje a zabraňující autorizovaným uživatelům provádění nesprávných změn zdrojů nebo je nesprávně používat. Vlastnost, že systém vykonává svou zamýšlenou funkci nenarušeným způsobem, bez záměrné nebo náhodné neautomatizované manipulace se systémem.

Quality of a data processing system fulfilling its operational purpose and at the same time preventing unauthorized users from making changes in resources or from using the resources or from improper use of these. Property that a system performs its intended function without disruption, without intentional or accidental non-automated system manipulation.

Internet

Globální systém propojených počítačových sítí, které používají standardní internetový protokol (TCP/IP). Internet slouží miliardám uživatelů po celém světě. Je to síť sítí, která se skládá z milionů soukromých, veřejných, akademických, obchodních a vládních sítí, s místním až globálním rozsahem, které jsou propojeny širokou škálou elektronických, bezdrátových a optických síťových technologií.

Global system of interconnected computer networks which use the standard internet protocol (TCP/IP). Internet serves billions of users around the world. It is a network of networks consisting of millions of private, public, academic, commercial and government networks, with a local to global outreach, that are all interconnected by a wide range of electronic, wireless and optical network technologies.

**Internet control message protocol
(ICMP)**

Jedná se o služební protokol, který je součástí **IP** protokolu. Jeho hlavním úkolem je zasílání chybových hlášení ohledně dostupnosti služeb, počítačů nebo routerů. K této účelům se využívá například nástroj ping nebo traceroute.

This is a service protocol which is part of the IP protocol. Its main mission is to report error messages regarding the availability of services, computers or

Network integrity**System Integrity****Internet****Internet control message protocol
(ICMP)**

routers. For these purposes, ping or tracerout instruments are used, for example.

Internet Protocol (IP)

Protokol, pomocí kterého spolu komunikují všechna zařízení na Internetu. Dnes nejčastěji používaná je jeho čtvrtá revize (IPv4), postupně se však bude přecházet na novější verzi (IPv6).

Protocol by which all equipment in the Internet mutually communicate. Today, the most used is the fourth revision (IPv4); however, step by step there will be a transition to a newer version (IPv6).

**Internetová společnočnost pro
přidělování jmen a čísel na
internetu (ICANN)**

Nezisková asociace odpovědná za řízení přidělování doménových jmen a **IP adres**, zachování provozní stability internetu, podporu hospodářské soutěže, k dosažení širokého zastoupení globální internetové komunity, a rozvíjet vhodné politiky a standardy, a rozvíjet své poslání prostřednictvím řízení zespoda – nahoru, a procesech konsensu.

*Non-profit organization responsible for the administration of domain names assignment as well **IP addresses**, for the maintenance of operational stability of internet, support of economic competition, achievement of broad representation of the global internet community, and which develops its mission by a bottom-to-top management and consensual processes.*

Interoperabilita

Schopnost společně působit při plnění stanovených cílů, neboli schopnost systémů, jednotek či organizací poskytovat služby jiným systémům, jednotkám či organizacím a akceptovat je od nich a používat takto sdílené služby pro efektivní společnou činnost.

Capability to act jointly in fulfilling set objectives, or the capability of systems, units or organizations to provide services to other systems, units or organizations and accept these from them and thus use shared services for an effective common activity.

Intranet

„Privátní“ (interní) počítačová síť využívající klasické technologie Internetu, která umožňuje zaměstnancům organizace efektivně vzájemně komunikovat a sdílet informace.

Private (internal) computer network using the classical Internet technology making it possible for employees of an organization to communicate effectively and share information.

Internet protocol (IP)**Internet corporation for assigned
names and numbers (ICANN)****Interoperability****Intranet**

IP adresa**IP address**

Číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP (internetový protokol) slouží k rozlišení síťových rozhraní připojených k počítačové síti. V současné době nejrozšířenější verze IPv4 používá 32b číslo zapsané dekadicky po osmicech bitů (např. 123.234.111.222).
Number which uniquely identifies a network interface which uses IP (internet protocol) and serves for the differentiation of interfaces connected in the computer network. At present, the most widespread version IPv4 uses a number of 32 bits written in decimal in groups of eight bits (e.g. 123.234.111.222).

IRC**Internet relay chat (IRC)**

Forma živé (real-time) komunikace textových zpráv (chat) nebo synchronní konference. Jedná se o systémy určené zejména pro skupinové komunikace v diskusních fórech, tzv. kanály, ale také umožňuje one-to-one (jedna-ku-jedné) komunikace přes soukromou zprávu, jakož i chat a přenos dat prostřednictvím přímého Klient-s-klientem (client-to-client). Dnes již není tolik používán, nahradili jej novější nástroje jako Skype, ICQ nebo Jabber.

Form of live (real-time) communication of text messages (chat) or synchronous conferences. These are systems intended primarily for group communications in discussion forums, so-called channels, but it enables also one-to-one communication via a private message, as well as a chat and data transfer using direct client-to-client. Today, it is not used so much; it has been replaced by newer instruments such as Skype, ICQ or Jabber.

IT síť**IT network**

Systém geograficky rozptýlený tvořený propojenými IT systémy pro výměnu dat, obsahující různé složky propojených IT systémů a jejich rozhraní s datovými a komunikačními sítěmi, které je doplňují.

Geographically distributed system formed by interconnected IT systems for information exchange and containing different components of the interconnected systems and their interfaces with data communication networks which complement them.

IT systém**IT system**

Soubor zařízení, metod, dat, metadat, postupů a případně osob, který je uspořádán tak, aby plnil funkce při zpracování informací

Set of devices, methods, data, metadata, procedures and sometimes persons that is arranged so as to fulfil some functions during information processing.

Keylogger (Keystroke logger)**Keylogger (Keystroke logger)**

Software, který snímá stisky jednotlivých kláves, bývá však antivirem

považován za virus, v případě softwaru se jedná o určitou formu spyware, ale existují i hardwarové keyloggery. Často se používá pro utajený monitoring všech aktivit na PC, jenž je pro ostatní uživatele neviditelný a chráněný heslem. Umožňuje automatické zaznamenávání všech stisků kláves (psaný text, hesla apod.), navštívených www stránek, chatů a diskuzí přes ICQ, MSN apod., spouštěných aplikací, screenshotů práce s počítačem, práce uživatele se soubory a další. Zaznamenaná data mohou být skrytě odesílána emailem.

Software reading when individual keys are pushed; may however be regarded as a virus by an antivirus programme, in case of software it may be a certain form of spyware but there are even hardware keyloggers. It is often used for secret monitoring of all PC activities, is invisible for other users and protected by a password. It enables automatic logging of all keystrokes (written text, passwords, etc.), visits to www pages, chats and discussions over ICQ, MSN and similar, running applications, screenshots of computer work, user file handling and other. Logged data could be secretly sent by email.

Klepání na porty

Port Knocking

Označuje v počítačových sítích metodu, jak si z nedůvěryhodného počítače otevřít přístup do počítače nebo počítačové sítě chráněné firewallem bez nutnosti se na počítač s firewallem přihlásit a jako administrátor jeho nastavení změnit. Tento způsob umožňuje mít firewall vůči nedůvěryhodným počítačům zdánlivě úplně uzavřený a přesto mít možnost pomocí speciální utajené sekvence paketů jeho nastavení změnit. Metoda umožňuje vyhnout se zneužití bezpečnostních chyb v programech obsluhujících trvale otevřené porty.

Denotes a method in computer networks how to gain access from an untrusted computer into a computer or computer network protected by a firewall, without the need to sign on with the computer protected by a firewall and change the setting like an administrator. This way creates a semblance that the firewall is closed to untrusted computers and yet gives a chance of changing the setting by a special secret sequence. The method bypasses abuse of security errors in programmes serving permanently open ports.

Kód autentizace zprávy

Message authentication code

Bitový řetězec, který je funkcí dat (v zašifrovaném nebo nezašifrovaném tvaru) a tajného klíče a je připojen k datům, aby umožnil autentizaci dat.

Bit string which is a function of data (in an encrypted or plain form) and the secret key, and is attached to data in order to authenticate them.

Kompromitace

Compromising

Narušení informační bezpečnosti, které může mít za následek modifikaci programů nebo dat, jejich zničení, nebo jejich dostupnost pro neautorizované entity.

Compromise of information security which may result in programme or data modification, their destruction, or their availability to unauthorized entities.

Komunikace rizika

Výměna nebo sdílení informací o riziku mezi tím, kdo rozhoduje a ostatními zúčastněnými stranami.

Exchange or sharing of information between the decision-maker and other participating parties.

Komunikační systém

Systém, který zajišťuje přenos informací mezi koncovými účastníky. Zahrnuje koncové komunikační zařízení, přenosové prostředí, správu systému, personální obsluhu a provozní podmínky a postupy. Může zahrnovat i prostředky kryptografické ochrany.

System which provides for the transfer of information among end users. It includes end communication devices, transfer environment, system administration, handling by personnel and operational conditions and procedures. It may also include means of cryptographic protection.

Konfigurační databáze**Configuration management database (CMDB)**

Úložiště dat používané pro záznam atributů konfiguračních položek a vztahů mezi konfiguračními položkami po celou dobu jejich životního cyklu.

Data warehouse used for records of configuration items' attributes and relations among configuration items during their whole life cycle.

Konfigurační položka**Configuration item (CI)**

Prvek, který musí být řízen za účelem dodávání služby nebo služeb.

Element which must be controlled in order to deliver a service or services.

Kontaminace**Contamination**

Vložení dat s určitou bezpečnostní klasifikací nebo bezpečnostní kategorií do nesprávné bezpečnostní kategorie.

Input of data with a certain security classification or security category into a wrong security category.

Kontinuita činností organizace**Business continuity**

Procesy a/nebo postupy k zajištění nepřetržitého chodu organizace.

Processes and/or procedures to ensure continuous operation of an organization.

Kontinuita služeb

Schopnost řídit rizika a události, které by mohly mít vážný dopad naslužby s cílem nepřetržitě dodávat služby na dohodnutých úrovních.

Capability to manage risks and events which could seriously impact services, with the objective of providing continuous services at the agreed levels.

Kriminalita, související s pokročilými technologiemi

Trestná činnost, zaměřená na vyspělou techniku jako cíl, prostředí nebo nástroj pachatele trestného činu (zpravidla se jedná zároveň aktivitu, označitelnou za „počítačovou“ či „informační“ kriminalitu). Ve své podstatě přitom může jít ve všech výše zmíněných variantách o velmi různorodou směsici činu, kdy konkrétní technologie může být jak předmětem zájmu, objektem (prostředím) nebo nástrojem pro jejich uskutečnění. To v konečném důsledku může vést k přístupu, kdy je zmíněná množina aktivit chápána: (1) značně široce („jakákoli trestná či jinak závadová činnost s prvky výpočetní techniky“), včetně případu, kdy je např. počítačová sestava použita při padělání peněz nebo cenných listin; (2) značně úzce tedy výhradně jako činy, spáchané proti informačním technologiím, které nemohou být spáchány žádným jiným způsobem ani proti jinému cíli.

Criminal activity focused on advanced technology as the objective, means or instrument of the criminal act perpetrator (often it is also the activity which could be labelled as "computer" or "information" criminality). In essence, in all of these versions it may be a very diverse mixture of activities when concrete technology may be the item of interest, the object (environment), or the instrument for the act. This can, as the final consequence, lead to the approach when the above-mentioned set of principles is considered: (1) rather broadly ("any criminal or otherwise harmful activity with the elements of computing technology"), including the case when, for example, a computer system is used for money or stock counterfeiting; (2) rather narrowly that is as acts committed against information technologies, which cannot be committed by any other means nor against any other target.

Kritéria rizika

Referenční hodnoty parametrů, podle kterých se hodnotí závažnost rizika.

Reference values of parameters which are used to assess risk severity.

Kritická informační infrastruktura **Critical information infrastructure**

Zákonem jasně vymezený komplex informačních systémů, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva.

Service continuity**High-tech crime****Risk criteria**

Complex of information systems clearly defined by law, whose unfunctionality would result in a serious impact on state security, economy, public administration and provision of the basic daily needs of population.

Kritická infrastruktura**Critical infrastructure**

Systémy a služby, jejichž nefunkčnost nebo špatná funkčnost by měla závažný dopad na bezpečnost státu, jeho ekonomiku, veřejnou správu a v důsledku na zabezpečení základních životních potřeb obyvatelstva.

Systems and services whose unfunctionality or wrong functionality would result in a serious impact on state security, its economy, public administration and in the end on provision of the basic daily needs of population.

**Kritická komunikační
infrastruktura (státu)****Critical communication
infrastructure**

V případě státu: zákonem jasně vymezený komplex služeb nebo sítí elektronických komunikací, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva.

In case of the state: complex of services or networks of electronic communications, clearly defined by law, whose unfunctionality would result in a serious impact on state security, public administration and provision of the basic daily needs of the population.

Krise**Crisis**

Situace, ve které je významným způsobem narušena rovnováha mezi základními charakteristikami systému na jedné straně a postojem okolního prostředí na straně druhé.

Situation where the equilibrium among the basic components of the system on the one hand, and approach of the environment on the other hand, is disrupted in a serious way.

Krizová připravenost**Crisis preparedness**

Příprava opatření k řešení vlastních krizových situací a k podílu na řešení krizových situací ve svém okolí.

Preparation of measures to solve own crisis situations and partially participate in solving crisis situations in the neighbourhood.

Krizová situace**Crisis / Emergency situation**

Mimořádná událost podle zákona o integrovaném záchranném systému, narušení kritické infrastruktury nebo jiné nebezpečí, při nichž je vyhlášen stav nebezpečí, nouzový stav nebo stav ohrožení státu (dále jen „krizový stav“).

Emergency situation as per the law on integrated emergency system, compromise of the critical infrastructure, or any other danger when a state of hazard, state of emergency, or threat to the state is announced (henceforth only "emergency situation").

Krizové opatření**Crisis measure**

Organizační nebo technické opatření určené k řešení krizové situace a odstranění jejích následků, včetně opatření, jimiž se zasahuje do práv a povinností osob.

Organizational or technical measure to solve a crisis situation and remedy its consequences, including measures interfering with the rights and obligations of people.

Krizové plánování**Crisis planning**

Aktivita příslušných orgánů krizového řízení zaměřená na minimalizaci (prevenci) možnosti vzniku krizových situací. Hledání nejvhodnějších způsobů protikrizové intervence, optimalizaci metod a forem zvládání těchto nežádoucích jevů (tj. redukci dopadů krizových situací) a stanovení nejracionálnějších a ekonomicky nejvýhodnějších cest obnovy postižených systémů a jejich návratu do nového běžného stavu.

Activity of the relevant bodies of crisis management aimed at minimizing (prevention of) the origin of crisis situations. Searching for the most suitable ways of anti-crisis intervention, optimization of methods and forms to handle these unwanted phenomena (that is, reduction of the impacts of crisis situations) and establishing the most rational and economical ways of recovery for the affected systems and their return into the normal daily state.

Krizové řízení**Crisis management**

Souhrn řídících činností orgánů krizového řízení zaměřených na analýzu a vyhodnocení bezpečnostních rizik a plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s přípravou na krizové situace a jejich řešením, nebo ochranou kritické infrastruktury.

Collection of management activities of the bodies of crisis management aimed at the analysis and evaluation of security risks and planning, organization, implementation and verification of activities conducted in connection with Preparation for crisis situations and their solution or protection of critical infrastructure.

Krizový plán**Crisis plan**

Souhrnný plánovací dokument, který zpracovávají zákonem stanované subjekty, a který obsahuje souhrn opatření a postupů k řešení krizových situací.

Aggregate planning document elaborated by entities set forth by law and which

contains a set of measures and procedures to solve crisis situations.

Krizový stav

Legislativní opatření vyhlášované Parlamentem ČR (stav ohrožení státu a válečný stav), vládou ČR (nouzový stav) nebo hejtmanem kraje / primátorem (stav nebezpečí) za účelem řešení krizové situace.

Legislative measure announced by the Parliament of the Czech Republic (threat to the state, and the state of war), by the Government of the Czech Republic (state of emergency) or governer of the region/mayor (state of danger), in order to solve a crisis situation.

Kryptografie

Nauka o šifrování – disciplína, která zahrnuje zásady, prostředky a metody pro transformaci dat aby byl ukryt jejich sémantický obsah, zabráněno jejich neautorizovanému použití nebo zabráněno jejich nezjištěné modifikaci.

Science of cryptography – a discipline covering the principles, means and methods to transform data in order to conceal their semantic content, to prevent an unauthorized use or prevent unrecognized modification.

Kybergrooming (Child grooming, Cyber grooming (Child grooming, Kybergrooming)

Chování uživatelů internetových komunikačních prostředků (chat, ICQ atd.), kteří se snaží získat důvěru dítěte a s cílem ho zneužít (zejm. sexuálně) či zneužít k nelegálním aktivitám.

Behaviour of users of internet communication instruments (chat, ICQ, et al.) who try to get the trust of a child in order to either abuse the child (especially sexually) or misuse the child for illegal activity.

Kybernetická bezpečnost

Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.

Collection of legal, organizational, technological and educational means aimed at providing protection of cyberspace.

Kybernetická kriminalita

Trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti (Více také **Počítačová kriminalita**).

Crisis state**Cryptography****Cyber security****Cyber crime**

Criminal activity in which a computer appears in some way as an aggregate of hardware and software (including data), or only some of its components may appear, or sometimes a larger number of computers either standalone or interconnected into a computer network appear, and this either as the object of interest of this criminal activity (with the exception of such criminal activity whose objects are the described devices considered as immovable property) or as the environment (object) or as the instrument of criminal activity (See Computer crime).

Kybernetická obrana**Cyber defence**

Obrana proti kybernetickému útoku a zmírnování jeho následků. Také rezistence subjektu na útok a schopnost se účinně bránit.

Defence against a cyber attack and mitigation of its consequences. Also, resistance of the subject towards an attack and a capability to defend itself effectively.

Kybernetická strategie**Cyber strategy**

Obecný postup k rozvoji a využití schopností pracovat v kybernetickém prostoru, integrovaný a koordinovaný s ostatními operačními oblastmi k dosažení nebo podpoře dosažení stanovených cílů pomocí identifikovaných prostředků, metod a nástrojů v určitém časovém rozvrhu.

General approach to the development and use of capabilities to operate in cyberspace, integrated and coordinated with other areas of operation, in order to achieve or support the set objectives by using identified means, methods and instruments in a certain timetable.

Kybernetická špionáž**Cyber espionage**

Získávání strategicky citlivých či strategicky důležitých informací od jednotlivců nebo organizací za použití či cílení prostředků IT. Používá se nejčastěji v kontextu získávání politické, ekonomické nebo vojenské převahy.

Obtaining strategically sensitive or strategically important information from individuals or organizations by using or targetting IT means. It is used most often in the context of obtaining a political, economic or military supremacy.

Kybernetická válka**Cyber war, Cyber warfare**

Použití počítačů a Internetu k vedení války v kybernetickém prostoru. Soubor rozsáhlých, často politicky či strategicky motivovaných, souvisejících a vzájemně vyvolaných organizovaných kybernetických útoků a protiútoků.

Use of computers and the Internet to wage a war in cyberspace. System of extensive, often politically motivated, related and mutually provoked organized cyber attacks and counterattacks.

Kybernetický prostor

Digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.

Digital environment enabling the origin, processing and exchange of information, made up of information systems and the services and networks of electronic communications.

Kybernetický protiútok

Útok na IT infrastrukturu jako odpověď na předchozí kybernetický útok. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.

Attack on IT infrastructure as a response to a previous cyber attack. It is used most often in the context of either politically or militarily motivated attacks.

Kybernetický útok

Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.

Attack on IT infrastructure having the objective of causing damage and obtaining sensitive or strategically important information. It is used most often in the context of either politically or militarily motivated attacks.

Kyberterorismus

Trestná činnost páchaná za primárního využití či cílení prostředků IT s cílem vyvolat strach či neadekvátní reakci. Používá se nejčastěji v kontextu extremisticky, nacionalisticky a politicky motivovaných útoků.

Criminal activity done using or targeting primarily IT means with the objective of creating fear or inadequate response. It is used most often in the context of attacks having an extremist, nationalistic or politically motivated character.

Lamer

Osoba, zpravidla úplný začátečník, který se nevyzná v dané problematice IT.

Person, usually a complete beginner, who is unfiliar with the given IT issues.

Léčka

Úmyslné umístění zjevných závad do systému zpracování dat za účelem detekce pokusů o průnik nebo pro zmatení protivníka, které závady by měl využít.

Intentional placement of obvious defects into a data processing system in order to detect penetration attempts, or to deceive an adversary who should use the defect.

Cyberspace**Cyber counterattack****Cyber attack****Cyber terrorism****Lamer****Entrapment**

Leetspeak

Jazyk, který nahrazuje písmena latinské abecedy čísly a tisknutelnými znaky ASCII. Používá se hodně na internetu (chat a online hry). Tento počítačový dialekt zpravidla anglického jazyka nemá pevná gramatická pravidla a slova je možné tvořit také jejich zkracováním, např. vynecháním písmen nebo zkomolením („nd“ – end, „U“ – you, „r“ – are).

Language replacing the letters of the Latin alphabet by numerals and printable ASCII characters. It is used quite a lot in the internet (chat and online games). This computer dialect, usually of the English language, has no fixed grammatical rules and words may be formed by shortening, e.g. by omissions of letters or corruption ("nd" – end, "U" – you, "r" – are).

Licence

Oprávnění a také dokument, který toto oprávnění zaznamená.

Permission as well as to the document recording that permission.

Log

Zkrácený výraz pro Log file.

Shortened expression for Log file.

Leetspeak**Licence****Log****Logical bomb**

Škodlivá logika, která působí škodu systému zpracování dat a je spuštěna určitými specifickými systémovými podmínkami. Program (podmnožina Malware), který se tajně vkládá do aplikací nebo operačního systému, kde za předem určených podmínek provádí destruktivní aktivity. Logická bomba se skládá ze dvou základních částí: rozbušky a akce. Předem specifikovanou podmínkou startující logickou bombu může být například konkrétní datum (výročí určité události – Více např. „Virus 17. listopad“). V tomto případě se jedná o typ tzv. časované bomby (Time Bomb).

Harmful logic causing damage to a data processing system and being triggered by certain specific system conditions. Programme (subset of Malware) which is secretly put into applications or into an operating system where, under predetermined conditions, it performs destructive activities. Predetermined specified condition triggering the logical bomb may be, for example, a fixed date (anniversary of a certain event – See for example "Virus 17. November"). In this case the type is a so-called time bomb.

Logické řízení přístupu**Logical access control**

Použití mechanizmů týkajících se dat nebo informací k zajištění řízení přístupu.

Use of mechanisms related to data or information to enable control of access.

Lokální internetový registr**Local internet registry (LIR)**

Jedná se o organizaci působící obvykle v rámci jedné sítě, které je přidělen blok IP adres od RIR. LIR přiděluje bloky IP adres svým zákazníkům připojeným do dané sítě. Většina LIR jsou poskytovatelé internetových služeb, podniky či akademické instituce. Související výrazy – RIR.

Organization, usually active in one network, which is assigned a block of IP addresses from RIR. LIR assigns the IP address blocks to its customers connected to the given network. Most LIRs are internet service providers, companies or academic institutions. Related expressions – RIR.

Lokální síť (LAN)**Local area network (LAN)**

Označení pro malé sítě, obvykle v rámci administrativně jednotných celků – firem, budov, společenství, které jsou budované za účelem snadného sdílení prostředků (IS, dat, služby, zařízení) a umožňují efektivní ochranu a nežádoucích jevů.

Term for small networks, usually within administratively uniform aggregates – companies, buildings, communities, which are formed with the aim to facilitate sharing of means (IS, data, services, equipment) and to enable an effective protection against undesirable phenomena.

MAC adresa**MAC address**

MAC = Media Access Control. Jedinečný identifikátor síťového zařízení, který je přidělen výrobcem.

MAC = Media Access Control. Unique identifier of a network device allotted by the manufacturer.

Management bezpečnostních informací a událostí (SIEM)**Security information and event management (SIEM)**

Systém, jehož úkolem je sběr, analýza a korelace dat – událostí v síti. SIEM systémy kombinují metody detekce a analýzy anomálních událostí v síti, poskytují informace použitelné k řízení sítě a provozovaných služeb.

System whose task is to acquire, analyze and correlate data – events in the network. SIEM systems combine the methods of detection and analysis of abnormal events in the network, provide information usable for network management and operated services.

Maškaráda (IP maškaráda)

Mechanismus umožňující připojit do **Internetu** velké množství zařízení, pro které nejsou k dispozici tzv. veřejné **IP** adresy. Takováto zařízení dostanou přiděleny tzv. privátne IP adresy a přístup do Internetu se realizuje pomocí mechanismu překladu adres (NAT, Network Address Translation).

*Mechanism which allows to connect to the **Internet** a large number of devices for which no so-called public **IP addresses** are available. These devices are assigned so-called private **IP addresses** and access to the **Internet** is implemented through the mechanism of address translation (NAT, Network Address Translation).*

Minimální úroveň chodu organizace

Minimální úroveň služeb a/nebo produktů, která je přijatelná pro dosahování cílů organizace během havárie.

Minimal level of services and/or products which is acceptable to attain the objectives of an organization during a contingency.

Modrá obrazovka smrti

Slangové označení chybového hlášení, které operační systém Microsoft Windows zobrazí, pokud došlo k závažné systémové chybě, ze které není schopen se zotavit. Toto chybové hlášení se zobrazí přes celou obrazovku, bílým písmem na modrém pozadí (odtud název).

Slang expression for an error message displayed by the Microsoft Windows operating system if there is a serious system error from which the system cannot recover. This error message is screen-wide, white letters on blue background (hence the name).

Monitorování

Nepřetržitá kontrola, dozor, kritické pozorování nebo určování stavu pro identifikování změny od požadované nebo očekávané úrovně výkonnosti.

Permanent checking, supervision, critical observation or determination of status in order to identify a change from the required or expected level of performance.

Nápravné opatření

Opatření k odstranění příčiny zjištěné neshody nebo jiné nežádoucí situace.

Action to remove the cause of an identified noncompliance or other undesirable situation.

Masquerade (IP masquerading)**Minimum business continuity objective (MBCO)****Blue screen of death (BSOD)****Monitoring****Corrective action**

Národní autorita**National authority**

Státní úřad odpovědný za problematiku kybernetické bezpečnosti (gestor).

State authority responsible for the issues of cyber security (guarantee).

Následek**Consequence**

Výsledek události působící na cíle.

Result of an event which affects the objectives.

NATO CCD COE**NATO Cooperative cyber defence centre of excellence**

NATO středisko pro spolupráci v kybernetické obraně (*Filtры tee 12, Tallinn 10132, Estonsko, http://www.ccdcoe.org*).

NATO centre for cooperation in cyber security (Filters tee 12, Tallinn 10132, Estonia, http://www.ccdcoe.org).

NATO CDMA**NATO Cyber defence management authority**

Úřad NATO pro správu kybernetické obrany, jehož smyslem je zastřešovat a propojovat existující schopnosti kybernetické obrany v rámci Aliance.

NATO authority to manage cyber defence with the aim of providing an umbrella and interconnections for existing capabilities of cyber defence within the Alliance.

NATO CIRC – Technické centrum (NCIRC TC)**NATO computer incident response capability – Technical centre (NCIRT TC)**

Centrum technické podpory NATO CIRC – druhá úroveň. Zajišťuje schopnost reakce na incidenty, sledování incidentů, obnovení systémů a poskytuje přímou technickou podporu a pomoc provoznímu a bezpečnostnímu managementu provozovaných informačních systémů NATO.

NATO CIRC technical support centre – second level. It enables the capability to respond to incidents, monitor incidents, perform system recovery, and provides a direct technical support and help to the operational and security management of the operational NATO information systems.

Nepopiratelnost**Non-repudiation**

Schopnost prokázat výskyt údajné události nebo činnosti a vznikajících entit s cílem řešit spory o výskytu nebo absence výskytu události nebo činnosti a zapojení entit do události.

Capability to prove the occurrence of an alleged event or activity, and originating entities with the objective to solve controversies about the

occurrence of an event or an absence of an occurrence, or about the activity and involvement of entities into the events.

Neshoda**Nonconformity**

Nesplnění požadavku.

Non-conformity with a request.

Neustálé zlepšování**Continual improvement**

Opakující se činnost pro zvyšování schopnosti plnit požadavky.

Repeated activity for the increase of a capability to meet the requirements.

Nevyžádaná pošta**Spam**

Nevyžádaná reklamní pošta, nebo jiné nevyžádané sdělení, zpravidla komerčního charakteru, které je šířeno Internetem. Nejčastěji se jedná o nabídky afrodisiak, léčiv nebo pornografie. Není-li systém dostatečně zabezpečen, může nevyžádaná pošta tvorit značnou část elektronické korespondence.

Unsolicited mail such as commercials, or another unsolicited message, usually of a commercial character, which is distributed on the Internet. Most often these are offers for afrodisiacs, medicaments or pornography. Unless the system is adequately protected, unsolicited mail can make up a substantial part of electronic correspondence.

Období přístupu**Access period**

Časové období, během něhož je povolen přístup k určitému objektu.

Time period during which access to a certain object is allowed.

Obecné zahlcení**Generic traffic flood**

Forma útoku typu **DDoS**.

Form of a DDoS attack.

Obnova dat**Data restoration/ Data recovery**

Akt znovuvytvoření či znovuzískání dat, která byla ztracena, nebo byla narušena jejich integrita. Metody zahrnují kopírování dat z archívu, rekonstrukci dat ze zdrojových dat, nebo opakování ustavení dat z alternativních zdrojů.

Act of re-creation, or re-acquisition, of data lost, or whose integrity was compromised. Methods include copying from an archive, restoration of data from source data, or repeated establishment of data from alternative sources.

Obranná infrastruktura**Defence infrastructure**

Soubor objektů, staveb, pozemků a zařízení včetně nezbytných služeb, výrobních a nevýrobních systémů potřebných k zajištění jejich provozu, bez ohledu na formu vlastnictví a způsob využití, jejichž zničení, narušení nebo omezení jejich činnosti by za stavu ohrožení státu nebo za válečného stavu ohrozilo plnění úkolů: (1) Ozbrojených sil České republiky při realizaci Plánu obrany ČR a operačních plánů včetně mobilizačních opatření, (2) zpracovatelů při realizaci jejich dílčích plánů obrany a ostatních prvků bezpečnostního systému ČR, (3) spojeneckých ozbrojených sil při realizaci jejich operačních plánů, (4) ochrany obyvatelstva.

Set of objects, buildings, ground plots and equipment including necessary services, production and non-production systems needed to ensure their operation, regardless of the form of ownership and the way of utilization; whose destruction, damage or limitation of activity would, under situation of threat to the state or a state of war, put in danger fulfilment of tasks: (1) of Armed Forces of the Czech Republic (CZE) during the implementation of the Plan of defence of CZE as well as operational plans including plans for mobilization, (2) of experts during implementation of their partial plans of defence and other elements of security system of CZE, (3) of allied armed forces during the implementation of their operational plans, (4) of protection of population.

Obtížná zjistitelnost**Stealth**

Zabránění nebo omezení možnosti zjištění (identifikace) objektu.

Prevention or limitation of object's identification.

Odhad rizika**Risk estimation**

Proces k určení hodnot pravděpodobnosti a následků rizika.

Process to determine values of probability and consequences of risk.

Odhalení, prozrazení, zveřejnění**Disclosure**

V kontextu IT obvykle používáno k vyjádření faktu, že byla odhalena data, informace nebo mechanismy, které na základě politik a technických opatření měly zůstat skryty.

In IT context it is usually used for the expression of the fact that data, information or mechanisms were disclosed which should be hidden on the basis of policies and technical measures.

Odmítnutí služby

Odmítnutí služby je technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a k pádu nebo nefunkčnosti a nedostupnosti systému pro ostatní uživatele a to útokem mnoha koordinovaných útočníků.

Denial of service is the technique of attack by many coordinated attackers on the internet services or pages resulting in flooding by requests or breakdown or unfunctionality or unavailability of the system for other users.

Odolnost

Schopnost organizace, systému či sítě odolat hrozbám a čelit vlivu výpadků.

Capability of an organization, system or network to resist threats and brace itself against the influence of outages.

Odposlech**Wiretapping**

Jedná se o jakýkoliv odposlech telefonního přenosu nebo konverzace provedený bez souhlasu obou stran, pomocí přístupu na samotný telefonní signál.

This is any tapping of a telephone transmission or conversation done without the consent of both parties, by accessing the telephone signal proper.

Odposlech / Nežádoucí odposlech**Eavesdropping**

Neautorizované zachytávání informací.

Unauthorized catching of information.

Odposlech webu**Webtapping**

Sledování webových stránek, které pravděpodobně obsahují utajované nebo citlivé informace, a lidí, jež k nim mají přístup.

Monitoring of web pages which may contain classified or sensitive information, and of people, who have access to them.

Odpovědnost**Accountability**

Odpovědnost entity za její činnosti a rozhodnutí.

Responsiblity of an entity for its activity and decision.

Odvětvová kritéria**Sector criteria**

Technické nebo provozní hodnoty k určování prvku kritické infrastruktury v odvětvích energetika, vodní hospodářství, potravinářství a zemědělství, zdravotnictví, doprava, komunikační a informační systémy, finanční trh a měna, nouzové služby a veřejná správa.

Technological or operational values to determine an element of critical infrastructure in the sectors of energy, water management, food and agriculture, health, transport, communication and information systems, finance market and currencies, emergency services and public administration.

Ochrana dat**Data protection**

Administrativní, technická, procedurální, personální nebo fyzická opatření implementovaná za účelem ochrany dat před neautorizovaným přístupem nebo porušením integrity dat.

Administrative, technological, procedural, staffing or physical measures implemented in order to protect data against an unauthorized access or against corruption of data integrity.

Ochrana kritické infrastruktury**Critical infrastructure protection**

Opatření zaměřená na snížení rizika narušení funkce prvku kritické infrastruktury.

Measures aimed at lowering the risk of corruption of an element of the critical infrastructure.

Ochrana před kopírováním**Copy protection**

Použití speciální techniky k detekci nebo zamezení neautorizovaného kopírování dat, software a firmware.

Use of a special technique for the detection or prevention of unauthorized copying of data, software and firmware.

Ochrana souboru**File protection**

Implementace vhodných administrativních, technických nebo fyzických prostředků k ochraně před neautorizovaným přístupem, modifikací nebo vymazáním souboru.

Implementation of suitable administrative, technological or physical means for the protection against unauthorized access, modification or erasure of a file.

Opatření**Control**

Znamená řízení rizika, včetně politik, postupů, směrnic, obvyklých postupů (praktik) nebo organizačních struktur, které mohou být administrativní, technické, řídící nebo právní povahy.

It means control of a risk, including all policies, procedures, directives, usual procedures (practices) or organizational structures, which may be of an administrative, technological, management or legal character.

Open software foundation (OSF)**Open software foundation (OSF)**

Nezisková organizace založená v roce 1988 na základě zákona U.S. Cooperative Research Act of 1984, aby vytvořila otevřenou normu pro realizaci operačního

systému UNIX.

A not-for-profit organization founded in 1988 under the U.S. National Cooperative Research Act of 1984 to create an open standard for an implementation of the UNIX operating system.

Operační systém**Operating system**

Programové prostředky, které řídí provádění programů a které mohou poskytovat různé služby, např. přidělování prostředků, rozvrhování, řízení vstupů a výstupů a správu dat. Příkladem operačního systému je systém MS Windows, LINUX, UNIX, Solaris apod.

Software which controls programme executions and which can offer various services, e.g. assignment of devices, scheduling, control of input and output and data administration. Examples of operating systems are the MS DOS system, LINUX, UNIX, Solaris, and other.

Osobní počítač**Computer, personal computer (PC)**

V souladu se zněním CSN 36 9001 se jedná o „stroj na zpracování dat provádějící samočinné posloupnosti různých aritmetických a logických operací“. Jinými slovy: stroj charakterizovaný prací s daty, která probíhá podle předem vytvořeného programu uloženého v jeho paměti.

In accordance with the wording of CSN 36 9001 this is "a data processing machine executing independent sequences of various arithmetic and logical operations." In other words: a machine characterized by processing data according to a previously created programme stored in its memory.

Otevřené bezpečnostní prostředí**Open-security environment (OSE)**

Prostředí, ve kterém je ochrana dat a zdrojů před náhodnými nebo úmyslnými činy dosažena použitím normálních provozních postupů.

Environment where data and source protection against accidental or intentional acts is achieved by using standard operational procedures.

Otevřený komunikační systém**Open communication system**

Představuje (zahrnuje) globální počítačovou síť včetně jejích funkcionalit, podporovanou jak soukromými společnostmi, tak veřejnými institucemi.

It represents (includes) a global computer network including all its functions and supported both by private companies and public institutions.

Ovládnutí**Governance**

Zajištění toho, aby bezpečnostní politiky a strategie byly skutečně implementovány a aby požadované procesy byly korektně dodržovány.

Making sure that security policies and strategies be really implemented and that the required processes be correctly adhered to.

Paket

Blok dat přenášený v počítačových sítích, které používají technologii "přepojování paketu". Paket se skládá z řídících dat a z uživatelských dat. Řídící data obsahují informace nutné k doručení paketu (adresa cíle, adresa zdroje, kontrolní součty, informace o pořadí paketu). Uživatelská data obsahují ta data, která mají doručena do cíle (cílovému adresátovi).

Block of data transferred in computer networks and using the technology of "packet switching". A packet consists of control data and user data. Control data contain information necessary for packet delivery (destination address, source address, checksums, and information on packet priority). User data contain those data items which should be delivered to the target (destination addressee).

Pasivní hrozba

Hrozba zpřístupnění informací, aniž by došlo ke změně stavu systému zpracování dat nebo počítačové sítě.

Threat of making an access to data without actually changing the state of the data processing system or the computer network.

Páteřní síť

Ústřední část telekomunikační sítě, která poskytuje různé služby zákazníkům, připojených přes přístupovou síť.

Central part of a telecommunication network that provides various services to customers who are connected by the access network.

Penetrační testování

Zkoumání funkcí počítačového systému a sítí s cílem najít slabá místa počítačové bezpečnosti tak, aby bylo možno tato slabá místa odstranit.

Analysis of functions of a computer system and networks with the objective of finding out weak spots in computer security so that these could be removed.

Periferní zařízení

Zařízení, které je řízeno počítačem a může s ním komunikovat, např. jednotky vstupu/výstupu a pomocné paměti.

Equipment controlled by a computer and able to communicate with it, e.g. input/output devices and auxiliary memory.

Pharming

Podvodná metoda používaná na Internetu k získávání citlivých údajů od obětí útoku. Principem je napadení **DNS** a přepsání **IP** adresy, což způsobí přesměrování klienta na falešné stránky internetbankingu, e-mailu, sociální sítě, atd. po zadání **URL** do prohlížeče. Tyto stránky jsou obvykle k nerozeznání od

Packet**Passive threat****Network core****Penetration testing****Peripheral equipment****Pharming**

skutečných stránek banky a ani zkušení uživatelé nemusejí poznat tuto záměnu (na rozdíl od příbuzné techniky phishingu).

*Fraudulent method used on the Internet to obtain sensitive data from the victim of the attack. The principle is an attack on **DNS** and rewriting the **IP** address which results in redirecting the client to a false address of internetbanking, email, social network, etc., after inserting the **URL** into the browser. These pages are as a rule indistinguishable from the real pages of a bank and even experienced users may not recognize this change (unlike the related technique of phishing).*

Phishing („rybaření“, „rhybaření“, Phishing „házení udic“)

Podvodná metoda, usilující o zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtu apod. za účelem jejich následného zneužití (výběr hotovosti z konta, neoprávněný přístup k datům atd.). Vytvoření podvodné zprávy, šířené většinou elektronickou poštou, jež se snaží zmíněné údaje z uživatele vylákat. Zprávy mohou být maskovány tak, aby co nejvíce imitovaly důvěryhodného odesílatele. Může jít například o padělaný dotaz banky, jejíž služeb uživatel využívá, se žádostí o zaslání čísla účtu a PIN pro kontrolu (použití dialogového okna, předstírajícího, že je oknem banky – tzv. spoofing). Tímto způsobem se snaží přistupující osoby přesvědčit, že jsou na známé adrese, jejímuž zabezpečení důvěřují (stránky elektronických obchodů atd.). Tak bývají rovněž velice často zcizována například čísla kreditních karet a jejich PIN.

Fraudulent method having the objective of stealing the digital identity of a user, the sign-on names, passwords, bank account numbers and accounts etc. in order to subsequently misuse these (drawing cash from the account, unauthorized access to data etc). Creation of a fraudulent message distributed mostly by electronic mail trying to elicit the mentioned data from the user. The messages may be masqueraded so as to closely imitate a trustworthy sender. It may be a forged request from a bank whose services the user accesses with a request to send the account number and PIN for a routine check (use of the dialog window purporting to be a bank window – so-called spoofing). Thus the fraudster tries to convince accessing persons that they are at the right address whose security they trust (pages of electronic shops etc.). Also, very often credit card numbers and PINS are stolen in this fashion.

Phreaker

Osoba provádějící „hacking“ prostřednictvím telefonu. Používáním různých triků manipulujících se službami telefonních společností.

Person doing "hacking" on the phone, using various tricks manipulating the services of telephone companies.

Phreaker

Phreaking**Phreaking**

Označení pro napojení se na cizí telefonní linku v rozvodnicích, veřejných telefonních budkách nebo přímo na nadzemní/podzemní telefonní vedení, díky čemuž lze: (1) volat zadarmo kamkoliv, (2) surfovávat zadarmo po internetu a (3) odposlouchávat cizí telefonní hovory. Platba za hovor jde samozřejmě na účet oběti (registrovaného uživatele linky anebo telekomunikační společnosti). Za phreaking se považuje i nabourávání se různými metodami do mobilní sítě nebo výroba odposlouchávacích zařízení.

Denotation for tapping into a somebody else's telephone line in distribution panels, public telephone booths or directly in the ground/below ground telephone lines and thanks to these: (1) it is possible to call anywhere free of charge, (2) surf the internet free of charge, and (3) listen to somebody else's telephone conversations. Payment for the call is of course at the cost of the victim (registered user of the line, or the telephone company). Tapping into a mobile network by using various methods or the manufacture of listening devices is also considered phreaking.

Ping**Ping**

Nástroj používaný v počítačových sítích pro testování dosažitelnosti počítače nebo cílové sítě přes IP sítě. Ping měří čas návratu odezvy a zaznamenává objem ztracených dat (packets).

Instrument used in computer networks for testing computer availability over IP networks. Ping measures the time of response and records the volume of lost data (packets).

Ping of death**Ping of death**

Typ útoku na počítač, který zahrnuje chybně odeslaný **ICMP** paket nebo jinak nebezpečný paket, např. odesílání IP paketu většího než maximální velikost IP paketu, který zhroutí cílový počítač nebo odesláním paketu docílí překročení maximální velikosti **IP** paketů, což způsobí selhání systému.

Type of an attack on a computer which includes an ICMP packe sent in error or an otherwise dangerous packet, e.g. a packet sent larger than the maximum size of IP packet which collapses the target computer, or, by sending the packet the attacker exceeds the maximum size of IP packets which results in a failure of the system.

Plán kontinuity činností**Business continuity plan**

Dokumentovaný soubor postupů a informací, který je vytvořen sestaven a udržován v pohotovosti pro užití při incidentu za účelem umožnění organizaci uskutečňovat své kritické činnosti na přijatelné, předem stanovené úrovni.

Documented set of procedures and information which is made up and maintained in readiness for use during an incident in order to enable an organization to implement its critical activities at an acceptable and previously set level.

Plán obnovy / Havarijní plán**Disaster recovery plan / Contingency plan**

Plán pro záložní postupy, odezvu na nepředvídanou událost a obnovu po havárii.

Plan for backup procedures, response to an unforeseen event and recovery after a contingency.

Plán řízení rizik**Risk management plan**

Schéma v rámci managementu rizik specifikující přístup, dílčí části managementu a zdroje, které se mají použít k managementu rizik.

Scheme in the framework of risks specifying access, parts of management and sources to be used for risk management.

Počítačová / Kybernetická šikana**Cyberbullying**

Druh šikany, který využívá elektronické prostředky, jako jsou mobilní telefony, e-maily, pagery, internet, blogy a podobně k zasílání obtěžujících, urážejících či útočných mailů a SMS, vytváření stránek a blogů dehonestujících vybrané jedince nebo skupiny lidí.

Type of bullying using electronic means such as mobile phones, emails, pagers, internet, blogs and similar for sending harassing, offending or attacking mails and SMSs, creation of pages and blogs defaming selected individuals or groups of people.

Počítačová bezpečnost**Computer security (COMPUSEC)**

Obor informatiky, který se zabývá zabezpečením informací v počítačích (odhalení a zmenšení rizik spojených s používáním počítače). Počítačová bezpečnost zahrnuje: (1) zabezpečení ochrany před neoprávněným manipulováním se zařízeními počítačového systému, (2) ochranu před neoprávněnou manipulací s daty, (3) ochranu informací před krádeží (nelegální tvorba kopí dat) nebo poškozením, (4) bezpečnou komunikaci a přenos dat (kryptografie), (5) bezpečné uložení dat, (6) dostupnost, celistvost a nepodvrhnutelnost dat. Je to také zavedení bezpečnostních vlastností hardwaru, firmwaru a softwaru do počítačového systému, aby byl chráněn proti neoprávněnému vyzrazení, úpravě, změnám nebo vymazání skutečností nebo aby jim bylo zabráněno nebo proti odmítnutí přístupu. Ochrana dat a zdrojů před náhodnými nebo škodlivými činnostmi.

Branch of informatics dealing with securing of information in computers

(discovering and lowering risks connected to the use of the computer). Computer security includes: (1) enabling protection against unauthorized manipulation with the devices of a computer system, (2) protection against unauthorized data manipulation, (3) protection of information against pilferage (illegal creation of data copies), (4) secure communication and data transfer (cryptography), (5) secure data storage, (6) availability, integrity and authenticity of data. It is also the introduction of security properties of hardware, firmware and software into the computer system so that it is protected against unauthorized disclosure, amendments, changes or erasure of facts or to prevent these, or against access denial. Protection of data and sources against accidental or harmful activities.

**Počítačová kriminalita /
Kybernetická kriminalita**

Computer crime / Cyber crime

Zločin spáchaný pomocí systému zpracování dat nebo počítačové sítě nebo přímo s nimi spojený.

Crime committed using a data processing system or computer network or directly related to them.

Počítačová síť

Computer network

Soubor počítačů spolu s komunikační infrastrukturou (komunikační linky, technické vybavení, programové vybavení a konfigurační údaje), jejímž prostřednictvím si (počítače) mohou vzájemně posílat a sdílet data.

Aggregate of computers together with the communication infrastructure (communication lines, hardware, software and configuration data) using which the computers can send and share data.

Počítačové obtěžování

Cyber-harassment

Internetové obtěžování (i jednotlivý případ), zpravidla obecnější či vulgární povahy. Často bývá součástí cyberstalkingu. Více také *Cyberstalking*.

Internet harassment (even an individual case) usually of an obscene or vulgar character. It is often part of cyberstalking. See also Cyberstalking.

Počítačový podvod

Computer fraud

Podvod spáchaný pomocí systému zpracování dat nebo počítačové sítě nebo přímo s nimi spojený.

Fraud committed using a data processing system or computer network or directly related to them.

Počítačový virus

Computer virus

Počítačový program, který se replikuje připojováním své kopie k jiným programům. Může obsahovat část, která ho aktivuje, pokud dojde ke splnění některých podmínek (např. čas) v hostitelském zařízení. Šíří se prostřednictvím

Internetu (elektronická pošta, stahování programů z nespolehlivých zdrojů), pomocí přenosných paměťových médií apod. Toto dělá za účelem získání různých typů dat, zcizení identity, znefunkční počítače, atd.

Computer programme which replicates itself by attaching its copies to other programmes. It may contain a part which activates it when certain conditions are met (e.g. time) in the host device. It is distributed using the Internet (electronic mail, downloading programmes from unreliable sources), using mobile storage media and others. This is done in order to obtain various types of data, for identity theft, for putting the computer out of operation, etc.

Podrobná inspekce paketů (DPI)

Deep packet inspection (DPI)

Forma filtrování paketů v počítačové síti, která prohlíží datovou část (a možná také hlavičku) paketu při průchodu inspekčním bodem, a hledá nesoulad s protokolem, viry, spam, průniky nebo také definovaná kriteria pro rozhodnutí, zda paket může projít či zda je nutné přesměrování na jiné místo určení, nebo za účelem sběru statistických informací.

A form of computer network packet filtering that examines the data part (and possibly also the header) of a packet as it passes an inspection point, searching for protocol non-compliance, viruses, spam, intrusions, or defined criteria to decide whether the packet may pass or if it needs to be routed to a different destination, or, for the purpose of collecting statistical information.

Podstoupení rizik

Risk retention

Přijetí břemene ztráty nebo prospěchu ze zisku vyplývajícího z určitého rizika.

Accepting the burden of a loss or benefit from profit ensuing from a certain risk.

Podvržení IP adresy

IP spoofing

Podvržení zdrojové IP adresy u zařízení (počítače), které iniciuje spojení (s příjemcem) za účelem zatajení skutečného odesilatele. Tato technika bývá využívána především v útocích typu **DoS**.

Substitution of a spurious IP address on a device (a computer) which triggers connection (with a recipient) in order to hide the real sender. This technique is used particularly in attacks of DoS type.

Pokročilá a trvalá hrozba (APT)

Advanced persistent threat (APT)

Typickým účelem APT je dlouhodobé a vytrvalé infiltraci a zneužívání cílového systému za pomoci pokročilých a adaptivních technik (na rozdíl od běžných jednorázových útoků).

Typical purpose of APT is a long-term and persistent infiltration into, and abuse of, the target system using advanced and adaptive techniques (unlike usual single attacks).

Politika řízení přístupu

Soubor zásad a pravidel, která definují podmínky pro poskytnutí přístupu k určitému objektu.

Set of principles and rules which define conditions to provide an access to a certain object.

Politika řízení rizik

Prohlášení o celkových záměrech a směrování organizace týkající se řízení rizik.

Statement on the overall intentions and direction of an organization related to risk management.

Poplašná zpráva

Snaží se svým obsahem vyvolat dojem důvěryhodnosti. Informuje např. o šíření virů nebo útočí na sociální cítění adresáta. Může obsahovat škodlivý kód nebo odkaz na internetové stránky se škodlivým obsahem.

It tries to create an impression of trustworthiness by its content. It informs, for example, about the spread of viruses or it inveighs against the social feeling of the addressee. It may contain harmful code or a link to internet pages with harmful content.

Port

Používá se při komunikaci pomocí protokolů **TCP** či **UDP**. Definuje jednotlivé síťové aplikace běžící v rámci jednoho počítače. Může nabývat hodnot v rozmezí 0 – 65535. Například webové stránky jsou obvykle dostupné na portu 80, server pro odesílání mailové pošty na portu 25, ftp server na portu 21. Tyto hodnoty je možné změnit a u některých síťových služeb správci někdy záměrně nastavují jiná než běžně používaná čísla portů kvůli zmatení případného útočníka.

It is used for communication using the TCP or UDP protocols. It defines the individual net applications running on one computer. It may take on values in the range 0 – 65535. For example, web pages are usually accessible on port 80, server to send out electronic mail on port 25, ftp server on port 21. These values may be changed and with some network services the administrators sometimes set other than normally used port numbers in order to deceive a potential attacker.

Port scanner

Program na testování otevřených portů.

Programme to test open ports.

Access control policy**Risk management policy****Hoax****Port****Port scanner**

Portál

Informace (obsahové oblasti, stránky, aplikace, data z vnějších zdrojů) soustředěná v jednom ústředním místě, ke kterým je přístup prostřednictvím webového prohlížeče.

Information (content regions, pages, applications, and data from external sources) concentrated in one central place which can be accessed using a web browser.

Portál veřejné správy

Informační systém vytvořený a provozovaný se záměrem usnadnit veřejnosti dálkový přístup k pro ni potřebným informacím z veřejné správy a komunikaci s ním.

Information system created and operated with the intention of facilitating remote access to, and communication with, the necessary information from the public administration.

Poskytovatel služby

Každá fyzická nebo právnická osoba, která poskytuje některou ze služeb informační společnosti.

Any natural or legal person providing some of the services of the information society.

Poskytovatel služeb internetu

Organizace, která nabízí přístup k internetu svým zákazníkům.

Organization offering access to internet to its customers.

Postoj k riziku

Přístup organizace k posuzování rizika a případně zabývání se rizikem, k spoluúčasti, převzetí nebo odmítání rizika.

Approach of an organization towards assessing risk and, also, dealing with risk, sharing risk, taking over or refusal of risk.

Postup

Specifikovaný způsob provádění činnosti nebo procesu.

Specified manner of executing an activity or process.

Posuzování rizika**Risk assessment**

Celkový proces identifikace rizik, analýzy rizik a hodnocení rizik

Overall process of risk identification, risk analysis and risk assessment.

Poškození dat**Data corruption**

Náhodné nebo záměrné narušení integrity dat.

Accidental or intentional corruption of data integrity.

Povolení přístupu**Access permission**

Všechna přístupová práva subjektu vzhledem k určitému objektu.

All access rights of a subject related to a certain object.

Požadavky na službu**Service requirement**

Potřeby zákazníka a uživatelů služby včetně požadavků na úroveň služby a potřeby poskytovatele služby.

Needs of customers and users of services, including requirements for the service level and the needs of a service provider.

Pracovní stanice**Workstation**

Funkční jednotka, obvykle se specifickými výpočetními schopnostmi, která obsahuje uživatelské vstupní a výstupní jednotky, např. programovatelný terminál nebo samostatný počítač.

Functional unit, usually with specific computing capabilities, having user input and output devices, e.g. a programmable terminal or a stand-alone computer.

Pravděpodobnost, možnost výskytu**Likelihood**

Možnost, že něco nastane.

Possibility that something occurs.

Pretexting**Pretexting**

Jeden z druhů sociálního inženýrství. Jedná se o vytváření a využívání smyšleného scénáře, s cílem přesvědčit oběť k učinění potřebné akce, či k získání potřebné informace. Jedná se o skloubení lži s jinou pravdivou informací, získanou dříve.

One kind of social engineering. It creates and uses fictitious screenplay with the objective of convincing the victim to perform the required action, or to obtain the required information.

Privátní IP adresa**Private IP address**

Skupiny **IP** adres definované v RFC 1918 jako vyhrazené pro použití ve vnitřních sítích. Tyto IP adresy nejsou směrovatelné z internetu. Jedná se o následující rozsahy: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255 a 192.168.0.0 – 192.168.255.255.

Groups of IP addresses defined under RFC 1918 as reserved for use in internal networks. These IP addresses are not routed from the internet. Here are these ranges: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255 and 192.168.0.0 – 192.168.255.255.

Problém**Problem**

Primární příčina jednoho nebo více incidentů.

Primary cause of one or more incidents.

Proces**Process**

Soubor vzájemně souvisejících nebo vzájemně působících činností, které přeměňují vstupy na výstupy.

Set of mutually related or mutually influencing activities transforming inputs into outputs/

Proces řízení rizik**Risk management process**

Systematické uplatňování manažerských politik, postupů a zavedené praxe u činností sdělování, konzultování, stanovení kontextu, a zjišťování, analyzování, hodnocení, ošetřování, monitorování a přezkoumávání rizik.

Systematic implementation of management policies, procedures and well-established practices for the activities of sharing, consulting, context setting, and finding out, analyzing, evaluating, treating, monitoring and cross-checking risks.

Profil rizik**Risk profile**

Popis jakéhokoliv souboru rizik.

Description of any set of risks.

Program**Program**

Syntaktická jednotka vyhovující pravidlům určitého programovacího jazyka; skládá se z popisů (deklarací) a příkazů nebo instrukcí nutných pro splnění určité funkce či vyřešení určité úlohy nebo problému.

Syntactic unit satisfying the rules of a certain programming language; it consists of descriptions (declarations) and commands or instructions necessary

to fulfil some function or solve some task or problem.

Prohlášení o aplikovatelnosti**Statement of applicability**

Dokumentované prohlášení popisující cíle opatření a opatření, které jsou relevantní a aplikovatelné na ISMS dané organizace.

Documented statement describing the objectives of measures and the measures which are relevant and applicable for the ISMS of a given organization.

Prohlášení o úrovni služeb**Service level declaration (SLD)**

Specifikace nabízených služeb, která se může měnit na základě individuálních dohod podle aktuálních potřeb jednotlivých uživatelů. Jedná se tedy o podrobnější SLA. Více **SLA**.

*Specification of offered services which can change on the basis of individual agreements according to the actual needs of individual customers. Hence, a more detailed SLA. See **SLA**.*

Projekt ISMS**ISMS project**

Strukturované činnosti, které provádí organizace při zavedení ISMS.

Structured activities executed by an organization during the ISMS introduction.

Prolamovač hesel**Password cracker**

Program určený k luštění hesel, a to buď metodou **Brute force attack** nebo **Dictionary attack**.

*Programme designed to crack passwords either by the **Brute force attack** or **Dictionary attack**.*

Prolomení**Breach**

Neoprávněné proniknutí do systému.

Illegal breach into a system.

Proniknutí / průnik**Penetration**

Neautorizovaný přístup k počítačovému systému, síti nebo službě.

Unauthorized access to a computer system, network or service.

Prostředky Informační války**Information warfare**

Integrované využití všech vojenských možností, které zahrnuje zajištění informační bezpečnosti, klamání, psychologické operace, elektronický boj a ničení. Podílejí se na něm všechny druhy průzkumu, komunikační

a informační systémy. Cílem informační války je bránit informačnímu toku, ovlivňovat a snižovat účinnost nebo likvidovat systém velení a řízení protivníka a současně chránit vlastní systémy velení a řízení před podobnými akcemi ze strany protivníka.

Integrated use of all military capabilities including information security, deception, psychological operations, electronic warfare and destruction. All forms of reconnaissance, communication and information systems contribute to it. The objective of information warfare is to put obstacles in the flow of information, influence and decrease efficiency or liquidate 'the system of command and control of the adversary, and at the same time to protect own systems of command and control from similar actions of the adversary.

**Prostředky pro zpracování
informací**

Jakýkoliv systém, služba nebo infrastruktura, zpracovávající informace anebo lokality, ve kterých jsou umístěny.

Any system, service or infrastructure processing information, or the localities of their placement.

Protiopatření

Information processing facilities

Činnost, zařízení, postup, technika určena k minimalizaci zranitelnosti.

Activity, equipment, procedure, technology intended to minimize vulnerability.

Protokol

Protocol

Úmluva nebo standard, který řídí nebo umožňuje připojení, komunikaci, a datový přenos mezi počítači, obecně koncovými zařízeními. Protokoly mohou být realizovány hardwarem, softwarem, nebo kombinací obou.

Agreement or standard which controls or enables a link, communication and data transfer among computers, in general among end devices. Protocols can be implemented by hardware, software, or a combination of both.

Protokol ARP

Address resolution protocol (ARP)

Protokol definovaný v dokumentu RFC 826 umožňuje převod síťových adres (**IP**) na hardwarové (**MAC**) adresy. ARP neužívá autentizaci, takže ho lze zneužít k útokům např. typu MITM.

*Protocol defined in the document RFC 826 enables the translation of network addresses (**IP**) to hardware (**MAC**) addresses. ARP does not use authentication hence it cannot be misused for attacks, e.g. of the MITM type.*

Provozní dokumentace

Operational documentation

Dokumentace informačního systému veřejné správy, která popisuje funkční a technické vlastnosti informačního systému.

Documentation of the information system of public administration describing the functional and technological features of the information system.

Provozovatel informačního systému veřejné správy **Operator of the information system of public administration.**

Subjekt, který provádí alespoň některé informační činnosti související s informačním systémem. Provozováním informačního systému veřejné správy může správce pověřit jiné subjekty, pokud to jiný zákon nevylučuje.

Subject performing at least some of the activities related to the information system. The administrator of the information system of public administration can commission other subjects unless prohibited by a law.

Proxy trojan

Maskuje ostatní počítače jako infikované počítače. Umožňuje útočníkovi zneužít napadený počítač pro přístup k dalším počítačům v síti, čímž pomáhá útočníkovi skrýt jeho skutečnou identitu.

Masks other computers as infected. Enables the attacker to abuse the infected computer for an access to other computers in the network and thus aids the attacker to hide its identity.

Průlezová kritéria

Soubor hledisek pro posuzování závažnosti vlivu narušení funkce prvků kritické infrastruktury s mezními hodnotami, které zahrnují rozsah ztrát na životě, dopad na zdraví osob, mimořádně vážný ekonomický dopad nebo dopad na veřejnost v důsledku rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života.

Set of viewpoints to assess how serious is the corruption of an element in the critical infrastructure with bounds which include the scope of life losses, impact on the health of people, extraordinary serious economic impact or impact on the public due to an extensive limitation of providing the necessary services or any other serious intervention into the daily life.

Prvek kritické infrastruktury

Element of the critical infrastructure

Zejména stavba, zařízení, prostředek nebo veřejná infrastruktura, určené podle průlezových a odvětvových kritérií; je-li prvek kritické infrastruktury součástí evropské kritické infrastruktury, považuje se za prvek evropské kritické infrastruktury.

Building, equipment, device or public infrastructure in particular, determined using the cross-criteria and sector criteria; if the element in the critical infrastructure is a part of the European critical infrastructure, it is considered to be an element of the European critical infrastructure.

Prvek služby

Samostatný celek služby, který, když se spojí s dalšími celky, zajišťuje dodávku celé služby.

Independent component of a service which, when united with other components provides the whole service.

Předčasně ukončené spojení

Spojení ukončené dříve nebo jiným způsobem, než je předepsáno. Často může umožnit neoprávněným entitám neautorizovaný přístup.

Connection terminated earlier, or in another way, than prescribed. It can often provide unauthorized access to unauthorized persons.

Přechod

Činnosti týkající se přesunutí nové nebo změněné služby do či z provozní prostředí.

Activity related to a shift of new or altered service into or out of the operational environment.

Překlad sítiových adres**Network address translation (NAT)**

Mechanismus umožňující přístup více počítačů z lokální sítě do Internetu pod jedinou veřejnou IP adresou. Počítače z lokální sítě mají přiděleny tzv. privátní IP adresy. Hraniční prvek takové lokální sítě zajišťuje překlad privátních IP adres na veřejnou. Více také **Private IP address**.

*Mechanism enabling access of several computers from a local network to the Internet under one public IP address. Computers from the local address are assigned so-called private IP addresses. The border element of such a local network provides for the translation of a private IP address to a public one. See also **Private IP address**.*

Přenos rizik**Risk transfer**

Sdílení nákladů ze ztrát s jinou stranou nebo sdílení prospěchu ze zisku vyplývajícího z rizika.

Sharing of costs with another party or sharing of benefits from profit flowing from risk.

Přesměrováče**Re-dial, Pharming crime ware**

Programy (podmnožina Malware), jejichž úkolem je přesměrovat uživatele na určité stránky namísto těch, které původně hodlal navštívit. Na takových stránkách dochází k instalaci dalšího Crimeware (víru), nebo touto cestou dojde ke značnému zvýšení poplatku za připojení k Internetu (prostřednictvím telefonních linek se zvýšeným tarifem).

Programmes (subset of Malware) whose task is to redirect users to certain pages instead of those originally intended to be visited. On these pages there is an installation of other Crimeware (virus), or there is a substantial increase in the Internet connection fee (using telephone lines with a higher rate).

Přezkoumání**Review**

Činnost vykonávaná k určení vhodnosti, přiměřenosti a efektivnosti předmětu zkoumání k dosažení stanovených cílů.

Activity done in order to assess the suitability, adequacy and efficiency of the analyzed subject to achieve set objectives.

Přijetí rizika**Risk acceptance**

Rozhodnutí přijmout riziko.

Decision to accept risk.

Příklad dobré praxe, osvědčený způsob**Best practice**

Vyzkoušená metoda nebo postup, která v dané oblasti nabízí nejefektivnější řešení, které se opakovaně osvědčilo a vede k optimálním výsledkům.

Well-tested method or procedure which in the given area offers the most effective solution which has been repeatedly proven as right and leads towards optimum results.

Přístupové právo**Access right**

Povolení pro subjekt přistupovat ke konkrétnímu objektu pro specifický typ operace.

Permission for a subject to access a concrete object for a specific type of operation.

Rámec řízení rizik**Risk management framework**

Soubor prvků poskytujících základy a organizační uspořádání pro navrhování, implementování, monitorování, přezkoumávání a neustálé zlepšování managementu rizik v celé organizaci.

Set of components providing the fundamentals and organizational arrangement for the design, implementation, monitoring, re-analysis and continuous improvement of risk management in the whole organization.

Ransomware**Ransom ware**

Program, který zašifruje data a nabízí jejich rozšifrování po zaplacení výkupného (např. virus, trojský kůň).

Programme which encrypts data and offers to decrypt them after a ransom payment (e.g. a virus, Trojan horse).

Redukce rizik**Risk reduction**

Činnosti ke snížení pravděpodobnosti, negativních následků nebo obou těchto parametrů spojených s rizikem.

Activity to lower the probability and lessen negative consequences, or both of these parameters linked to risk.

Redundance**Redundancy**

Obecný význam je nadbytečnost, hojnost. V **IT** se používá ve smyslu záložní. Například redundantní (záložní) zdroj napájení, redundantní (záložní) data.

General meaning is redundancy, abundance. In IT it is used in the sense of backup. For example, a redundant (backup) power supply, redundant (backup) data.

Regionální Internetový Registr**Regional internet registry (RIR)**

Organizace starající se o přidělování rozsahů veřejných IP adres, autonomních systémů v její geografické působnosti. V současnosti existuje pět RIRů: RIPE NCC – Evropa a blízký východ, ARIN – USA a Kanada, APNIC – Asijsko-pacifická oblast, LACNIC – Latinská Amerika, AfriNIC – Afrika.

Organization looking after the assignment of public IP address ranges, autonomous systems in its geographical scope. There are five RIRs at present: RIPE NCC – Europe and Near East, ARIN – USA and Canada, APNIC – Asia – Pacific Region, LACNIC – Latin America, AfriNIC – Africa.

Regist doménových jmen**Domain name registry**

Databáze všech doménových jmen, která jsou zapsána v rozšíření domény nejvyššího řádu nebo druhé nejvyšší domény.

A database of all domain names registered in a top-level domain or second-level domain extension.

Rekonstrukce dat**Data reconstruction**

Metoda obnovy dat analyzováním původních zdrojů.

Method of data reconstruction by analyzing the original sources.

Replay, replay útok**Replay, replay attack**

Situace, kdy je zachycená kopie legitimní transakce (datová sekvence), opětovně přehrána neautorizovaným subjektem, a to zpravidla s nelegálním úmyslem (např. pro otevření vozidla s centrálním zamykáním).

Situation when a copy of a legitimate transaction (data sequence) is intercepted, repeatedly replayed by an unauthorized subject usually with illegal intent (e.g. to open a car with a central lock).

Request For Comment (RFC)

Používá se pro označení řady standardů popisujících Internetové protokoly, systémy a další věci související s fungováním internetu. Například RFC 5321 popisuje protokol **SMTP** pro výměnu a zpracování elektronické pošty.

It is used to denote standards describing internet protocols, systems and other items related to internet operation. For example, RFC 5321 describes the SMTP protocol for the exchange and processing of electronic mail.

Riziko

(1) Nebezpečí, možnost škody, ztráty, nezdaru. (2) Účinek nejistoty na dosažení cílů. (3) Možnost, že určitá hrozba využije zranitelnosti aktiva nebo skupiny aktiv a způsobí organizaci škodu.

(1) Danger, possibility of damage, loss, failure. (2) Effect of uncertainty to achieve objectives. (3) Possibility that a certain threat would utilize vulnerability of an asset or group of assets and cause damage to an organization.

Riziko bezpečnosti informací

Souhrn možností, že hrozba využije zranitelnost aktiva nebo skupiny aktiv a tím způsobí organizaci škodu.

Aggregate of possibilities that a threat would utilize the vulnerability of an asset or group of assets and thus cause damage to an organization.

Role

Souhrn určených činností a potřebných autorizací pro subjekt působící v informačním systému nebo komunikačním systému.

Aggregate of specified activities and necessary authorizations for a subject operating in the information or communication system.

Rootkit

Programy umožňující maskovat přítomnost zákeřného software v počítači. Dokáží tak před uživatelem skrýt vybrané běžící procesy, soubory na disku, či další systémové údaje. Existují pro Windows, LINUX i UNIX.

Programmes making it possible for insidious software to mask its presence in a computer. Thus they can hide from the user selected running processes, files on disc or other system data. They exist for Windows, LINUX and UNIX.

Rovný s rovným**Peer to peer (P2P)**

Jedná se o počítačovou síť, kde spolu přímo komunikují jednotliví klienti. Tento model se dnes využívá především u výměnných sítí. S rostoucím množstvím uživatelů totiž u tohoto modelu roste celková přenosová kapacita. Zatímco u klasického modelu klient-server je tomu přesně naopak.

This is a computer network where individual clients communicate directly. This model is primarily used in interchangeable networks. Total transmission capability grows as a rule with the growing number of users in this model. In the classic model client-server this is quite the reverse.

Rozhraní**Interface**

Místo a způsob propojení systémů nebo jejich částí.

Location and mode of interconnecting systems or their parts.

Řetězový dopis**Chain letter**

Dopis odeslaný mnoha adresátům a obsahující informaci, kterou má každý příjemce předat mnoha dalším adresátům. Často využívá nátlaku („Pokud tento dopis do 3 dnů nepošleš 25 dalším osobám, do 10 dnů tě potká něco hrozného.“).

Letter sent out to many recipients and containing information which each recipient has to pass on to many other addressees. It is a frequently used method of pressure ("If you do not send this letter to 25 other people, something terrible happens to you in 25 days").

Řízení bezpečnostních incidentů**Information security incident management**

Procesy pro detekci, hlášení a posuzování bezpečnostních incidentů, odezvu na bezpečnostní incidenty, zacházení a poučení se z bezpečnostních incidentů.

Processes for detection, reporting and assessing of security incidents, response to security incidents, handling and learning from security incidents.

Řízení kontinuity organizace**Business continuity management (BCM)**

Holistický manažerský proces, který identifikuje možné hrozby a jejich potenciální dopady na chod organizace a který poskytuje rámec pro prohlubování odolnosti organizace tím, že rozšiřuje její schopnosti efektivně reagovat na krizové události a tím chránit zájmy svých klíčových partnerů a zákazníků, svoji pověst, značku a svoje činnosti.

Holistic management model which identifies possible threats and their potential impact on the operations of an organization and which provides a framework for deepening the immunity of an organization by expanding its capabilities to respond effectively to emergency events and thus protect the interests of its key partners and customers, its reputation and its activities.

Řízení přístupu**Access control**

Znamená zajistění, že přístup k aktivu je autorizován a omezen na základě obchodních (podnikatelských) a bezpečnostních požadavků.

Making sure that access to an asset is authorized and limited on the basis of business (entrepreneurial) and security requirements.

Řízení rizik**Risk management**

Koordinované činnosti pro vedení a řízení organizace s ohledem na rizika.

Coordinated activities to manage and control an organization in view of the risks.

Řízení služeb**Service management**

Množina schopností a procesů pro vedení a řízení činností a zdrojů poskytovatele služeb pro návrh, přechod, dodávku a zlepšování služeb, aby byly naplněny požadavky služeb.

Set of capabilities and processes to manage and control the activities and sources of the service provider for the design, handover, delivery and improvement of services so that the requirements placed on them be met.

Řízení zranitelností**Vulnerability management**

Cyklická praxe pro identifikaci, třídění, opakování zprostředkování a zmírňování zranitelností. Obecně se tato praxe vztahuje na zranitelnosti programového vybavení v počítačových systémech, může však být často rozšířena na organizační chování a strategické rozhodovací procesy.

Cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities. This practice generally refers to software vulnerabilities in computing systems however it can also extend to organizational behavior and strategic decision-making processes.

Sandbox**Sandbox**

Bezpečnostní mechanismus sloužící k oddělení běžících procesů od samotného operačního systému. Používá se například při testování podezřelého softwaru.

Security mechanism serving to separate running processes from the operating system proper. It is used, for example, in testing suspicious software.

Sdílení**Sharing**

Možnost společně a současně se dělit o jeden nebo více zdrojů informací, paměti nebo zařízení.

Possibility to have a portion at the same time of one or more information sources, memory or devices.

Secure shell (SSH)**Secure shell (SSH)**

Protokol, který poskytuje bezpečný vzdálený login při použití nezabezpečené sítě.

A protocol that provides secure remote login utilising an insecure network.

Secure socket layer (SSL)

Protokol, respektive vrstva vložená mezi vrstvu transportní (např. **TCP/IP**) a aplikační (např. **HTTP**), která poskytuje zabezpečení komunikace šifrováním a autentizací komunikujících stran.

*Protocol or a layer inserted between the transport layer (e.g. **TCP/IP**) and the application layer (e.g. **HTTP**) which enables communication security by encryption and authentication of the communicating parties.*

Security software disabler

Zablokuje software pro zabezpečení **PC** (firewall, antivir).

*It blocks software to secure the **PC** (Firewall, Antivirus).*

Serverová farma

Skupina síťových serverů, které jsou používány k zefektivnění vnitřních procesů tím, že distribuují zátěž mezi jednotlivé zapojené složky, aby urychlily výpočetní procesy využitím síly více serverů. Když jeden server ve farmě selže, jiný může jeho služby nahradit.

Group of network servers used to increase the efficiency of internal processes by distributing load among individual linked components in order to speed up computing processes by using the power of more servers. When one server in the farm fails, another one can replace it.

Service set identifier (SSID)

Jedinečný identifikátor (název) každé bezdrátové (**WiFi**) počítačové sítě.

*Unique identifier (name) of every wireless (**WiFi**) computer network.*

Sexting

Elektronické rozesílání textových zpráv, fotografií či videí se sexuálním obsahem. Tyto materiály často vznikají v rámci partnerských vztahů. Takovéto materiály však mohou představovat riziko, že jeden partner z nejrůznějších pohnutek zveřejní fotografie či videa svého partnera.

Electronic distribution of text messages, photographies or videos with a sexual content. These materials often originate in partner relations. Such materials, however, may represent a risk that one partner, out of various motives, would publish photographies or videos of the other partner.

Secure socket layer (SSL)**Server cluster****Service set identifier (SSID)****Sexting**

Seznam pro řízení přístupu (ACL) Access control list (ACL)

Seznam oprávnění připojený k nějakému objektu (např. diskovému souboru); určuje, kdo nebo co má povolení přistupovat k objektu a jaké operace s ním může provádět. U bezpečnostního modelu používajícího ACL systém před provedením každé operace prohledá ACL a naleze v něm odpovídající záznam, podle kterého se rozhodne, zda operace smí být provedena.

List of authorizations attached to some subject (e.g. a disc file); it determines who or what has the right to access the object and which operations it can do with it. In the security model using the ACL system, it searches ACL prior to performing any operation and looks up the corresponding record and on the basis of it makes a decision if the operation may be executed.

Shareware

Volně distribuovaný software, který je chráněn autorskými právy. V případě že se uživatel rozhodne tento software využívat déle, než autor umožňuje, je uživatel povinen splnit podmínky pro používání. Může jít například o zaplacení určité finanční částky, registrace uživatele, atd.

Freely distributed software protected by copyright. In case the user decides to use this software longer than the author permits, the user is obliged to satisfy conditions for use. These can be, for example, payment of a certain financial amount, user registration, etc.

Schopnost pro reakci na počítačové hrozby (CIRC)

Schopnost reakce na počítačové incidenty. Je součástí kybernetické obrany a k tomu využívá opatření zejména v oblasti **INFOSEC**. Zajišťuje centralizovanou schopnost rychle a efektivně reagovat na rizika a zranitelnosti v systémech, poskytuje metodiku pro oznamování a zvládání incidentů, zajišťuje podporu a pomoc provozním a bezpečnostním správám systémů. Je součástí realizace havarijního (krizového) plánování pro případy obnovy systémů.

Capability of responding to computer incidents. It is part of cyber defence and uses in particular measures of INFOSEC. Ensures centralized capability for fast and effective reaction to risks and vulnerabilities in systems provides methodology for reporting and managing incidents provides support and help to the operational and security managements of systems. It is part of the emergency (crisis) planning for cases of system recovery.

Shareware**Computer incident response capability (CIRC)**

**Simple mail transfer protocol
(SMTP)**

Internetový protokol určený pro přenos zpráv elektronické pošty. Popisuje komunikaci mezi poštovními servery.

*Internet protocol for the transmission of messages of electronic mail.
It describes communication among mail servers.*

Simulace

Použití systému zpracování dat k vyjádření vybraných vlastností chování fyzického nebo abstraktního systému.

Use of a data processing system to extract selected properties in the behaviour of a physical or abstract system.

Sít'

Množina počítačových terminálů (pracovních stanic) a serverů, které jsou vzájemně propojeny, aby si navzájem vyměňovaly data a mohly spolu komunikovat.

Set of computer terminals (workstations) and servers which are mutually interconnected in order to exchange data and communicate.

Sít' elektronických komunikací

Přenosové systémy, popřípadě spojovací nebo směrovací zařízení a jiné prostředky, včetně prvků sítě, které nejsou aktivní, které umožňují přenos signálů po vedení, rádiovými, optickými nebo jinými elektromagnetickými prostředky, včetně družicových sítí, pevných sítí s komutací okruhů nebo paketů a mobilních zemských sítí, sítí pro rozvod elektrické energie v rozsahu, v jakém jsou používány pro přenos signálů, sítí pro rozhlasové a televizní vysílání a sítí kabelové televize, bez ohledu na druh přenášené informace.

Transmission systems, or as the case may be, communication and routing equipment and other devices, including elements of the network which are not active, which make for the transmission of signals over wire lines, by radio, optical or other electromagnetic devices, including satellite networks, fixed lines with commuted circuits or packets, and mobile ground networks, networks for the distribution of electrical energy in the extent to transmit signals, networks for radio and television broadcast and networks for cable television, regardless of the type of transmitted information.

Skript

Soubor instrukcí zapsaný v některém formálním jazyce, kterým je řízena činnost zařízení, programu či systému.

Set of instructions written in some formal language which control the workings of devices, programme or system.

**Simple mail transfer protocol
(SMTP)****Simulation****Network****Network of electronic
communications****Script**

Skrytý kanál

Přenosový kanál, který může být použít pro přenos dat způsobem, který narušuje bezpečnostní politiku.

Transmission channel which could be used for data transfer in a way impairing security policy.

Skupina pro reakce na počítačové bezpečnostní incidenty (CSIRT)

Tým odborníků na informační bezpečnost, jejichž úkolem je řešit bezpečnostní incidenty. CSIRT poskytuje svým klientům potřebné služby při řešení bezpečnostních incidentů a pomáhá jim při obnově systému po bezpečnostním incidentu. Aby snížily rizika incidentů a minimalizovaly jejich počet, pracoviště CSIRT poskytují svým klientům také preventivní a vzdělávací služby. Pro své klienty poskytují informace o odhalených slabinách používaných hardwarových a softwarových prostředků a o možných útocích, které těchto slabin využívají, aby klienti mohli dostatečně rychle osetřit odhalené slabiny.

Team of experts in information security whose task is to tackle security incidents. CSIRT provides its clients with the necessary services for solutions of security incidents and helps them in recovering the system after a security incident. In order to minimize incident risks and minimize their number, CSIRT offices provide also preventive and educational services. For clients, they provide information on detected weaknesses of used hardware and software instruments and about possible attacks which make use of these weaknesses so that the clients may quickly address these weaknesses.

Skupina pro reakci na počítačové hrozby (CERT)

CERT je jiný užívaný název pro CSIRT, na rozdíl od označení CSIRT je CERT registrovaná ochranná známka. Více CSIRT.

CERT is another name for CSIRT; unlike CSIRT, CERT is a registered trade mark. See CSIRT.

Slovníkový útok

Metoda zjišťování hesel, kdy crackovací program zkouší jako možné heslo všechna slova ve slovníku. Jedná se o metodu poměrně rychlou, záleží to na velikosti slovníku a na tom, zda oběť používá jednoduchá hesla.

Method for finding passwords when the cracking programme tries out all dictionary words in a dictionary for the password. This is a relatively fast method, depending on the size of the dictionary and whether the victim uses simple passwords.

Covert Channel**Computer security incident response team (CSIRT)****Computer emergency response team (CERT)****Dictionary attack**

Služba**Service**

Činnost informačního systému uspokojující dané požadavky oprávněného subjektu spojená s funkcí informačního systému.

Activity of the information system meeting the given requirements of an authorized subject related to the function of the operating system.

Služba elektronických komunikací Electronic communication service

Služba obvykle poskytovaná za úplatu, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací, včetně telekomunikačních služeb a přenosových služeb v sítích používaných pro rozhlasové a televizní vysílání a v sítích kabelové televize, s výjimkou služeb, které nabízejí obsah prostřednictvím sítí a služeb elektronických komunikací nebo vykonávají redakční dohled nad obsahem přenášeným sítěmi a poskytovaným službami elektronických komunikací; nezahrnuje služby informační společnosti, které nespočívají zcela nebo převážně v přenosu signálů po sítích elektronických komunikací.

Service usually provided for a fee which consists wholly or predominantly of signal transmission over electronic communication networks, including telecommunication services and transmission services in networks used for radio and television broadcast and networks for cable television, excluding services which provide content using the networks and services of electronic communications or have editing supervision of the content transmitted over the networks and provided services of electronic communications; it does not include services of the information society which do not rest wholly or predominantly on the transmission of signals over networks of electronic communications.

Služba informační společnosti**Information society service**

Jakákoliv služba poskytovaná elektronickými prostředky na individuální žádost uživatele podanou elektronickými prostředky, poskytovaná zpravidla za úplatu; služba je poskytnuta elektronickými prostředky, pokud je odeslána prostřednictvím sítě elektronických komunikací a vyzvednuta uživatelem z elektronického zařízení pro ukládání dat.

Any service provided by electronic means at the individual request of a user and put in by electronic means, usually provided for a fee. The service is provided by electronic means if it is sent by means of an electronic communication network and picked up by the user from electronic equipment for data storage.

Směrnice**Guideline**

(Závazné) doporučení toho, co se očekává, že má být provedeno, aby byl dosažen určitý cíl.

(Binding) recommendation of what is expected to be done in order to achieve a certain target.

Sniffer

Program umožňující odposlouchávání všech protokolů, které počítač přijímá / odesílá (používá se např. pro odposlouchávání přístupových jmen a hesel, čísel kreditních karet).

Programme for the eavesdropping of all the protocols which a computer receives/sends (it is used, for example, for eavesdropping of access names or passwords, numbers of credit cards).

Sociální inženýrství

Způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace.

Way of people manipulation in order to perform a certain action or to obtain a certain information.

Sociální síť

Propojená skupina lidí, kteří se navzájem ovlivňují. Tvoří se na základě zájmů, rodinných vazeb nebo z jiných důvodů. Tento pojem se dnes také často používá ve spojení s internetem a nástupem webů, které se na vytváření sociálních sítí přímo zaměřují (Facebook, Lidé.cz apod.), sociální síť se mohou vytvářet také v zájmových komunitách kolem určitých webů, například na jejich fórech.

Interconnected group of people who interact. It is formed on the basis of interests, family ties or other reasons. This idea is at present often used in connection with internet and the onset of webs which are directly targeted at social networks (Facebook, Lidé.cz etc.), social networks can also form in interest communities around certain web sites, for example at their forums.

Software (programové vybavení)

Sada programů používaných v počítači, které vykonávají zpracování dat, či konkrétních úloh. Software lze dále rozdělit na: a) systémový software – vstupně/výstupní systémy, operační systémy nebo grafické operační systémy; b) aplikační software – aplikace, jednoduché utility nebo komplexní programové systémy; c) firmware – ovládací program hardwaru.

Set of programmes used in a computer which execute data processing or a concrete task. Software can be further subdivided into: a) system software – input/output devices, operating systems or graphics operation systems; b) application software – applications, simple utilities or complex programming systems; c) firmware – hardware control programme.

Sniffer**Social engineering****Social network****Software**

Software veřejné domény

Software, který je umístěn do veřejné domény, jinými slovy neexistuje vůbec žádné vlastnictví, jako například autorské právo, obchodní značka či patent.

Software that has been placed in the public domain, in other words there is absolutely no ownership such as copyright, trademark, or patent.

Softwarové pirátství

Neautorizované používání, kopírování nebo distribuce programového vybavení.

Unauthorized use, copying or distribution of software.

Soubor

Obecná pojmenovaná množina dat. Může se jednat o dokument, multimediální data, databázi či prakticky jakýkoli jiný obsah, který je pro uživatele nebo software užitečné mít permanentně přístupný pod konkrétním jménem.

General named set of data. It can be a document, multimedia data, database or practically any other content, which the user or software may find useful to have permanently available under a concrete name.

Soubor logů

Soubor obsahující informace o aktivitách subjektů v systému, přístup k tomuto souboru je řízen.

File containing information on the activities of subjects in the system, access to this file is controlled.

Souborový systém**File system**

Způsob organizace a uložení dat ve formě souborů tak, aby k nim bylo možné snadno přistupovat. Souborové systémy jsou uloženy na vhodném typu elektronické paměti, která může být umístěna přímo v počítači (pevný disk) nebo může být zpřístupněna pomocí počítačové sítě.

Method of organization and storage of data in the form of files so that access to them would be easy. File systems are stored on a suitable type of electronic memory which can be located directly in the computer (hard disc) or can be made accessible using a computer network.

Soukromí**Privacy**

Soukromí je schopnost nebo právo jednotlivce nebo skupiny zadržovat informace o sobě. Soukromí je rovněž hmotný nebo myšlenkový prostor subjektu.

Privacy is the capability or right of an individual or group to retain information about themselves. Privacy is also the material or mental space of the subject.

Spear phishing (rybaření oštěpem) Spear phishing

Sofistikovanější útok typu **Phishing**, který využívá předem získané informace o oběti. Díky většímu zacílení na konkrétní uživatele dosahuje tato metoda většího účinku než běžný útok typu **Phishing**. Více **Phishing**.

More sophisticated attack than Phishing, which uses prior obtained information about the victim. Thanks to a more focused targeting on a concrete user this method attains higher effect than a standard attack of the Phishing type. See Phishing.

Spojování / Fúze**Linkage / Fusion**

Účelná kombinace dat nebo informací z jednoho systému zpracování dat s daty nebo informacemi z jiného systému tak, aby bylo možné odvolat chráněnou informaci.

Useful combination of data or information from one data processing system, with data or information from another system, so as to declassify protected information.

Spolehlivost**Reliability**

Vlastnost konzistentního zamýšleného chování nebo výsledků.

Attribute of consistent intentional behaviour or results.

**Správce aktiva (provozovatel
informačního systému)****Assets (information system)
Operator**

Jedinec (entita), který zabezpečuje zpracování informací nebo poskytování služeb a vystupuje vůči ostatním fyzickým a právnickým osobám v informačním systému jako nositel práv a povinností spojených s provozováním systému.

Individual (entity) who enables information processing or service providing and acts towards other natural and legal persons in the information system as the bearer of rights and obligations connected to operating the system.

**Správce informačního systému
veřejné správy****Operator of the information system
of public administration.**

Subjekt, který podle zákona určuje účel a prostředky zpracování informací a za informační systém odpovídá.

Subject who by law determines the objective and means for information processing and is responsible for the information system.

Správce systému**System administrator**

Osoba zodpovědná za řízení a údržbu počítačového systému.

Person responsible for the management and maintenance of a computer system.

Správce zabezpečení účtů**Security account manager**

Správce zabezpečení účtů v operačním systému Windows, např. databáze, ve které se uchovávají hesla uživatelů (hesla v operačním systému Windows NT se nacházejí např. v adresáři c:\winnt\repair a c:\winnt\config).

Administrator for securing the accounts in the Windows operating system, e.g. a database, where user passwords are kept (passwords in Windows NT operating system may be kept, for example, in the directory c:\winnt\repair and c:\winnt\config).

Spyware**Spyware**

Program skrytě monitorující chování oprávněného uživatele počítače nebo systému. Svá zjištění tyto programy průběžně (např. při každém spuštění) zasílají subjektu, který program vytvořil, respektive distribuoval. Takové programy jsou často na cílový počítač nainstalovány spolu s jiným programem (utilita, počítačová hra), s jehož funkcí však nesouvisí.

Programme which secretly monitors the behaviour of an authorized computer or system user. The findings are sent by these programmes continuously (e.g. at every startup) to the subject which created the programme or distributed it. Such programmes are frequently installed on the target computer together with another programme (utility, computer game), however, they bear no relation to it.

SQL injection**SQL injection**

Injekční technika, která zneužívá bezpečnostní chyby vyskytující se v databázové vrstvě aplikace. Tato chyba zabezpečení se projevuje infiltrací neoprávněných znaků do SQL příkazu oprávněného uživatele nebo převzetím uživatelského přístupu k vykonání SQL příkazu.

Injection technique which abuses security errors occurring in the database layer of an application. This security error manifests itself by infiltrating unauthorized characters into an SQL command of an authorized user, or by taking over user access, to execute the SQL command.

Stanovení kontextu**Establishing the context**

Vymezení vnějších a vnitřních parametrů, které mají být zohledněny při managementu rizik a nastavení rozsahu platnosti a kritérií rizik pro politiku managementu rizik.

Establishing the limits of external and internal parameters to be taken into account during risk management and setting of the risk validity ranges and risk criteria for the risk management policy.

Stav kybernetického nebezpečí**State of cyber danger**

Stavem kybernetického nebezpečí se rozumí stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb nebo sítí elektronických komunikací.

Under cyber danger we understand such a state when there is a large measure of danger to information security in information systems or security of services or of electronic communications.

Structured query language (SQL)**Structured query language (SQL)**

Standardizovaný dotazovací jazyk používaný pro práci s daty v relačních databázích.

Standard query language used to work with data in relational databases.

Stuxnet**Stuxnet**

Počítačový červ, který je vytvořen, aby útočil na průmyslové řídící systémy typu **SCADA**, jenž je využíván k řízení velkých průmyslových podniků, například továren, elektráren, produktovodů a dokonce armádních zařízení.

Computer worm created to attack industrial control systems of the SCADA type used to control large industrial enterprises, for example factories, power generating plants, product lines and even military objects.

Subjekt**Subject**

V počítačové bezpečnosti aktivní entita, která může přistupovat k objektům.

In computer security, an active entity which can access objects.

Subjekt kritické infrastruktury**Subject of critical infrastructure**

Provozovatel prvku kritické infrastruktury; jde-li o provozovatele prvku evropské kritické infrastruktury, považuje se tento za subjekt evropské kritické infrastruktury.

Operator of an element of critical infrastructure; if it is an operator of an element of the European critical infrastructure, the operator is considered to be a subject of the European critical infrastructure.

SYN-cookies**SYN-cookies**

Prvek obrany proti útoku zaplavením pakety protokolu **TCP** s příznakem **SYN**. Více **SYN Flood**.

Element of defence against a flooding by packets in the TCP protocol with the attribute SYN. See SYN-Flood.

SYN-flood

Kybernetický útok (typu Denial of Service) na server zaplavením pakety protokolu TCP. Útočník zasílá záplavu TCP/SYN paketů s padělanou hlavičkou odesílatele. Každý takový paket server přijme jako normální žádost o připojení. Server tedy odešle paket SYN-ACK a čeká na paket ACK. Ten ale nikdy nedorazí, protože hlavička odesílatele byla zfalšována. Takto polootevřená žádost nějakou dobu blokuje jiné, legitimní žádosti o připojení. Více **DoS**, **DDoS**, **SYN-cookie**.

*Cyber attack (Denial of Service type) on a server by flooding with packets in the TCP protocol. The attacker sends a flood of TCP/SYN packets with a forged heading of the sender. The server accepts every such packet as a normal request for a connection. Server then sends out the SYN-ACK packet and waits for the ACK packet. This however never arrives as the heading of the sender was forged. Such a semi-open request blocks out, for some time, other legitimate requests for a connection. See **DoS**, **DDoS**, **SYN-cookie**.*

Systém detekce průniku (IDS)**Intrusion detection system (IDS)**

Technický systém, který se používá pro zjištění, že byl učiněn pokus o průnik nebo takový čin nastal, a je-li to možné, pro reakci na průnik do informačních systémů a sítí.

Technical system that is used to identify that an intrusion has been attempted, is occurring, or has occurred and possibly respond to intrusions in information systems and networks.

Systém doménových jmen (DNS)**Domain name system (DNS)**

Distribuovaný hierarchický jmenný systém používaný v síti Internet. Překládá názvy domén na číselné **IP** adresy a zpět, obsahuje informace o tom, které stroje poskytují příslušnou službu (např. přijímají elektronickou poštu či zobrazují obsah webových prezentací).

*Distributed hierarchical name system used on the Internet network. It translates domain names into numerical **IP** addresses and back, contains information about which machines provide the relevant service (e.g. accepts electronic mail or show the content of web pages).*

Systém prevence průniku (IPS)**Intrusion prevention system (IPS)**

Varianta systémů detekce průniku, které jsou zvláště určeny pro možnost aktivní reakce.

Variant on intrusion detection systems that are specifically designed to provide an active response capability.

Systém řízeného přístupu

Prostředky pro automatizaci fyzického řízení přístupu (např. použití odznaků vybavených magnetickými proužky, inteligentních karet, biometrických snímačů).

Means for automating of the physical control of access (e.g. use of badges equipped with magnetic strips, smart cards, biometric sensors).

Systém řízení

Rámec politik, postupů, směrnic a přidružených zdrojů k dosažení cílů organizace.

Framework of policies, procedures, directives and affiliated sources to achieve the objectives of an organization.

Systém řízení bezpečnosti informací (SRBI)

Část systému řízení, založená na přístupu k bezpečnostním rizikům, k ustavení, implementování, provozování, monitorování, přezkoumávání, spravování a zlepšování bezpečnosti informací.

Part of the management system, based on the attitude towards security risks, definition, implementation, operation, monitoring, re-analysing, administration and improvement of information security.

Systém řízení kontinuity organizace**Business continuity management system (BCMS)**

Část celkového systému řízení organizace, která ustanovuje, zavádí, provozuje, monitoruje, přezkoumává, udržuje a zlepšuje kontinuitu fungování organizace.

Part of the overall system of managing an organization which defines, introduces, operates, monitors, re-analyses, maintains and improves operating continuity of an organization.

Šifrování**Encryption**

Kryptografická transformace dat, také nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí.

Cryptographic transformation of data, also the science about methods of hiding the meaning of messages by a transformation into a form which is readable with special knowledge only.

Škodlivý software**Malware – malicious software**

Je obecný název pro škodlivé programy. Mezi škodlivý software patří počítačové viry, trojské koně, červy, špiónažní software.

This is the general name for harmful programmes. Harmful software includes computer viruses, Trojan horses, worms, spyware.

Špatně utvořený dotaz

(1) Chybný dotaz, který může vyvolat nestandardní nebo neočekávané chování systému. (2) Způsob útoku.

(1) Erroneous query which may result in triggering a nonstandard or unexpected behaviour of a system. (2) Mode of an attack.

Tajná vrátká / Přístup ke službám **Maintenance hook**

Zadní vrátká v softwaru, která umožňují snadné udržování a přidání dalších charakteristik a která mohou umožnit vstup do programu v neobvyklých místech nebo bez obvyklých kontrol.

Loophole in software which enables easy maintenance and addition of other characteristics and which can enable an access to a programme in unusual locations or without the usual checks.

Technické prostředky (vybavení) **Hardware**

Fyzické součásti systému (zařízení) nebo jejich část (např. počítač, tiskárna, periferní zařízení).

Physical components of a system (equipment) or their parts (e.g. a computer, printer, peripheral devices).

Telefonní phishing **Phone phishing**

Tato technika využívá falešného hlasového automatu (Interactive Voice Response) s podobnou strukturou jako má originální bankovní automat ("Pro změnu hesla stiskněte 1, pro spojení s bankovním poradcem stiskněte 2"). Oběť je většinou vyzvána emailem k zavolání do banky za účelem ověření informace. Zde je pak požadováno přihlášení za pomocí PIN nebo hesla. Některé automaty následně přenesou oběť do kontaktu s útočníkem vystupujícím v roli telefonního bankovního poradce, což mu umožňuje další možnosti otázek.

This technique uses a false voice automaton (Interactive Voice Response) with a structure similar to the original banking automaton ("For a change of password press 1, for connection to a bank advisor press 2"). The victim is usually asked in an email to call the bank for information verification. Here, sign-on is requested using a PIN or a password. Some automata subsequently transfer the victim to a contact with the attacker playing the role of a telephone bank advisor which allows for other possibilities for questions.

TERENA**TERENA**

Trans-European Research and Education Networking Association, evropská mezinárodní organizace podporující aktivity v oblasti internetu, infrastruktur a služeb v rámci akademické komunity.

Trans-European Research and Education Networking Association, a European international organization supporting activities in the area of internet,

infrastructures and services in the academic community.

TF-CSIRT

Mezinárodní fórum umožňující spolupráci týmů **CSIRT** na evropské úrovni. Dělí se na dvě skupiny – uzavřenou, která je přístupná pouze akreditovaným týmům, a otevřenou, která je přístupná všem zájemcům o práci týmů **CSIRT**. TF-CSIRT je jednou z aktivit mezinárodní organizace **TERENA**. Pracovní skupina TF-CSIRT se schází obvykle několikrát ročně.

International forum enabling the cooperation of CSIRT teams on a European level. It is divided into two groups – a closed one which is open only to accredited teams, and an open one which is accessible to all parties interested in the CSIRT teams' work. TF-CSIRT is one of the activities of the TERENA international organization. Working group TF-CSIRT meets usually several times per year.

Torrent

Jedná se o soubor s koncovkou .torrent, který obsahuje informace o jednom nebo více souborech ke stažení. Více **BitTorrent**.

This is a file with the ending .torrent which contains information about one or more files to be downloaded. See BitTorrent.

Transmission control protocol (TCP)

Je jedním ze základních protokolů sady protokolů Internetu, konkrétně představuje transportní vrstvu. Použitím TCP mohou aplikace na počítačích propojených do sítě vytvořit mezi sebou spojení, přes které mohou přenášet data. Protokol garanteuje spolehlivé doručování a doručování ve správném pořadí. TCP také rozlišuje data pro vícenásobné, současně běžící aplikace (například webový server a emailový server) běžící na stejném počítači. TCP podporuje mnoho na internetu populárních aplikačních protokolů a aplikací, včetně **WWW**, emailu a **SSH**.

It is one of the basic protocols in the protocol set of the Internet; more precisely it represents the transport layer. Using the TCP, applications on interconnected computers can link up and transmit data over the links. The protocol guarantees a reliable delivery as well as delivery in the right order. TCP also differentiates data for multiple concurrently running applications (e.g. a web server and email server) running on the same computer. TCP is supported by many of the application protocols and applications popular on the internet, including WWW, email and SSH.

TF-CSIRT

Mezinárodní fórum umožňující spolupráci týmů **CSIRT** na evropské úrovni. Dělí se na dvě skupiny – uzavřenou, která je přístupná pouze akreditovaným týmům, a otevřenou, která je přístupná všem zájemcům o práci týmů **CSIRT**. TF-CSIRT je jednou z aktivit mezinárodní organizace **TERENA**. Pracovní skupina TF-CSIRT se schází obvykle několikrát ročně.

International forum enabling the cooperation of CSIRT teams on a European level. It is divided into two groups – a closed one which is open only to accredited teams, and an open one which is accessible to all parties interested in the CSIRT teams' work. TF-CSIRT is one of the activities of the TERENA international organization. Working group TF-CSIRT meets usually several times per year.

Torrent

Jedná se o soubor s koncovkou .torrent, který obsahuje informace o jednom nebo více souborech ke stažení. Více **BitTorrent**.

This is a file with the ending .torrent which contains information about one or more files to be downloaded. See BitTorrent.

Transmission control protocol (TCP)

Je jedním ze základních protokolů sady protokolů Internetu, konkrétně představuje transportní vrstvu. Použitím TCP mohou aplikace na počítačích propojených do sítě vytvořit mezi sebou spojení, přes které mohou přenášet data. Protokol garanteuje spolehlivé doručování a doručování ve správném pořadí. TCP také rozlišuje data pro vícenásobné, současně běžící aplikace (například webový server a emailový server) běžící na stejném počítači. TCP podporuje mnoho na internetu populárních aplikačních protokolů a aplikací, včetně **WWW**, emailu a **SSH**.

It is one of the basic protocols in the protocol set of the Internet; more precisely it represents the transport layer. Using the TCP, applications on interconnected computers can link up and transmit data over the links. The protocol guarantees a reliable delivery as well as delivery in the right order. TCP also differentiates data for multiple concurrently running applications (e.g. a web server and email server) running on the same computer. TCP is supported by many of the application protocols and applications popular on the internet, including WWW, email and SSH.

Transport layer security

Kryptografický protokol, který poskytuje komunikační bezpečnost pro Internet. Používá se asymetrické šifrování pro výměnu klíčů, symetrické šifrování pro důvěrnost a kody pro ověřování celistvosti zpráv. Široce se používá několik verzí těchto protokolů v aplikacích jako prohlížení na webu, elektronická pošta, faxování přes internet, instantní zprávy and voice-over-IP (**VoIP**).

A cryptographic protocol that provide communication security over the Internet. They use asymmetric cryptography for authentication of key exchange, symmetric encryption for confidentiality and message authentication codes for message integrity. Several versions of the protocols are in widespread use in applications such as web browsing, electronic mail, Internet faxing, instant messaging and voice-over-IP (VoIP).

Trojský kůň

Program, který plní na první pohled nějakou užitečnou funkci, ale ve skutečnosti má ještě nějakou skrytou škodlivou funkci. Trojský kůň se sám nereplikuje, šíří se díky viditelně užitné funkci, kterou poskytuje.

Programme which executes a useful function, taken at face value, but in reality has also some hidden harmful function. Trojan horse does not self-replicate, it is distributed thanks to the visible utility it provides.

Trusted introducer

Úřad, který sjednocuje evropské bezpečnostní týmy typu **CERT / CSIRT**. Zároveň také napomáhá vzniku **CERT / CSIRT** týmů a provádí jejich akreditace a certifikace. Je provozován organizací **TERENA**. Více **TERENA**.

Authority uniting European security teams of the type CERT/CSIRT. At the same time it also helps in creating the CERT/CSIRT teams and provides for their accreditation and certification. It is operated by the TERENA organization. See TERENA.

Třetí strana

Osoba nebo organizace nezávislá jak na osobě nebo organizaci, která poskytuje předmět posuzování shody (produkt, služba), tak i na odběrateli tohoto předmětu.

Person or organization independent both of the person or the organization which submits the object to be judged for compliance (product, service) and also independent of the purchaser of the object.

Typ přístupu

V počítačové bezpečnosti typ operace, specifikované přístupovým právem.

Transport layer security (TLS)**Trojan horse****Trusted introducer****Third party****Access type**

In computer security, type of an operation specified by an access right.

Účelnost**Efficiency**

Vztah mezi dosaženými výsledky a tím, jak správně byly zdroje využity.

Relation between the achieved results and how well have the sources been used.

Údaje**Data**

Z pohledu **ICT** reprezentace informací formalizovaným způsobem vhodným pro komunikaci, výklad a zpracování.

From the ICT point of view, this is a representation of information in a formalized way suitable for communication, explanation and processing.

Událost**Event**

Výskyt nebo změna určité množiny okolností.

Occurrence or change of a certain set of circumstances.

Úmyslné oklamání, podvržení**Spoofing**

Činnost s cílem podvést (oklamat) uživatele nebo provozovatele zpravidla pomocí předstírání falešné identity.

Activity with the objective of deceiving (misleading) a user or operator usually by sporting a false identity.

Uniform resource locator (URL)**Uniform resource locator (URL)**

Zdrojový identifikátor, který popisuje umístění konkrétního zdroje, včetně protokolu, sloužící k načítání tohoto zdroje. Nejznámějším příkladem URL je např. <http://www.nejakadomena.nekde>.

Source identifier describing the location of a concrete source, including a protocol, serving to link to this source. The best known such an example is <http://www.somedomain.somewhere>.

Universální unikátní identifikátor**Universal unique identifier (UUID)**

Standard pro identifikátory používaná při tvorbě softwaru, standardizovaný organizací Open Software Foundation (**OSF**) jako součást Distributed Computing Environment (**DCE**).

*An identifier standard used in software construction, standardized by the Open Software Foundation (**OSF**) as part of the Distributed Computing Environment (**DCE**).*

URL trojan

Přesměrovává infikované počítače připojené přes vytáčené připojení k Internetu na dražší tarify. Více hesla **Dialer a Trojan Horse**.

*It redirects infected computers connected via the dial-in Internet connection to more expensive rates. See **Dialer** and **Trojan Horse**.*

Úroveň přístupu

Úroveň autorizace požadovaná pro přístup k chráněným zdrojům.

Level of authorization required to access protected sources.

Úroveň rizika**Level of risk / risk level**

Velikost rizika vyjádřená jako kombinace následků a jejich možnosti výskytu.

Magnitude of risk expressed as the combination of consequences and the possibility of their occurrence.

**Úřad pro přidělování čísel na
Internetu (IANA)****Internet assigned numbers
authority (IANA)**

Autorita, která dohliží na přidělování **IP adres**, správu kořenových zón **DNS** (přidělování **TLD** domén a vznik generických domén) a správu a vývoj internetových protokolů. V současné době je **IANA** jedním z oddělení organizace **ICANN**.

*Authority overseeing **IP address** assignment, administration of **DNS** zones (assignment of **TLD** domains and the creation of generic domains) and the administration and development of internet protocols. At present, **IANA** is one of the departments of the **ICANN** organization.*

User datagram protocol (UDP)**User datagram protocol (UDP)**

Internetový síťový protokol pro nespojovou komunikaci (RFC 768).

An Internet networking protocol for connectionless communications (RFC 768).

Útok**Attack**

Pokus o zničení, vystavení hrozby, nežádoucí změnu, vyřazení z činnosti, zcizení nebo získání neautorizovaného přístupu k aktivu nebo uskutečnění neautorizovaného použití aktiva.

Attempt at destruction, exposure to a threat, unwanted change, putting out of operation, stealing or obtaining an unauthorized access to an asset or execution of an unauthorized use of an asset.

Útok na počítačovou síť**Computer network attack (CNA)**

Činnost realizovaná za účelem narušit, blokovat, znehodnotit nebo zničit informace uložené v počítači anebo na počítačové síti, či počítač anebo počítačovou síť samotnou. Útok na počítačové síti je určitým druhem kybernetického útoku.

Activity done in order to corrupt, block, degrade or destroy information stored in a computer or on a computer network, or the computer or computer network as such. Attack on a computer network is a certain sort of cyber attack.

Útok s použitím hrubé sily**Brute force attack**

Metoda k zjišťování hesel, kdy útočící program zkouší jako možné heslo všechny existující kombinace znaků, dokud nezjistí skutečné heslo. Tento způsob je časově velmi náročný. Jeho úspěšnost je závislá na délce hesla, složitosti hesla a na výpočetním výkonu použitého počítače.

Method to find passwords when the attacking programme tries all existing character combinations for a possible password. This method is very time-consuming. Its success depends on password length and the computing power of the used computer.

Uvolnění**Release**

Soubor jedné nebo více nových či změněných konfiguračních položek, které jsou nasazovány do provozního prostředí jako výsledek jedné nebo více změn.

Aggregate of one or more new or changed configuration items which are put into the operational environment as the result of one or more changes.

Uzavřené bezpečnostní prostředí**Closed-security environment**

Prostředí, ve kterém je věnována zvláštní pozornost (formou autorizací, bezpečnostních prověření, řízení konfigurace atd.) ochraně dat a zdrojů před náhodnými nebo úmyslnými činy.

Environment where special attention (by a form of authorizations, security checks, configuration control, etc.) is given to protection of data and sources from accidental or intentional actions.

Uživatel**User**

Každá fyzická nebo právnická osoba, která využívá službu informační společnosti, zejména za účelem vyhledávání či zpřístupňování informací.

Any natural or legal person using a service of the information society in order to look for, or make access to, information.

Uživatelský profil**User profile**

Popis uživatele, typicky používaný pro řízení přístupu. Může zahrnovat data jako ID uživatele, jméno uživatele, heslo, přístupová práva a další atributy.

Description of a user typically used for access control. It may include data such as user ID, user name, password, access rights and other attributes.

Validace dat

Proces používaný k určení, zda data jsou přesná, úplná nebo splňují specifikovaná kritéria. Validace dat může obsahovat kontroly formátu, kontroly úplnosti, kontrolní klíčové testy, logické a limitní kontroly.

Process used to determine if data are accurate, complete, or satisfy specified criteria. Data validation may contain checks of format, checks for completeness, control key tests, logical and limit checks.

Validace identity

Vykonání testů umožňujících systému na základě zpracování dat rozpoznat a ověřit entity.

Execution of tests enabling a system to recognize and validate entities on the basis of data processing.

Velikonoční vajíčko

Skrytá a oficiálně nedokumentovaná funkce nebo vlastnost počítačového programu, DVD nebo CD. Většinou se jedná pouze o neškodné hríčky a vtípky, grafické symboly, animace, titulky se jmény tvůrců apod. Tato skrytá funkce se nevyvolává obvyklým způsobem (menu, tlačítka apod.), ale netradiční kombinací běžných uživatelských činností, stiskem myši na nějakém neobvyklém místě, zvláštní posloupností stisku konkrétních kláves apod. Často bývají vajíčka skryta v obrazovce „O programu“ („About“), kde se dají zobrazit např. po poklepání na různé části tohoto panelu s podržením klávesy ALT apod.

Hidden and officially undocumented function or property of a computer programme, DVD or CD. Mostly these are puns and jokes doing no harm, graphics symbols, animations, subtitles with authors' names and similar. This hidden function is not activated in the usual way (menu, key, etc.) but by an unorthodox combination of the usual user activities, pushing a mouse key on an unusual place, special sequence of keys, and so on. Often, eggs are hidden on the screen under "About" where these can be displayed by tapping on various parts of this panel while holding the key ALT and similar.

Veřejná IP adresa

IP adresa, která je směrovatelná v **Internetu**. Takováto IP adresa je tedy dostupná z celé sítě **Internetu**, pokud tomu nebrání například konfigurace **firewallu** či routeru.

*IP address which is routable in the Internet. Such an address is then accessible from the whole **Internet** network unless prohibited for example by **firewall** or router configuration.*

Data validation**Identity validation****Easter egg****Public IP address**

Veřejná komunikační síť**Public telecommunication network**

Síť elektronických komunikací, která slouží zcela nebo převážně k poskytování veřejně dostupných služeb elektronických komunikací, a která podporuje přenos informací mezi koncovými body sítě, nebo síť elektronických komunikací, jejímž prostřednictvím je poskytovaná služba šíření rozhlasového a televizního vysílání.

Network of electronic communications serving wholly or predominantly to provide publicly available services of electronic communications and which supports information transfer among the endpoints of the network, or a network of electronic communications through which radio and television broadcast are provided as a service.

Veřejná telefonní síť**Public telephone network**

Síť elektronických komunikací, která slouží k poskytování veřejně dostupných telefonních služeb a která umožnuje mezi koncovými body sítě přenos mluvené řeči, jakož i jiných forem komunikace, jako je faksimilní a datový přenos.

Network of electronic communications to provide publicly available telephone services and which allows for the transmission of voiced speech as well as other forms of communications, such as facsimiles and data transmissions, among the endpoints of the networks.

Veřejně dostupná služba elektronických komunikací**Publicly available electronic communications service**

Služba elektronických komunikací, z jejíhož využívání není nikdo předem vyloučen.

Service of electronic communications from whose use no one may be a priori excluded.

Veřejný informační systém**Public information system**

Informační systém poskytující služby veřejnosti, který má vazby na informační systémy veřejné správy.

Information system providing services to the public and having relations to information system of the public administration.

Virtuální lokální síť**Virtual local area network (VLAN)**

Logicky nezávislá síť v rámci jednoho nebo více zařízení. Virtuální sítě lze definovat jako domény všesměrového vysílání (Více LAN) s cílem učinit logickou organizaci sítě nezávislou na fyzické vrstvě.

Logically independent network in the framework of one or more devices. Virtual networks can be defined as the domains of all-directional broadcast (See LAN) with the objective of making the logical network organization independent of the physical network.

Virtuální privátní síť

Jedná se o privátní počítačovou síť, která dovolí připojit vzdálené uživatele do cílené *LAN* přes *Internet*. Bezpečnost se řeší pomocí šifrovaného tunelu mezi dvěma body (nebo jedním a několika). Při navazování spojení je totožnost obou stran ověřována pomocí digitálních certifikátů.

This is a private computer network allowing for the connection of remote users to the targetet LAN via the Internet. Security is tackled using an encrypted tunnel between two points (or among one and several points). Identity of both parties is verified using digital certificates when making the connection.

Virus

Typ malware, který se šíří z počítače na počítač tím, že se připojí k jiným aplikacím. Následně může působit nežádoucí a nebezpečnou činnost. Má v sobě obvykle zabudován mechanismus dalšího šíření či mutací.

Type of malware spreading from one computer to another by attaching itself to other applications. Consequently it may cause unwanted and dangerous activity. Usually it has a built-in mechanism for further distribution or mutations.

Vlastník aktiva

Je myšlen jedinec, nebo entita, který má vedením organizace přidělenou odpovědnost za výrobu, vývoj, údržbu, použití a bezpečnost aktiva.

This is assumed to be an individual or entity whom the organization management has assigned the responsibility for production, development, maintenance, use and security of an asset.

Vlastník rizika

Osoba nebo entita s odpovědností a pravomocí řídit riziko a sledovat události, které dané riziko vyvolávají.

Person or entity with the responsibility and authority to control risk and monitor events which cause the risk.

Vnější kontext

Vnější prostředí, ve kterém se organizace snaží dosáhnout svých cílů.

External environment where an organization strives to achieve its objectives.

Vnitřní kontext

Vnitřní prostředí, ve kterém se organizace snaží dosáhnout svých cílů.

Internal environment where an organization strives to achieve its objectives.

Virtual private network (VPN)**Virus****Asset owner****Risk owner****External context****Internal context**

Vnitřní, interní skupina**Internal group**

Část organizace poskytovatele služeb, která uzavřela dokumentovanou dohodu s poskytovatelem služeb o svém podílu na návrhu, přechodu, dodávce a zlepšování služby nebo služeb.

Part of an organization of a service provider which has concluded a documented contract with the service provider about its share in the design, handover, delivery and improvement of a service or services.

Vrcholové vedení**Top management**

Osoba nebo skupina osob, která na nejvyšší úrovni vede a řídí organizaci.

Person or a group of persons who lead the organization at the highest level.

Vstup přes autorizovaného uživatele**Piggyback entry**

Neautorizovaný přístup k systému prostřednictvím legitimního spojení autorizovaného uživatele.

Unauthorized access to the system using a legitimate link of an authorized user.

Vyčištění**Clearing**

Cílené přepsání nebo vymazání klasifikovaných dat na datovém mediu, které má speciální bezpečnostní klasifikaci a bezpečnostní kategorii, takže dané medium může být opakovaně použito pro zápis ve stejně bezpečnostní klasifikaci a bezpečnostní kategorii.

Targeted overwriting or erasure of classified data on a data medium which has a special security classification and security category so that the given medium could be repeatedly used for a record in the same security classification and security category.

Vyhnutí se riziku**Risk avoidance**

Rozhodnutí nedopustit zapojení se do rizikových situací, nebo je vyloučit.

Decision not to allow an involvement into risk situations, or to exclude these.

Výchozí stav konfigurace**Configuration baseline**

Konfigurační informace formálně se vztahující k určitému času během života služby nebo prvku služby.

Configuration information formally related to a certain time in the lifetime of a service, or element of the service.

Vystavení hrozbám

Možnost, že konkrétní útok využije specifickou zranitelnost systému zpracování dat.

Possibility that a concrete attack would use a specific vulnerability of a data processing system.

Vytěžování počítačové sítě

Zneužití informací uložených na počítači nebo v počítačové síti.

Abuse of information stored on the computer or computer network.

Využití návnady

Způsob útoku, kdy útočník nechá infikované CD, flashdisk nebo jiné paměťové médium na místě, kde jej oběť s velkou pravděpodobností nalezne, např. ve výtahu, na parkovišti. Poté již nechá pracovat zvědavost, se kterou oběť dříve či později vloží toto médium do svého počítače. Tím dojde k instalaci viru, za pomoci kterého získá útočník přístup k počítači nebo celé firemní počítačové sítě.

Mode of attack when the attacker leaves an infected CD, flashdisc or another storage medium where the victim can find it with a high probability, e.g. in a lift, on the car park. This leaves curiosity to play out and sooner or later the victim inserts the medium into the computer. This results in virus installation with which the attacker gets an access to the computer or the whole companywide computer network.

Wardriving

Vyhledávání nezabezpečených bezdrátových Wi-Fi sítí osobou jedoucí v dopravním prostředku, pomocí notebooku, PDA nebo smartphonem.

Searching for insecure wireless Wi-Fi networks by a person sitting in a means of transport, using a notebook, PDA or smartphone.

Warez

Termín počítačového slangu označující autorská díla, se kterými je nakládáno v rozporu s autorským právem. Podle druhu bývá někdy warez rozdělován na gamez (počítačové hry), appz (aplikace), crackz (cracky) a také moviez (filmy). Nejčastějším způsobem šíření warezu je dnes hlavně **Internet**.

*Term from the computer slang denoting copyright-protected creations which are treated in violation of the copyright. Warez is sometimes split into gamez (computer games), appz (applications), crackz (cracks) and also moviez (films). Today, the most frequent way of distribution is mainly the **Internet**.*

Exposure**Computer network exploitation
(CNE)****Baiting****Wardriving****Warez**

Webový vandalizmus

Útok, který pozmění (zohyzdí) webové stránky nebo způsobí odmítnutí služby (denial-of-service attacks).

Attack which alters (defaces) web pages or causes a service denial (denial-of-service attacks).

White hat

Etičký hacker, který je často zaměstnáván jako expert počítačové bezpečnosti, programátor nebo správce sítí. Specializuje se na penetrační testy a jiné testovací metodiky k zajištění IT bezpečnosti v organizaci.

Ethical hacker who is often employed as an expert in computer security, programmer or network administrator. He or she specializes on penetration tests and other testing methodologies to ensure IT security in an organization.

Whois

Internetová služba, která slouží pro zjišťování kontaktních údajů majitelů internetových domén a IP adres.

Internet service to find contact data of the owners of internet domains and IP addresses.

WiFi

Bezdrátová technologie pro šíření dat („vzduchem“), vhodná pro tvorbu sítových infrastruktur tam, kde je výstavba klasické kabelové sítě nemožná, obtížná nebo nerentabilní (kulturní památky, sportoviště, veletrhy). Pro přenos dat postačí vhodně umístěné navazující přístupové body, lemuječí cestu od vysílače k příjemci.

Wireless technology for data distribution ("by air"), suitable for the creation of network infrastructures in places where the building of a classical cable network is impossible, difficult or not cost-effective (cultural monuments, sports facilities, fair grounds). Suitably located successive points of access along the route from the transmitter to the recipient are sufficient for data transmission.

WiMax

Telekomunikační technologie, která poskytuje bezdrátový přenos dat pomocí nejrůznějších přenosových režimů, od point-to-multipoint spojení pro přenos a plně mobilní internetový přístup.

Telecommunication technology providing wireless data transmission using various transmission modes, from point-to-multipoint to completely mobile internet access for the transmission.

Web vandalism**White hat****Whois****WiFi****WiMax**

Wireshark

Dříve **Ethereal**. Protokolový analyzer a paketový sniffer, který umožnuje odposlouchávání všech protokolů, které počítač přijímá / odesílá přes síťové rozhraní. Wireshark dokáže celý paket dekódovat a zobrazit tak, jak jej počítač odeslal. Jeho výhodou je, že je šířen pod svobodnou licencí **GNU / GPL**.

*Formerly **Ethereal**. Protocol analyzer and packet sniffer which enables eavesdropping of all protocols which the computer receives and sends via an interface. Wireshark can decode the whole packet and show it in a way as sent out by the computer. Its advantage is that it is distributed under a free licence **GNU/GPL**.*

World wide web (WWW)

Graficky orientovaná služba **Internetu** – systém vzájemně propojených hypertextových stránek využívajících formátovaný text, grafiku, animace a zvuky.

*Graphically-oriented service of the **Internet** – a system of interconnected hypertext pages using formatted text, graphics, animation and sounds.*

X.509

Standard pro systémy založené na veřejném klíči (**PKI**) pro jednoduché podepisování. X.509 specifikuje např. formát certifikátu, seznamy odvolaných certifikátů, parametry certifikátů a metody kontroly platnosti certifikátů.

*Standard for systems based on the public key (**PKI**) for simple signatures. X.509 specifies, for example, the format of a certificate, lists of cancelled certificates, parameters of certificates and methods for checking the validity of certificates.*

Zadní vrátka

Skrytý softwarový nebo hardwareový mechanizmus obvykle vytvořený pro testování a odstraňování chyb, který může být použít k obejít počítačové bezpečnosti. Metoda v počítačovém systému nebo v algoritmu, která útočníkovi umožnuje obejít běžnou autentizaci uživatele při vstupu do programu nebo systému a zároveň mu umožňuje zachovat tento přístup skrytý před běžnou kontrolou. Pro vniknutí do operačního systému mohou obejít **firewall** například tím, že se vydávají za webový prohlížeč. Tento kód může mít formu samostatně instalovaného programu nebo se jedná o modifikaci stávajícího systému. Samotný vstup do systému pak míval formu zadání fiktivního uživatelského jména a hesla, které napadený systém bez kontroly přijme a přidělí uživateli administrátorská práva.

Hidden software or hardware mechanism usually created for testing and error removal which can be used to bypass computer security. A method in a computer system or in an algorithm which allows the attacker to bypass the

Wireshark**World wide web (WWW)****X.509****Backdoor / trapdoor**

normal user authentication at the access to a programme or system and simultaneously allows to have this access hidden from normal checks. Firewall can be bypassed, in order to penetrate into the operating system, for example, by pretending to be a web browser. This code can assume the form of an independently installed programme or it could be a modification of an existing system. The access to the system as such tends to have the form of a fictitious user name and password which the attacked system accepts without checking and assigns to the user administrative rights.

Zahlcení pingy

Jednoduchý **DoS** útok, kdy útočník zaplaví oběť s požadavky „ICMP Echo Request“ (ping). Útok je úspěšný, pokud útočník má větší šířku pásma, než oběť, nebo může kooperovat s dalšími útočníky současně. Více ICMP flood.

Simple DoS attack when the attacker floods the victim with requests "ICMP Echo Request" (ping). The attack is successful provided the attacker has a wider bandwidth than the victim, or, the attacker can at the same time cooperate with other attackers. See ICMP flood.

Zahlcení TCP SYN

Typ útoku **DDoS**, zasílá záplavu **TCP/SYN** paketů s padělanou hlavičkou odesílatele. Každý takový paket je serverem přijat jako normální žádost o připojení. Server tedy odešle **TCP/SYN-ACK** packet a čeká na **TCP/ACK**. Ten ale nikdy nedorazí, protože hlavička odesílatele byla zfalšována. Tako polootevřená žádost nějakou dobu blokuje jiné, legitimní žádosti o připojení.

Type of a DDoS attack, it sends a flood of TCP/SYN packets with a forged heading of the sender. Each such packet is accepted by the server as a normal request for a connection. Server then sends out a TCP/SYN-ACK packet and waits for TCP/ACK. This however never arrives as the user heading was forged. Thus a half-open request blocks, for some time, other legitimate requests for a connection.

Zahlcení UDP

Je typ **DoS** útoku pomocí User datagram protocol (**UDP**). Útočník pošle nespecifikované množství UDP paketů na náhodný port systému oběti. Přijímací systém oběti není schopen určit, která aplikace si daný paket vyžádala, což vygeneruje ICMP paket nedoručitelnosti **UDP** paketu. Jestliže na přijímací port oběti přijde více UDP paketů, může dojít ke zkolaování systému.

This is a type of an attack using the User datagram protocol (UDP). The attacker sends out an unspecified number of packets to a random port of the system of the victim. Receiving system of the victim is unable to determine which application requested such a packet, which generates an ICMP packet of undeliverability of the UDP packet. If more UDP packets arrive in the receiving

Ping flood

TCP SYN flood

UDP flood

port of the victim, the system may collapse.

Zainteresovaná strana**Interested party**

Subjekt mající zájem na výkonnosti nebo úspěchu organizace.

Subject having an interest in the efficiency or success of an organization.

Zákazník**Customer**

Organizace nebo část organizace, která přijímá službu nebo služby.

Organization or its part receiving a service or services.

Základní prvky řízení**Baseline controls**

Minimální soubor ochranných opatření ustavených pro určitý systém nebo organizaci.

Minimal set of protective measures set for a certain system or organization.

Základní vstupně-výstupní systém**Basic input output system (BIOS)**

Programové vybavení, které se používá při startu počítače pro inicializaci a konfiguraci připojených hardwarových zařízení a následnému spuštění operačního systému.

Software used during the startup of a computer for initialization and configuration of connected hardware devices and subsequent start of the operating system.

Zálohovací procedura**Backup procedure**

Postup k zajištění rekonstrukce dat v případě selhání nebo havárie.

Procedure to enable data reconstruction in case of a failure or contingency.

Záložní soubor**Backup file**

Datový soubor, vytvořený za účelem pozdější možné rekonstrukce dat. Kopie dat uložená na jiném nosiči (nebo i místě). Záložní data jsou využívána v případě ztráty, poškození nebo jiné potřeby práce s daty uloženými v minulosti.

Data file created with the objective of a possible future data reconstruction. Copies of data stored on another carrier (or even in a different place). Backup data are used in case of a loss, corruption or any other need to work with data stored in the past.

Záplata

Aktualizace, která odstraňuje bezpečnostní problém nebo nestabilní chování aplikace, rozšiřuje její možnosti či zvyšuje její výkon.

Update which removes a security problem or unstable behaviour of an application expands its possibilities and enhances its performance.

Zaplavení, zahlcení

Náhodné nebo záměrné vložení velkého objemu dat, jehož výsledkem je odmítnutí služby.

Accidental or intentional insertion of a large volume of data resulting in a service denial.

Závada

Provozní nefunkčnost, vynechání, nebo přehlédnutí, která umožňuje, aby byly ochranné mechanizmy obejity nebo vyřazeny z činnosti.

Operational dysfunction, omission, or oversight making it possible to bypass protective mechanisms or put them out of action.

Záznam

Dokument, v němž jsou uvedeny dosažené výsledky nebo v němž se poskytují důkazy o provedených činnostech.

Document with the record of achieved results or in which proofs about completed activities are provided.

Zbytková data

Data zanechaná v datovém médiu po vymazání souboru nebo části souboru. Nemusí se však jednat pouze o data, která zbyla po mazání souborů na disku, nezádoucí zbytková data může zanechat na lokálním počítači například i práce pomocí vzdáleného připojení (VPN). Může se jednat například o nasbíraná (do cache) data aplikace.

Data left behind in a data medium after the erasure of a file or part of it. It need not be, however, only data left after the erasure of disc files, unwanted residual data can be left on the local computer, for example, even by work using a remote connection (VPN). It could be data collected (into a cache), for example, of an application.

Zbytkové riziko

Riziko, které zůstává i po aplikaci příslušných opatření.

Risk remaining even after an application of the appropriate measures.

Patch**Flooding****Flaw / loophole****Record****Residual data****Residual risk**

Zdroj rizika**Risk source**

Prvek, který sám nebo v kombinaci s jinými prvky má vnitřní potenciální schopnost způsobit riziko.

Element, which either alone or in combination with other elements, has the internal capability to cause a risk.

Zlovolná logika**Malicious logic**

Program, implementovaný v hardwaru, firmwaru nebo softwaru, jehož účelem je vykonat nějakou neautorizovanou nebo škodlivou akci (např. logická bomba, trojský kůň, virus, červ apod.).

Programme implemented in hardware, firmware or software whose purpose is to perform some unauthorized or harmful action (e.g. a logical bomb, Trojan horse, virus, worm, etc.).

Znalostní báze**Knowledge base**

Databáze obsahující inferenční pravidla a informace o zkušenostech a odborných znalostech v určité oblasti.

Database containing reference rules and information about the experience and professional knowledge in a certain area.

Známá chyba**Known error**

Problém, který má určenu primární příčinu nebo je pomocí náhradního řešení stanovena metoda pro snížení či odstranění dopadů problému na službu.

Problem whose primary cause is known, or for which a method is established, to decrease or remove the impact of the problems on a service, using a substitute solution.

Zneužití**Exploit**

(1) Chyba, nebo chyba v programu, software, příkazové sekvence nebo kód, který umožňuje uživateli používat programy, počítače nebo systémy neočekávaně nebo nepovoleným způsobem. (2) Také bezpečnostní díra, nebo případ s využitím bezpečnostní díry.

(1) Error, or an error in a programme, software, command sequence, or a code enabling a user to use programmes, computers or systems unexpectedly or in an unauthorized way. (2) Also a security hole or a case using a security hole.

Zneužití počítače**Computer abuse**

Záměrná nebo z nedbalosti plynoucí neautorizovaná činnost, která ovlivňuje počítačovou bezpečnost systému zpracování dat nebo je s ní spojena.

Unauthorized activity caused by intent or negligence which impacts computer security of a data processing system, or is related to it.

Zombie

Infikovaný počítač, který je součástí sítě botnetů.

Infected computer which is part of botnet networks.

Zranitelnost

Slabé místo aktiva nebo řízení, které může být využito hrozbou.

Weak spot of an asset or control which can be made use of by a threat.

Ztráta**Loss**

Kvantitativní míra škody nebo ztráty, které jsou následkem kompromitace.

Quantitative measure of damage or loss as a consequence of a compromise.

Zvládání bezpečnostních incidentů**Information security incident management**

Procesy pro detekci, hlášení a posuzování bezpečnostních incidentů, odezvu na bezpečnostní incidenty, zacházení a poučení se z bezpečnostních incidentů.

Processes for detection, reporting and assessing of security incidents, response to security incidents, handling and learning from security incidents.

Zvládání rizika, ošetření rizika**Risk treatment**

Proces pro modifikování (změnu) rizika.

Process to modify (change) a risk.

Žádost o službu**Service request**

Žádost o informace, radu, přístup ke službě nebo o předem dohodnutou změnu.

Request for information, advice, access to service, or for a previously agreed change.

Žádost o změnu**Request for change**

Návrh na provedení změny služby, prvku služby nebo systému řízení služeb.

Proposal to make a change of a service, element of a service or a system of service control.

Životní cyklus**Life cycle**

Soubor etap, jimiž prochází řešení systému od okamžiku zahájení vývoje až do ukončení životnosti nebo likvidace, včetně realizace změn.

Collection of stages through which a system transits from the moment of development beginning up to end of life or liquidation, including the implementation of changes.

Poznámky:

Anglicko - český slovník / English - Czech Glossary

Aborted connection**Předčasně ukončené spojení**

Connection terminated earlier, or in another way, than prescribed. It can often provide unauthorized access to unauthorized persons.

Access control**Řízení přístupu**

Making sure that access to an asset is authorized and limited on the basis of business (entrepreneurial) and security requirements.

Access control certificate**Certifikát řízení přístupu**

Security certificate containing information on access control.

Access control information (ACI)**Informace řízení přístupu**

Any information used for the purpose of access control including context information.

Access control list (ACL)**Seznam pro řízení přístupu (ACL)**

List of authorizations attached to some subject (e.g. a disc file); it determines who or what has the right to access the object and which operations it can do with it. In the security model using the ACL system, it searches ACL prior to performing any operation and looks up the corresponding record and on the basis of it makes a decision if the operation may be executed.

Access control policy**Politika řízení přístupu**

Set of principles and rules which define conditions to provide an access to a certain object.

Access level**Úroveň přístupu**

Level of authorization required to access protected sources.

Access period**Období přístupu**

Time period during which access to a certain object is allowed.

Access permission**Povolení přístupu**

All access rights of a subject related to a certain object.

Access right

Permission for a subject to access a concrete object for a specific type of operation.

Přístupové právo**Access type**

In computer security, type of an operation specified by an access right.

Typ přístupu**Accountability**

Responsibility of an entity for its activity and decision.

Odpovědnost**Accredited user**

User having certain right or permission to work in the information system and with the applications in accordance with defined access guidelines.

Autorizovaný uživatel**Active threat****Aktivní hrozba**

Any threat of an intentional change in the state of a data processing system or computer network. Threat which would result in messages modification, inclusion of false messages, false representation, or service denial.

Address resolution protocol (ARP)**Protokol ARP**

*Protocol defined in the document RFC 826 enables the translation of network addresses (**IP**) to hardware (**MAC**) addresses. ARP does not use authentication hence it cannot be misused for attacks, e.g. of the MITM type.*

Address space**Adresový / adresní prostor**

*ICT denotation for a continuous range of addresses. Address space is made up of a set of unique identifiers (**IP addresses**). In the Internet environment, IANA organization is the administrator of the address range.*

Administrative / procedural security**Administrativní / procedurální bezpečnost**

Administrative measures to ensure computer security. These measures can be operational procedures or procedures related to responsibility, procedures for examining security incidents and revision of audit records.

Administrator**Administrátor**

Person responsible for the management of a part of a system (e.g. information system) for which he/she usually has the highest access privileges (supervisor rights).

Advanced persistent threat (APT)**Pokročilá a trvalá hrozba (APT)**

Typical purpose of APT is a long-term and persistent infiltration into, and abuse

of, the target system using advanced and adaptive techniques (unlike usual single attacks).

Adware**Advertising supported software**

Type of software licence whose use is free, a commercial appears in the programme, which is used to finance programme development.

Aggregation**Agregace**

Controlled loss or limitation of information or equipment, usually by aggregation, merge, or statistical methods.

Algorithm**Algoritmus**

Finite ordered set of completely defined rules in order to solve some problem.

Anonymous login**Anonymní přihlášení**

Login into network and access to its resources without authentication of the party.

Antispam**Antispamový filtr**

Sophisticated software comparing each email with a number of defined rules and if the email satisfies a rule, counts in the weight of the rule. The weights can vary in value, positive and negative. When the total of weights exceeds a certain value, it is labelled as spam.

Anti-stealth technique**Anti-stealth technika**

Ability of an antivirus programme to detect even stealth-viruses (sub-stealth-viruses) which are active in memory, for example by using direct disc reading bypassing the operating system.

Antivirus**Antivir**

See Antivirus Program.

Antivirus program**Antivirový program**

Single-purpose or multipurpose programme doing one or more of the following functions: searching for computer viruses (by a single or several different techniques, often with a possibility of their selection or setting mode for search – scanning, heuristic analysis, methods of checksums, monitoring of suspicious activities), healing of infected files, backup and recovery of system sectors on the disc, storing control information on files on disc, providing information on viruses, etc.

Asset

Anything that has value to an individual, company or public administration.

Aktivum**Asset owner**

This is assumed to be an individual or entity whom the organization management has assigned the responsibility for production, development, maintenance, use and security of an asset.

Vlastník aktiva**Assets (information system)****Správce aktiva (provozovatel informačního systému)****Operator**

Individual (entity) who enables information processing or service providing and acts towards other natural and legal persons in the information system as the bearer of rights and obligations connected to operating the system.

Assets value**Hodnota aktiv**

Objective expression of a generally perceived value or a subjective evaluation of the importance (criticality) of an asset, or a combination of both approaches.

Asymmetric cryptography**Asymetrická kryptografie**

Asymmetric cryptography (also public-key cryptography) is a group of cryptographic methods where different keys are used for encrypting and decrypting – more precisely a pair of mathematically-bound keys. The pair is made up of a public key and a private key. Public key is the encryption key, key owner makes it public, and anyone can encrypt messages for the owner; decryption key is private, the owner holds it in secrecy and uses it to decrypt messages. In addition to making the content of communication secret, asymmetric communication is used also for the electronic (digital) signature that is the possibility to verify the author of data.

Attack**Útok**

Attempt at destruction, exposure to a threat, unwanted change, putting out of operation, stealing or obtaining an unauthorized access to an asset or execution of an unauthorized use of an asset.

Attack surface**Attack surface**

Code within a computer system that can be run by unauthorized users.

Audit**Audit**

Systematic process of unbiased obtaining and evaluation of audit records, whose objective is to determine whether system activities are in accordance with defined security policies and operational procedures.

Audit event

Event detected by the system and resulting in triggering and recording the audit.

Audit trail

Chronological record of those system activities which suffice for restoring, backtracking and evaluation of the sequence of states in the environment as well as activities related to operations and procedures from their inception to the final result.

Authentication

Process of verification of subject identity.

Authentication exchange

Mechanism whose objective is to find out the identity of an entity (subject) by way of information exchange.

Authentication information

Information used to establish validity of proclaimed identity of a given entity.

Authenticity

Attribute confirming that the entity is what it claims to be.

Authorization

Granting rights including granting access on the basis of access rights. Process of rights granting to a subject to perform defined activities in the information system.

Automated security incident measurement (ASIM)

Automatic monitoring of network operations with the detection of non-authorized activities and undesirable events.

Availability

Property of availability and usability at the request of an authorized entity.

Backdoor / trapdoor

Hidden software or hardware mechanism usually created for testing and error removal which can be used to bypass computer security. A method in a computer system or in an algorithm which allows the attacker to bypass the normal user authentication at the access to a programme or system and simultaneously

Auditovaná událost**Auditní záznam****Autentizační výměna****Informace o autentizaci****Autenticita****Autorizace****Automatické monitorování výskytu bezpečnostního incidentu****Dostupnost****Zadní vrátka**

allows to have this access hidden from normal checks. Firewall can be bypassed, in order to penetrate into the operating system, for example, by pretending to be a web browser. This code can assume the form of an independently installed programme or it could be a modification of an existing system. The access to the system as such tends to have the form of a fictitious user name and password which the attacked system accepts without checking and assigns to the user administrative rights.

Backup file**Záložní soubor**

Data file created with the objective of a possible future data reconstruction. Copies of data stored on another carrier (or even in a different place). Backup data are used in case of a loss, corruption or any other need to work with data stored in the past.

Backup procedure**Zálohovací procedura**

Procedure to enable data reconstruction in case of a failure or contingency.

Baiting**Využití návnady**

Mode of attack when the attacker leaves an infected CD, flashdisc or another storage medium where the victim can find it with a high probability, e.g. in a lift, on the car park. This leaves curiosity to play out and sooner or later the victim inserts the medium into the computer. This results in virus installation with which the attacker gets an access to the computer or the whole companywide computer network.

Baseline controls**Základní prvky řízení**

Minimal set of protective measures set for a certain system or organization.

Basic input output system (BIOS)**Základní vstupně-výstupní systém**

Software used during the start-up of a computer for initialization and configuration of connected hardware devices and subsequent start of the operating system.

Batch viruses**Dávkové viry**

Computer viruses created using batch files. An interesting possibility for some operating systems (e.g. UNIX), exist however even for MS-DOS. They are not too widespread and are more of a rarity.

Best practice**Příklad dobré praxe, osvědčený způsob**

Well-tested method or procedure which in the given area offers the most effective solution which has been repeatedly proven as right and leads towards

optimum results.

Biometric**Biometrický**

Related to the use of specific attributes reflecting the unique bio-physiological characteristics as is a fingerprint or voice record to validate personal identity.

BitTorrent**BitTorrent**

Tool for peer-to-peer (P2P) distribution of files which spreads out the load of data transfers among all clients downloading data.

Black hat**Black hat**

See Cracker.

Blue screen of death (BSOD)**Modrá obrazovka smrti**

Slang expression for an error message displayed by the Microsoft Windows operating system if there is a serious system error from which the system cannot recover. This error message is screen-wide, white letters on blue background (hence the name).

Bot**Bot (Robot)**

Within the framework of cyber criminality: programmes which take over computers in the network and use them for criminal activities – for example, distributed attacks (DDoS) and mass distribution of unsolicited commercial emails. Individual bots are the basis for large groups of robots known as botnets. Computer wholly or partially taken over by a bot is known as "zombie".

Bot herder / Bot wrangler**Bot herder / Bot wrangler**

(1) Cracker who controls a large number of compromised machines (robots, bots, zombies). (2) The topmost computer in the botnet hierarchy controlling compromised computers of the given botnet.

Botnet**Botnet (sít' botů)**

Network of infested computers controlled by a single cracker who thus has the possibility to access the power of many thousands of machines at the same time. It allows for illegal activities on a large scale – in particular, attacks as DDoS and spam distribution.

Breach**Prolomení**

Illegal breach into a system.

Brute force attack

Method to find passwords when the attacking programme tries all existing character combinations for a possible password. This method is very time-consuming. Its success depends on password length and the computing power of the used computer.

BSD lincence

A family of permissive free software licenses, imposing minimal restrictions on the redistribution of covered software

Bug

Term in ICT to denote a programming error which causes a security problem in software. The attacker utilizes such a vulnerability to control the computer, make a running service dysfunctional or running improperly, to modify data and similar.

Business continuity

Processes and/or procedures to ensure continuous operation of an organization.

**Business continuity management
(BCM)**

Holistic management model which identifies possible threats and their potential impact on the operations of an organization and which provides a framework for deepening the immunity of an organization by expanding its capabilities to respond effectively to emergency events and thus protect the interests of its key partners and customers, its reputation and its activities.

Business continuity management system (BCMS)

Part of the overall system of managing an organization which defines, introduces, operates, monitors, re-analyses, maintains and improves operating continuity of an organization.

Business continuity plan

Documented set of procedures and information which is made up and maintained in readiness for use during an incident in order to enable an organization to implement its critical activities at an acceptable and previously set level.

Certification

(1) Procedure in the computer security by means of which a third party gives a guarantee that the whole system or its part meets security requirements. (2) Process for verification of the competence of communication and information

Útok s použitím hrubé sily**BSD licence****Chyba****Kontinuita činností organizace****Řízení kontinuity organizace****Systém řízení kontinuity organizace****Plán kontinuity činností****Certifikace**

systems for handling classified information, approval of such competence and issuance of a certificate.

Certification authority (CA)

In computer security, a third party which issues digital certificates and uses its authority to confirm the authenticity of data which exist in the freely accessible part of the certificate.

Certification body

Third party which assesses and certifies a system, for example system for the control of computer security for a client organization, with regard to international standards and other documentation needed for a certified system.

Certification document

Document stating that any system of control, for example system for the control of information security, meets the required standard and other documentation needed for a certified system.

Clearing

Targeted overwriting or erasure of classified data on a data medium which has a special security classification and security category so that the given medium could be repeatedly used for a record in the same security classification and security category.

Closed-security environment

Environment where special attention (by a form of authorizations, security checks, configuration control, etc.) is given to protection of data and sources from accidental or intentional actions.

Cloud computing

Mode of utilization of computing technology whereby scalable and flexible IT functions are accessible to users as a service. The advantage of clouds: easy software upgrade, unsophisticated client stations and software, cheap access to a mighty computing power without hardware investments, guaranteed availability. Disadvantages: confidential data are available also to the cloud provider.

Communication security (COMSEC)

Use of such security measures in communications which prohibit unauthorized persons to obtain information which could be gained from access to communication traffic and its evaluation, or which ensure the authenticity of the communication process. Computer security as applied to data communications – data transfer.

Certifikační autorita (CA)**Certifikační orgán****Certifikační dokument****Vyčištění****Uzavřené bezpečnostní prostředí****Cloud computing****Bezpečnost komunikací**

Communication system

System which provides for the transfer of information among end users. It includes end communication devices, transfer environment, system administration, handling by personnel and operational conditions and procedures. It may also include means of cryptographic protection.

Completely automated public**Turing test to tell computers from humans (CAPTCHA)**

Turing test used on the web in an effort to automatically differentiate real users from robots, for example when entering comments, at registration, etc. The test usually consists of an image with a deformed text and the task for the user is to rewrite the pictured text into the entry field. It is assumed that the human brain can properly recognize even corrupted text but an internet robot using OCR technology cannot do. Disadvantage of the image CAPTCHA is its unavailability for users with visual impairment; hence usually there is the option of having the letters from the image read aloud.

Compromising

Compromise of information security which may result in programme or data modification, their destruction, or their availability to unauthorized entities.

Computer abuse

Unauthorized activity caused by intent or negligence which impacts computer security of a data processing system, or is related to it.

Computer crime / Cyber crime

Crime committed using a data processing system or computer network or directly related to them.

Computer emergency response team (CERT)

CERT is another name for CSIRT; unlike CSIRT, CERT is a registered trade mark. See CSIRT.

Computer fraud

Fraud committed using a data processing system or computer network or directly related to them.

Computer incident response capability (CIRC)

Capability of responding to computer incidents. It is part of cyber defence and uses in particular measures of INFOSEC. Ensures centralized capability for fast and effective reaction to risks and vulnerabilities in systems provides

Komunikační systém**CAPTCHA****Kompromitace****Zneužití počítače****Počítačová kriminalita /
Kybernetická kriminalita****Skopina pro reakci na počítačové****hrozby (CERT)****Schopnost pro reakci na počítačové****hrozby (CIRC)**

130

methodology for reporting and managing incidents provides support and help to the operational and security managements of systems. It is part of the emergency (crisis) planning for cases of system recovery.

Computer network**Počítačová síť**

Aggregate of computers together with the communication infrastructure (communication lines, hardware, software and configuration data) using which the computers can send and share data.

Computer network attack (CNA)**Útok na počítačovou síť**

Activity done in order to corrupt, block, degrade or destroy information stored in a computer or on a computer network, or the computer or computer network as such. Attack on a computer network is a certain sort of cyber attack.

Computer network exploitation (CNE)**Vytěžování počítačové sítě**

Abuse of information stored on the computer or computer network.

Computer security (COMPUSEC)**Počítačová bezpečnost**

Branch of informatics dealing with securing of information in computers (discovering and lowering risks connected to the use of the computer). Computer security includes: (1) enabling protection against unauthorized manipulation with the devices of a computer system, (2) protection against unauthorized data manipulation, (3) protection of information against pilferage (illegal creation of data copies), (4) secure communication and data transfer (cryptography), (5) secure data storage, (6) availability, integrity and authenticity of data. It is also the introduction of security properties of hardware, firmware and software into the computer system so that it is protected against unauthorized disclosure, amendments, changes or erasure of facts or to prevent these, or against access denial. Protection of data and sources against accidental or harmful activities.

Computer security audit**Audit počítačové bezpečnosti**

Independent verification of measures implementation and their efficiency with the view of attaining computer security.

Computer security incident response team (CSIRT)**Skupina pro reakce na počítačové bezpečnostní incidenty (CSIRT)**

Team of experts in information security whose task is to tackle security incidents. CSIRT provides its clients with the necessary services for solutions of security incidents and helps them in recovering the system after a security incident. In order to minimize incident risks and minimize their number, CSIRT offices provide also preventive and educational services. For clients, they provide information on detected weaknesses of used hardware and software

instruments and about possible attacks which make use of these weaknesses so that the clients may quickly address these weaknesses.

Computer system audit**Audit počítačového systému**

Analysis of procedures used in data processing in order to evaluate their efficiency and correctness, and to recommend improvements.

Computer virus**Počítačový virus**

Computer programme which replicates itself by attaching its copies to other programmes. It may contain a part which activates it when certain conditions are met (e.g. time) in the host device. It is distributed using the Internet (electronic mail, downloading programmes from unreliable sources), using mobile storage media and others. This is done in order to obtain various types of data, for identity theft, for putting the computer out of operation, etc.

Computer, personal computer (PC) **Osobní počítač**

In accordance with the wording of CSN 36 9001 this is "a data processing machine executing independent sequences of various arithmetic and logical operations." In other words: a machine characterized by processing data according to a previously created programme stored in its memory.

Confidentiality**Důvěrnost**

Characteristic that information is not available or is not disclosed to unauthorized individuals, entities or processes.

Configuration baseline**Výchozí stav konfigurace**

Configuration information formally related to a certain time in the lifetime of a service, or element of the service.

Configuration item (CI)**Konfigurační položka**

Element which must be controlled in order to deliver a service or services.

Configuration management database (CMDB)**Konfigurační databáze**

Data warehouse used for records of configuration items' attributes and relations among configuration items during their whole life cycle.

Consequence**Následek**

Result of an event which affects the objectives.

Contamination**Kontaminace**

Input of data with a certain security classification or security category into a wrong security category.

Contingency plan

Plan for backup procedures, response to an unforeseen event and recovery after a contingency.

Havarijní plán

Procedure which is an alternative to the normal procedure in case of an occurrence of an unusual but assumed situation.

Contingency procedure**Havarijní postup**

Procedure which is an alternative to the normal procedure in case of an occurrence of an unusual but assumed situation.

Continual improvement**Neustálé zlepšování**

Repeated activity for the increase of a capability to meet the requirements.

Control**Opatření**

It means control of a risk, including all policies, procedures, directives, usual procedures (practices) or organizational structures, which may be of an administrative, technological, management or legal character.

Control objective**Cíle opatření**

Statement describing what is to be achieved by introducing a measure.

Controlled access system (CAS)**Systém řízeného přístupu**

Means for automating of the physical control of access (e.g. use of badges equipped with magnetic strips, smart cards, biometric sensors).

Cookie / HTTP cookie**Cookie / HTTP cookie**

Data which a web application can store in the computer of a signed-in user. The browser then sends these data automatically to the application at every future access. Cookie is at present mostly used for the recognition of a user who visited the application before, or for storing user setting of the web application. Nowadays, discussions are underway about cookies in connection to watching the movements and habits of users by some webs.

Copy protection**Ochrana před kopírováním**

Use of a special technique for the detection or prevention of unauthorized copying of data, software and firmware.

Corrective action**Nápravné opatření**

Action to remove the cause of an identified noncompliance or other undesirable situation.

Countermeasure**Protiopatření**

Activity, equipment, procedure, technology intended to minimize vulnerability.

Covert Channel

Transmission channel which could be used for data transfer in a way impairing security policy.

Crack

Unauthorized infringement of programme or system security protection, its integrity or system of its registration/activation.

Cracker

Individual trying to obtain an unauthorized access to a computer system. These individuals are often harmful and possess means for breaking into a system.

Creative commons (CC)

A non-profit organization headquartered in Mountain View, California, United States devoted to expanding the range of creative works available for others to build upon legally and to share. The organization has released several copyright-licenses known as Creative commons licenses free of charge to the public.

Credentials

Data transferred in order to establish proclaimed identity of a given entity, credentials.

Crisis

Situation where the equilibrium among the basic components of the system on the one hand, and approach of the environment on the other hand, is disrupted in a serious way.

Crisis / Emergency situation

Emergency situation as per the law on integrated emergency system, compromise of the critical infrastructure, or any other danger when a state of hazard, state of emergency, or threat to the state is announced (henceforth only "emergency situation").

Crisis management

Collection of management activities of the bodies of crisis management aimed at the analysis and evaluation of security risks and planning, organization, implementation and verification of activities conducted in connection with preparation for crisis situations and their solution or protection of critical infrastructure.

Skrytý kanál**Crack****Cracker (prolamovač)****Creative commons (CC)****Autorizační údaje****Krise****Krizová situace****Krizové řízení**

Crisis measure

Organizational or technical measure to solve a crisis situation and remedy its consequences, including measures interfering with the rights and obligations of people.

Crisis plan

Aggregate planning document elaborated by entities set forth by law and which contains a set of measures and procedures to solve crisis situations.

Crisis planning

Activity of the relevant bodies of crisis management aimed at minimizing (prevention of) the origin of crisis situations. Searching for the most suitable ways of anti-crisis intervention, optimization of methods and forms to handle these unwanted phenomena (that is, reduction of the impacts of crisis situations) and establishing the most rational and economical ways of recovery for the affected systems and their return into the normal daily state.

Crisis preparedness

Preparation of measures to solve own crisis situations and partially participate in solving crisis situations in the neighbourhood.

Crisis state

Legislative measure announced by the Parliament of the Czech Republic (threat to the state, and the state of war), by the Government of the Czech Republic (state of emergency) or governor of the region/mayor (state of danger), in order to solve a crisis situation.

Critical communication infrastructure

In case of the state: complex of services or networks of electronic communications, clearly defined by law, whose unfunctionality would result in a serious impact on state security, public administration and provision of the basic daily needs of the population.

Critical information infrastructure

Complex of information systems clearly defined by law, whose unfunctionality would result in a serious impact on state security, economy, public administration and provision of the basic daily needs of population.

Critical infrastructure

Systems and services whose unfunctionality or wrong functionality would result in a serious impact on state security, its economy, public administration and in the end on provision of the basic daily needs of population.

Krizové opatření**Krizový plán****Krizové plánování****Krizová připravenost****Kritická komunikační infrastruktura (státu)****Kritická informační infrastruktura****Kritická infrastruktura**

Critical infrastructure protection**Ochrana kritické infrastruktury**

Measures aimed at lowering the risk of corruption of an element of the critical infrastructure.

Cross-section criteria**Průřezová kritéria**

Set of viewpoints to assess how serious is the corruption of an element in the critical infrastructure with bounds which include the scope of life losses, impact on the health of people, extraordinary serious economic impact or impact on the public due to an extensive limitation of providing the necessary services or any other serious intervention into the daily life.

Cross-site scripting (XSS)**Cross-site scripting (XSS)**

Attack on web applications consisting in an attempt to find a security error in the application and using this for the insertion of own code. The inserted code usually tries to get personal data of users, content of database or to bypass the security elements of an application.

Cryptography**Kryptografie**

Science of cryptography – a discipline covering the principles, means and methods to transform data in order to conceal their semantic content, to prevent an unauthorized use or prevent unrecognized modification.

Customer**Zákazník**

Organization or its part receiving a service or services.

Cyber attack**Kybernetický útok**

Attack on IT infrastructure having the objective of causing damage and obtaining sensitive or strategically important information. It is used most often in the context of either politically or militarily motivated attacks.

Cyber counterattack**Kybernetický protiútok**

Attack on IT infrastructure as a response to a previous cyber attack. It is used most often in the context of either politically or militarily motivated attacks.

Cyber crime**Kybernetická kriminalita**

Criminal activity in which a computer appears in some way as an aggregate of hardware and software (including data), or only some of its components may appear, or sometimes a larger number of computers either standalone or interconnected into a computer network appear, and this either as the object of interest of this criminal activity (with the exception of such criminal activity whose objects are the described devices considered as immovable property) or as the environment (object) or as the instrument of criminal activity (See

Computer crime).

Cyber defence

Defence against a cyber attack and mitigation of its consequences. Also, resistance of the subject towards an attack and a capability to defend itself effectively.

Cyber espionage

Obtaining strategically sensitive or strategically important information from individuals or organizations by using or targeting IT means. It is used most often in the context of obtaining a political, economic or military supremacy.

Cyber grooming (Child grooming, Cybergrooming)

Behaviour of users of internet communication instruments (chat, ICQ, et al.) who try to get the trust of a child in order to either abuse the child (especially sexually) or misuse the child for illegal activity.

Cyber security

Collection of legal, organizational, technological and educational means aimed at providing protection of cyberspace.

Cyber strategy

General approach to the development and use of capabilities to operate in cyberspace, integrated and coordinated with other areas of operation, in order to achieve or support the set objectives by using identified means, methods and instruments in a certain timetable.

Cyber terrorism

Criminal activity done using or targeting primarily IT means with the objective of creating fear or inadequate response. It is used most often in the context of attacks having an extremist, nationalistic or politically motivated character.

Cyber war, Cyber warfare

Use of computers and the Internet to wage a war in cyberspace. System of extensive, often politically motivated, related and mutually provoked organized cyber attacks and counterattacks.

Cyberbullying

Type of bullying using electronic means such as mobile phones, emails, pagers, internet, blogs and similar for sending harassing, offending or attacking mails and SMSs, creation of pages and blogs defaming selected individuals or groups of people.

Kybernetická obrana**Kybernetická špionáž****Kybergrooming (Child grooming, Kybergrooming)****Kybernetická bezpečnost****Kybernetická strategie****Kyberterorismus****Kybernetická válka****Počítačová / Kybernetická šikana**

Cyber-harassment

Internet harassment (even an individual case) usually of an obscene or vulgar character. It is often part of Cyberstalking. See also Cyberstalking.

Cyberspace

Digital environment enabling the origin, processing and exchange of information, made up of information systems and the services and networks of electronic communications.

Cybersquatting

Registration of the domain name related to the name or trade mark of another company, with the purpose of subsequent offering the domain to this company at a high financial amount.

Cyberstalking

Different kinds of stalking and harassment using electronic media (especially using emails and social networks), the objective being for example to instil a feeling of fear in the victim. The culprit obtains information about the victim most often from web pages, forums, or other mass communication tools. Often such an activity is merely an intermediate step to a criminal act which may include a substantial limitation of human rights of the victim, or misuse the behaviour of the victim to steal, defraud, blackmail, etc.

Czech cyberspace

Cyberspace under the jurisdiction of the Czech Republic.

Data

From the ICT point of view, this is a representation of information in a formalized way suitable for communication, explanation and processing.

Data authentication

Process used to verify data integrity (verification that received and sent data are identical, verification that programme is not infected by a virus, for example).

Data corruption

Accidental or intentional corruption of data integrity.

Data integrity

Assurance that data were not changed. In the figurative sense denotes also the validity, consistency and accuracy of data, e.g. databases or file systems. It tends to be implemented by checksums, hash functions, self-correcting codes,

Počítačové obtěžování**Kybernetický prostor****Doménové pirátství****Cyberstalking****Český kyberprostor****Údaje****Autentizace dat****Poškození dat****Integrita dat**

redundancy, journaling, etc. In cryptography and information security in general, integrity means data validity.

Data protection**Ochrana dat**

Administrative, technological, procedural, staffing or physical measures implemented in order to protect data against an unauthorized access or against corruption of data integrity.

Data reconstruction**Rekonstrukce dat**

Method of data reconstruction by analysing the original sources.

Data restoration/ Data recovery**Obnova dat**

Act of re-creation, or re-acquisition, of data lost, or whose integrity was compromised. Methods include copying from an archive, restoration of data from source data, or repeated establishment of data from alternative sources.

Data security**Bezpečnost dat**

Computer security applied to data. Includes for example control of access, definition of policies and ensuring data integrity.

Data validation**Validace dat**

Process used to determine if data are accurate, complete, or satisfy specified criteria. Data validation may contain checks of format, checks for completeness, control key tests, logical and limit checks.

Database**Databáze**

Set of data arranged by a notional structure which describes properties of these data and relations among corresponding entities, serves one or more application areas.

Deep packet inspection (DPI)**Podrobná inspekce paketů (DPI)**

A form of computer network packet filtering that examines the data part (and possibly also the header) of a packet as it passes an inspection point, searching for protocol non-compliance, viruses, spam, intrusions, or defined criteria to decide whether the packet may pass or if it needs to be routed to a different destination, or, for the purpose of collecting statistical information.

Defacement**Defacement, Zkreslení webových stránek**

Breaking into the web server of an adversary and replacing its internet pages by the content created by the attacker. Corruption is not hidden, quite the reverse, it aims at medialization and its psychological power rests on the one hand in creating a feeling of threat and mistrust in own information systems of the

infected party, on the other hand in presenting the ideology or points of view of the attacker.

Defence infrastructure

Set of objects, buildings, ground plots and equipment including necessary services, production and non-production systems needed to ensure their operation, regardless of the form of ownership and the way of utilization; whose destruction, damage or limitation of activity would, under situation of threat to the state or a state of war, put in danger fulfilment of tasks: (1) of Armed Forces of the Czech Republic (CZE) during the implementation of the Plan of defence of CZE as well as operational plans including plans for mobilization, (2) of experts during implementation of their partial plans of defence and other elements of security system of CZE, (3) of allied armed forces during the implementation of their operational plans, (4) of protection of population.

Demilitarized zone (DMZ)

Part of the network infrastructure of an organization which concentrates services provided to someone in the neighbourhood, or to the whole internet. These external (public) services are usually the easiest target of an internet attack; a successful attacker however only gets to DMZ, not straight into the internal network of the organization.

Denial of service (DoS)

Denial of service is the technique of attack by many coordinated attackers on the internet services or pages resulting in flooding by requests or breakdown or unfunctionality or unavailability of the system for other users.

Dialer

Harmful programme which connects the computer or smart phone of the user to Internet by a commuted line using a very expensive service provider (usually of the attacker).

Dictionary attack

Method for finding passwords when the cracking programme tries out all dictionary words in a dictionary for the password. This is a relatively fast method, depending on the size of the dictionary and whether the victim uses simple passwords.

Digital signature / electronic signature

Data attached to a message, which allow the receiver to verify the source of the message. Asymmetric cryptography is often used (signature is created by the private part of key and is verified by the public part). Goes usually hand in hand with the verification of data of the message.

Obranná infrastruktura**Demilitarizovaná zóna (DMZ)****Odmítnutí služby****Dialer****Slovníkový útok****Digitální podpis / Elektronický podpis**

Disaster recovery plan /**Contingency plan**

Plan for backup procedures, response to an unforeseen event and recovery after a contingency.

Disclosure**Odhalení, prozrazení, zveřejnění**

In IT context it is usually used for the expression of the fact that data, information or mechanisms were disclosed which should be hidden on the basis of policies and technical measures.

Distributed computing environment**(DCE)**

A software system developed in the early 1990s by a consortium that included Apollo Computer (later part of Hewlett-Packard), IBM, Digital Equipment Corporation, and others. The DCE supplies a framework and toolkit for developing client/server applications.

Distributed denial of service (DDoS)**Distribuované odmítnutí služby**

Distributed denial of service is the technique of attack by many coordinated attackers on the internet services or pages resulting in flooding by requests or breakdown or unfunctionality or unavailability of the system for other users.

Document**Dokument**

Information in a readable form. Document may be in a paper form or an electronic form as for example specification of policies, service level agreement, incident record or diagram of the computer room arrangement. See also Record.

Domain name**Doménové jméno**

Name to identify a computer, equipment or service in the network (including the internet). Example of a domain name: www.afcea.cz.

Domain name registry**Regist doménových jmen**

A database of all domain names registered in a top-level domain or second-level domain extension.

Domain name system (DNS)**Systém doménových jmen (DNS)**

Distributed hierarchical name system used on the Internet network. It translates domain names into numerical IP addresses and back, contains information about which machines provide the relevant service (e.g. accepts electronic mail or show the content of web pages).

Domain name system security extensions (DNSSEC)**Bezpečnostní rozšíření systému doménových jmen (DNSSEC)**

Set of specifications which enable the security of information provided to DNS by a system in IP networks (Internet, for example). DNSSEC uses asymmetric

encryption (one key for encryption and the second one for decryption). The owner of the domain which uses DNSSEC generates both the private and the public key. Using its private key it then electronically signs technical data about the domain which are then input into DNS. Using the public key which is stored at an authority superior to the domain, it is possible to verify the authenticity of the signature. A number of large servers use DNSSEC at present.

Domain name system server (DNS server)

DNS server / Jmenný server

Distributed hierarchical name system used in the Internet network. It translates the names of domains to numerical IP addresses and back, contains information about which machines provide the relevant service (e.g. receive emails or show content of web applications) etc.

Easter egg

Velikonoční vajíčko

Hidden and officially undocumented function or property of a computer programme, DVD or CD. Mostly these are puns and jokes doing no harm, graphics symbols, animations, subtitles with authors' names and similar. This hidden function is not activated in the usual way (menu, key, etc.) but by an unorthodox combination of the usual user activities, pushing a mouse key on an unusual place, special sequence of keys, and so on. Often, eggs are hidden on the screen under "About" where these can be displayed by tapping on various parts of this panel while holding the key ALT and similar.

Eavesdropping

Odposlech / Nežádoucí odposlech

Unauthorized catching of information.

Effectiveness

Efektivnost, účinnost

Scope in which planned activities are implemented and planned results are achieved.

Efficiency

Účelnost

Relation between the achieved results and how well have the sources been used.

Electronic attack

Elektronický útok

Use of electromagnetic energy for the purposes of an attack. Includes weapons with directed energy, high-power microwave and electromagnetic pulses and RF equipment.

Electronic communication service

Služba elektronických komunikací

Service usually provided for a fee which consists wholly or predominantly of signal transmission over electronic communication networks, including

telecommunication services and transmission services in networks used for radio and television broadcast and networks for cable television, excluding services which provide content using the networks and services of electronic communications or have editing supervision of the content transmitted over the networks and provided services of electronic communications; it does not include services of the information society which do not rest wholly or predominantly on the transmission of signals over networks of electronic communications.

Electronic defence**Elektronická obrana**

Use of electromagnetic energy to provide protection and to secure useful utilization of the electromagnetic spectrum (includes protection of forces, spaces, etc.).

Electronic mail (E-mail)**Elektronická pošta**

Text, voice or picture message sent using public network of electronic communications which can be stored in the network or end-user terminal until collected by the user.

Electronic means**Elektronické prostředky**

Primarily a network of electronic communications, electronic communication equipment, terminals, automatic call and communication systems, telecommunication and electronic mail.

Electronic signature**Elektronický podpis**

See Digital signature.

Electronic warfare**Elektronický boj**

Military activity using electromagnetic energy in support of offensive and defensive actions in order to achieve offensive and defensive supremacy. This means engaging in fighting in the environment using electromagnetic radiation. It is a separate discipline but as one of the elements it supports cyber security within NNEC.

Element of the critical infrastructure**Prvek kritické infrastruktury**

Building, equipment, device or public infrastructure in particular, determined using the cross-criteria and sector criteria; if the element in the critical infrastructure is a part of the European critical infrastructure, it is considered to be an element of the European critical infrastructure.

Emulation

Use of a data processing system to emulate another data processing system; emulating system receives the same data, runs the same programmes and exhibits the same results as the emulated system.

Encryption

Cryptographic transformation of data, also the science about methods of hiding the meaning of messages by a transformation into a form which is readable with special knowledge only.

Entity / identity Authentication

Execution of tests making it possible for a data processing system to recognize and authenticate the entity.

Entrapment

Intentional placement of obvious defects into a data processing system in order to detect penetration attempts, or to deceive an adversary who should use the defect.

Establishing the context**Stanovení kontextu**

Establishing the limits of external and internal parameters to be taken into account during risk management and setting of the risk validity ranges and risk criteria for the risk management policy.

European critical infrastructure**Evropská kritická infrastruktura**

Critical infrastructure in the territory of the Czech Republic whose infringement would result in a serious impact also on another member of the European union.

European network and information security agency (ENISA)**Agentura pro elektronickou a informační bezpečnost**

Agency founded in 2004 by the European Union as a cooperative centre in the area of network and information security. Its role is to create an information platform for the exchange of information, knowledge and "best practices" and thus help EU, its member states, private sector and the public in the prevention and solutions of security problems.

Event**Událost**

Occurrence or change of a certain set of circumstances.

Exploit**Zneužití**

(1) Error, or an error in a programme, software, command sequence, or a code enabling a user to use programmes, computers or systems unexpectably or in an unauthorized way. (2) Also a security hole or a case using a security hole.

Exposure

Possibility that a concrete attack would use a specific vulnerability of a data processing system.

External context

External environment where an organization strives to achieve its objectives.

Extranet

Analogy of the intranet, available however on a larger scale than for internal needs only but fully public – for example, for business partners or foreign branches.

Failover

Automatic switch to a backup system or process at the instant of failure of the previous one in order to achieve a very short time of outage and increase in reliability.

Failure access

Unauthorized and usually unintentional access to data in a data processing system which is the result of hardware or software failure.

File

General named set of data. It can be a document, multimedia data, database or practically any other content, which the user or software may find useful to have permanently available under a concrete name.

File protection

Implementation of suitable administrative, technological or physical means for the protection against unauthorized access, modification or erasure of a file.

File system

Method of organization and storage of data in the form of files so that access to them would be easy. File systems are stored on a suitable type of electronic memory which can be located directly in the computer (hard disc) or can be made accessible using a computer network.

File transfer protocol (FTP)

An Internet standard (RFC 959) for transferring files between a client and a server.

Vystavení hrozbám**Vnější kontext****Extranet****Failover****Chybný přístup****Soubor****Ochrana souboru****Souborový systém****File transfer protocol (FTP)**

Firewall

Comprehensive system of security measures which should prevent unauthorized electronic access to a computer or concrete services in the network. Also, a system of devices or set of devices, which could be configured in such a way as to allow, forbid, encrypt, decrypt or act as a mediator (proxy) for all computer communications among various security domains, based on a set of rules and other criteria. Firewall can be implemented as hardware or software, or a combination of both.

Firmware

Programme controlling hardware.

Flaw / loophole

Operational dysfunction, omission, or oversight making it possible to bypass protective mechanisms or put them out of action.

Flooding

Accidental or intentional insertion of a large volume of data resulting in a service denial.

Forensic analysis / investigation

Analysis used on digital data to obtain proofs about the activities of users (attackers) in the area of information and communication technologies.

Forum for incident response and security teams (FIRST)

Worldwide organization uniting about 200 workplaces of the CSIRT/CERT type.

Freeware

Proprietary software usually distributed free (or for a symbolic reward). We speak sometimes about a kind of software licence. Conditions for the free use and distribution are defined in the licence agreement. The author of the freeware usually retains the copyright.

Generic TLD

See TLD.

Generic traffic flood

Form of a DDoS attack.

Firewall**Firmware****Závada****Zaplavení, zahlcení****Forensní analýza / vyšetřování****FIRST****Freeware****Obecné zahlcení**

GNU / GPL

General public licence GNU – licence for free software requesting that related creations be available under the same licence.

GNU privacy guard (GPG)

Free version of PGP. See PGP.

Governance

Making sure that security policies and strategies be really implemented and that the required processes be correctly adhered to.

Grey hat

*An individual who according to the activity stands between **White hat** and **Black hat** hackers, since the individual abuses security weakness of systems or a product in order to publicly draw attention to their vulnerability. However, publicizing these sensitive information may be an opportunity to persons of the **Black hat** character to commit criminal acts.*

Guideline

(Binding) recommendation of what is expected to be done in order to achieve a certain target.

Hack / Hacking

Often used in the sense under the entry Crack. The second usual use is in the sense of a fitting, unusual, witty, or fast solution of a programming or administrative issue.

Hacker

Person: (1) who engages in the study and analysis of details of programmable systems most often for an intellectual inquisitiveness and keeps on improving this ability (White Hat); (2) who enjoys programming and who programs well and fast; (3) who is an expert for a certain operating system or a programme, e.g. UNIX. The idea of Hacker is often improperly used for persons who abuse their knowledge during breaking into an information system and thus break the law. See Cracker.

Hackers for hire (H4H)

Acronym for hackers who offer their services to other criminal, terrorist or extremist groups (hired hackers).

GNU / GPL

General public licence GNU – licence for free software requesting that related creations be available under the same licence.

PGP**Ovládnutí****Grey Hat****Směrnice****Hack / Hacking****Hacker****Hackers for hire (H4H)**

Hactivism

Use of hacker skills and techniques to achieve political objectives and to support political ideology.

Hardware

Physical components of a system (equipment) or their parts (e.g. a computer, printer, peripheral devices).

Help desk

Online (as a rule, telephone) service offered by an automated information system and through which users can get help for using shared or specialized services of the system.

High-tech crime

Criminal activity focused on advanced technology as the objective, means or instrument of the criminal act perpetrator (often it is also the activity which could be labelled as "computer" or "information" criminality). In essence, in all of these versions it may be a very diverse mixture of activities when concrete technology may be the item of interest, the object (environment), or the instrument for the act. This can, as the final consequence, lead to the approach when the above-mentioned set of principles is considered: (1) rather broadly ("any criminal or otherwise harmful activity with the elements of computing technology"), including the case when, for example, a computer system is used for money or stock counterfeiting; (2) rather narrowly that is as acts committed against information technologies, which cannot be committed by any other means nor against any other target.

Hoax

It tries to create an impression of trustworthiness by its content. It informs, for example, about the spread of viruses or it inveighs against the social feeling of the addressee. It may contain harmful code or a link to internet pages with harmful content.

Honeypot

Serves as a bait luring the attacker (malware) and after trapping a potentially dangerous software there is an automatic analysis.

Hypertext transfer protocol (HTTP) **Hypertext transfer protocol (HTTP)**

An application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

Hactivism**Technické prostředky (vybavení)****Horká linka****Kriminalita, související s pokročilými technologiemi****Poplašná zpráva****Honeypot**

Hypertext transfer protocol secure (HTTPS)

A widely used communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. Technically, it is not a protocol in and of itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (**HTTP**) on top of the **SSL/TLS** protocol, thus adding the security capabilities of **SSL/TLS** to standard **HTTP** communications.

Chain letter

Letter sent out to many recipients and containing information which each recipient has to pass on to many other addressees. It is a frequently used method of pressure ("If you do not send this letter to 25 other people, something terrible happens to you in 25 days").

Chat

Way of direct (online) communication of several persons using the Internet.

ICMP flood

An attack using the ICMP protocol. Most often used are ICMP echo (**Ping**) packets which serve to establish if the remote (target) equipment is available. Sending out a large number of these ICMP messages (or large ICMP echo packets) may result in clogging the remote system and its slowdown or total unavailability. This is a simply executed attack of the **DDoS** type.

Identification

Act or process during which an entity submits an identifier to the system and on its basis the system can recognize the entity and differentiate it from other entities.

Identifier

Identity information that unambiguously distinguishes one entity from another one in a given domain.

Identity

Set of attributes which uniquely define a definite object – a thing, person, and event.

Identity token

Token used to find out and verify (authenticate) the identity.

Hypertext transfer protocol secure (HTTPS)**Řetězový dopis****Chat****ICMP záplava****Identifikace****Identifikátor****Identita****Identifikační předmět**

Identity validation**Validace identity**

Execution of tests enabling a system to recognize and validate entities on the basis of data processing.

Impact**Dopad**

(1) Adverse change in the attained degree of objectives. (2) Consequences of a certain act or event.

Incident**Incident**

*Incident in the **ICT** environment assumed to be an event which is usually related to the outage of a network, service, or to a deterioration of its quality.*

Info-crime**Informační kriminalita**

Criminal activity with a determined relation to software, data, more precisely to stored information, more precisely all activities resulting in unauthorized reading, handling, erasing, abusing, changing or other data interpreting.

Information**Informace**

Any sign expression which makes sense for the communicator and receiver.

Information (cyber) society**Informační (kybernetická) společnost**

Society capable of utilizing, and indeed utilizing, information and communication technologies. The basis is an incessant exchange of knowledge and information and handling them under the assumption of understanding these. This society considers creation, distribution and manipulation of information as the most significant economic and cultural activity.

Information and communication technology (ICT)**Informační a komunikační technologie**

Under information and communication technology we understand all technology dealing with processing and transfer of information, in particular computing and communication technology and software.

Information asset**Informační aktivum**

Knowledge and data of value (importance) to an organization.

Information assurance**Information assurance**

Set of measures to achieve the required level of confidence in the protection of communication, information and other electronic as well non-electronic systems and information stored, processed or transferred in these systems with regard to confidentiality, integrity, availability, undeniability and authenticity.

Information operation (IO)

Planned, goal-oriented and coordinated activity done in support of political and military objectives of an operation, to influence the decision-making process of a possible adversary and its allies by affecting its information, information processes and communication infrastructure and at the same using information and protection for own information and communication infrastructure. IO is exclusively a military activity which has to coordinate military information activities with the objective of influencing the thinking (will), understanding and capabilities of the adversary or potential adversary. All information activities should be conducted in line with the objectives of the military operation and to support them at the same time.

Information processing facilities

Any system, service or infrastructure processing information, or the localities of their placement.

Information security

Security (protection) of confidentiality, integrity and availability of information.

Information security (INFOSEC)

Implementation of general security measures and procedures for: (1) protection of information against loss or compromise (loss of confidentiality, integrity and reliability), or as the case may be for their detection and adoption of remedial actions. (2) Continuation of information accessibility and ability to work with them within the scope of functional rights. Measures INFOSEC cover security of computers, transmission, emissions and encryption security and exposing threats to facts and systems and prevention thereof.

Information security event

Identified occurrence of a state of the system, service or network noting a possible breaking of policy, information security or a failure of measures or of formerly unknown situation which could be important for security.

Information security incident management

Processes for detection, reporting and assessing of security incidents, response to security incidents, handling and learning from security incidents.

Information security incident management

Processes for detection, reporting and assessing of security incidents, response to security incidents, handling and learning from security incidents.

Informační operace (IO)**Prostředky pro zpracování informací****Bezpečnost informací****Bezpečnost informací / informačních systémů****Řízení bezpečnostních incidentů****Zvládání bezpečnostních incidentů**

Information security management system (ISMS)	Systém řízení bezpečnosti informací (SRBI)
--	---

Part of the management system, based on the attitude towards security risks, definition, implementation, operation, monitoring, re-analysing, administration and improvement of information security.

Information security risk	Riziko bezpečnosti informací
----------------------------------	-------------------------------------

Aggregate of possibilities that a threat would utilize the vulnerability of an asset or group of assets and thus cause damage to an organization.

Information security threat	Bezpečnostní hrozba
------------------------------------	----------------------------

Potential cause of an undesirable event which may result in a damage to system and its assets, e.g. destroying, undesired accessing (compromising), data modification or inaccessibility of services.

Information society service	Služba informační společnosti
------------------------------------	--------------------------------------

Any service provided by electronic means at the individual request of a user and put in by electronic means, usually provided for a fee. The service is provided by electronic means if it is sent by means of an electronic communication network and picked up by the user from electronic equipment for data storage.

Information system	Informační systém
---------------------------	--------------------------

(1) A functional aggregate enabling goal-oriented and systematic acquisition, processing, storage and access to information and data. Includes data and information sources, mediums, hardware, software and utilities, technologies and procedures, related standards and employees; (2) A complex of elements existing in mutual interaction (L. von Bertalanfy, 1956).

Information warfare	Prostředky Informační války
----------------------------	------------------------------------

Integrated use of all military capabilities including information security, deception, psychological operations, electronic warfare and destruction. All forms of reconnaissance, communication and information systems contribute to it. The objective of information warfare is to put obstacles in the flow of information, influence and decrease efficiency or liquidate the system of command and control of the adversary, and at the same time to protect own systems of command and control from similar actions of the adversary.

Informatisation of society	Informatizace společnosti
-----------------------------------	----------------------------------

Process of promoting new literacy in a society focused on adopting new methods of work with computers, information and information technology.

Infoware

Application for the automatic support of classical battle events, more precisely a set of activities serving to protect, mine out, damage, suppress or destroy information or information sources, with the objective of achieving a significant advantage in a battle or victory over a concrete adversary. The notion of Infoware must not be mistaken with the notion Infowar that is information war.

Insider

Dangerous user (employee, intern) who abuses a legal access to the communication and information system of an organization, in particular in order to perform unauthorized pilferage of sensitive data and information.

Integrity

Attribute of protection for accuracy and completeness of assets.

Interested party

Subject having an interest in the efficiency or success of an organization.

Interface**Rozhraní**

Location and mode of interconnecting systems or their parts.

Internal context**Vnitřní kontext**

Internal environment where an organization strives to achieve its objectives.

Internal group**Vnitřní, interní skupina**

Part of an organization of a service provider which has concluded a documented contract with the service provider about its share in the design, handover, delivery and improvement of a service or services.

Internet**Internet**

Global system of interconnected computer networks which use the standard internet protocol (TCP/IP). Internet serves billions of users around the world. It is a network of networks consisting of millions of private, public, academic, commercial and government networks, with a local to global outreach, that are all interconnected by a wide range of electronic, wireless and optical network technologies.

Internet assigned numbers authority (IANA) **Úřad pro přidělování čísel na Internetu (IANA)**

Authority overseeing IP address assignment, administration of DNS zones

(assignment of **TLD** domains and the creation of generic domains) and the administration and development of internet protocols. At present, **IANA** is one of the departments of the **ICANN** organization.

Internet control message protocol (ICMP)

This is a service protocol which is part of the **IP** protocol. Its main mission is to report error messages regarding the availability of services, computers or routers. For these purposes, ping or traceroute instruments are used, for example.

Internet corporation for assigned names and numbers (ICANN)

Non-profit organization responsible for the administration of domain names assignment as well **IP addresses**, for the maintenance of operational stability of internet, support of economic competition, achievement of broad representation of the global internet community, and which develops its mission by a bottom-to-top management and consensual processes.

Internet protocol (IP)

Protocol by which all equipment in the Internet mutually communicate. Today, the most used is the fourth revision (**IPv4**); however, step by step there will be a transition to a newer version (**IPv6**).

Internet relay chat (IRC)

Form of live (real-time) communication of text messages (chat) or synchronous conferences. These are systems intended primarily for group communications in discussion forums, so-called channels, but it enables also one-to-one communication via a private message, as well as a chat and data transfer using direct client-to-client. Today, it is not used so much; it has been replaced by newer instruments such as *Skype*, *ICQ* or *Jabber*.

Internet security

Protection of confidentiality, integrity and accessibility of information in the Internet network.

Internet service provider (ISP)

Organization offering access to internet to its customers.

Interoperability

Capability to act jointly in fulfilling set objectives, or the capability of systems, units or organizations to provide services to other systems, units or organizations and accept these from them and thus use shared services for an

Internet control message protocol (ICMP)

Internetová společnočnost pro přidělování jmen a čísel na internetu (ICANN)

Internet Protocol (IP)

IRC

Bezpečnost internetu

Poskytovatel služeb internetu

Interoperabilita

effective common activity.

Intranet

Private (internal) computer network using the classical Internet technology making it possible for employees of an organization to communicate effectively and share information.

Intrusion detection system (IDS)

Technical system that is used to identify that an intrusion has been attempted, is occurring, or has occurred and possibly respond to intrusions in information systems and networks.

Intrusion prevention system (IPS)

Variant on intrusion detection systems that are specifically designed to provide an active response capability.

IP address

Number which uniquely identifies a network interface which uses IP (internet protocol) and serves for the differentiation of interfaces connected in the computer network. At present, the most widespread version IPv4 uses a number of 32 bits written in decimal in groups of eight bits (e.g. 123.234.111.222).

IP spoofing

Substitution a spurious IP address on a device (a computer) which triggers connection (with a recipient) in order to hide the real sender. This technique is used particularly in attacks of DoS type.

IS security policy

General purpose of management and direction in the control of information system security with the definition of criteria to assess risks.

ISMS project

Structured activities executed by an organization during the ISMS introduction.

IT network

Geographically distributed system formed by interconnected IT systems for information exchange and containing different components of the interconnected systems and their interfaces with data communication networks which complement them.

Intranet**Systém detekce průniku (IDS)****Systém prevence průniku (IPS)****IP adresa****Podvržení IP adresy****Bezpečnostní politika informačního systému****Projekt ISMS****IT síť**

IT security policy

Rules, directives and practices deciding how are assets including sensitive information administered, protected and distributed inside the organization and its ICT systems.

IT system

Set of devices, methods, data, metadata, procedures and sometimes persons that is arranged so as to fulfil some functions during information processing.

Key authentication

Process of verification that the public key truly belongs to that person.

Keylogger (Keystroke logger)

Software reading when individual keys are pushed; may however be regarded as a virus by an antivirus programme, in case of software it may be a certain form of spyware but there are even hardware keyloggers. It is often used for secret monitoring of all PC activities, is invisible for other users and protected by a password. It enables automatic logging of all keystrokes (written text, passwords, etc.), visits to www pages, chats and discussions over ICQ, MSN and similar, running applications, screenshots of computer work, user file handling and other. Logged data could be secretly sent by email.

Knowledge base

Database containing reference rules and information about the experience and professional knowledge in a certain area.

Known error

Problem whose primary cause is known, or for which a method is established, to decrease or remove the impact of the problems on a service, using a substitute solution.

Lamer

Person, usually a complete beginner, who is unfamiliar with the given IT issues.

Leetspeak

Language replacing the letters of the Latin alphabet by numerals and printable ASCII characters. It is used quite a lot in the internet (chat and online games). This computer dialect, usually of the English language, has no fixed grammatical rules and words may be formed by shortening, e.g. by omissions of letters or corruption ("nd" – end, "U" – you, "r" – are).

Bezpečnostní politika IT**IT systém****Autentizace klíče****Znalostní báze****Známá chyba****Lamer****Leetspeak**

Level of risk / risk level**Úroveň rizika**

Magnitude of risk expressed as the combination of consequences and the possibility of their occurrence.

Licence**Licence**

Permission as well as to the document recording that permission.

Life cycle**Životní cyklus**

Collection of stages through which a system transits from the moment of development beginning up to end of life or liquidation, including the implementation of changes.

Likelihood**Pravděpodobnost, možnost výskytu**

Possibility that something occurs.

Linkage / Fusion**Spojování / Fúze**

Useful combination of data or information from one data processing system, with data or information from another system, so as to declassify protected information.

Local area network (LAN)**Lokální síť (LAN)**

Term for small networks, usually within administratively uniform aggregates – companies, buildings, communities, which are formed with the aim to facilitate sharing of means (IS, data, services, equipment) and to enable an effective protection against undesirable phenomena.

Local internet registry (LIR)**Lokální internetový registr**

Organization, usually active in one network, which is assigned a block of IP addresses from RIR. LIR assigns the IP address blocks to its customers connected to the given network. Most LIRs are internet service providers, companies or academic institutions. Related expressions – RIR.

Log**Log**

Shortened expression for Log file.

Log file**Soubor logů**

File containing information on the activities of subjects in the system, access to this file is controlled.

Logical access control**Logické řízení přístupu**

Use of mechanisms related to data or information to enable control of access.

Logical bomb**Logická bomba**

Harmful logic causing damage to a data processing system and being triggered by certain specific system conditions. Programme (subset of Malware) which is secretly put into applications or into an operating system where, under predetermined conditions, it performs destructive activities. Predetermined specified condition triggering the logical bomb may be, for example, a fixed date (anniversary of a certain event – See for example "Virus 17. November"). In this case the type is a so-called time bomb.

Loss**Ztráta**

Quantitative measure of damage or loss as a consequence of a compromise.

MAC address**MAC adresa**

MAC = Media Access Control. Unique identifier of a network device allotted by the manufacturer.

Maintenance hook**Tajná vrátka / Přístup ke službám**

Loophole in software which enables easy maintenance and addition of other characteristics and which can enable an access to a programme in unusual locations or without the usual checks.

Malformed query**Špatně utvořený dotaz**

(1) Erroneous query which may result in triggering a nonstandard or unexpected behaviour of a system. (2) Mode of an attack.

Malicious logic**Zlovolná logika**

Programme implemented in hardware, firmware or software whose purpose is to perform some unauthorized or harmful action (e.g. a logical bomb, Trojan horse, virus, worm, etc.).

Malware – malicious software**Škodlivý software**

This is the general name for harmful programmes. Harmful software includes computer viruses, Trojan horses, worms, spyware.

Man in the middle (MITM)**Člověk uprostřed**

Type of attack whereby the attacker intercepts, reads and modifies communication between two communicating parties without their knowledge.

Management system**Systém řízení**

Framework of policies, procedures, directives and affiliated sources to achieve the objectives of an organization.

Manipulation / modification detection**Detekce manipulace**

Procedure to ascertain whether data were modified, either by accident or by design.

Masquerade (IP masquerading)**Maškaráda (IP maškaráda)**

Mechanism which allows to connect to the Internet a large number of devices for which no so-called public IP addresses are available. These devices are assigned so-called private IP addresses and access to the Internet is implemented through the mechanism of address translation (NAT, Network Address Translation).

Message authentication / data origin authentication**Autentizace zprávy**

Verification that message was sent by the alleged originator to the intended receiver and that this message was not changed in transmission. Verification of the identity of information source-sender of the message. Frequently, digital signature is used.

Message authentication code**Kód autentizace zprávy**

Bit string which is a function of data (in an encrypted or plain form) and the secret key, and is attached to data in order to authenticate them.

Minimum business continuity objective (MBCO)**Minimální úroveň chodu organizace**

Minimal level of services and/or products which is acceptable to attain the objectives of an organization during a contingency.

Monitoring**Monitorování**

Permanent checking, supervision, critical observation or determination of status in order to identify a change from the required or expected level of performance.

National authority**Národní autorita**

State authority responsible for the issues of cyber security (guarantee).

National security council**Bezpečnostní rada státu**

Permanent working body of the government of the Czech Republic (CZE) for the coordination of security of CZE and preparation of proposals to implement them.

NATO computer incident response capability – Technical centre (NCIRT TC)

NATO CIRC technical support centre – second level. It enables the capability to respond to incidents, monitor incidents, perform system recovery, and provides a direct technical support and help to the operational and security management of the operational NATO information systems.

NATO Cooperative cyber defence centre of excellence

NATO centre for cooperation in cyber security (Filters tee 12, Tallinn 10132, Estonia, <http://www.ccdcoe.org>).

NATO Cyber defence management authority

NATO authority to manage cyber defence with the aim of providing an umbrella and interconnections for existing capabilities of cyber defence within the Alliance.

Network**Sít'**

Set of computer terminals (workstations) and servers which are mutually interconnected in order to exchange data and communicate.

Network address translation (NAT) Překlad sít'ových adres

*Mechanism enabling access of several computers from a local network to the Internet under one public IP address. Computers from the local address are assigned so-called private IP addresses. The border element of such a local network provides for the translation of a private IP address to a public one. See also *Private IP address*.*

Network behavior anomaly detection (NBAD)**Detekce anomálního chování sítě (NBAD)**

A solution for helping protection against zero-day attacks on the network. NBAD is the continuous monitoring of a network for unusual events or trends. NBAD is an integral part of network behaviour analysis, which offers security in addition to that provided by traditional anti-threat applications such as firewalls, antivirus software and spyware-detection software.

Network core**Páteřní síť**

Central part of a telecommunication network that provides various services to customers who are connected by the access network.

Network integrity**Integrita sítě**

Functionality and operational capability of interconnected networks of electronic communications, protection of these networks against failures caused

by electromagnetic jamming or operational loading.

Network of electronic communications

Transmission systems, or as the case may be, communication and routing equipment and other devices, including elements of the network which are not active, which make for the transmission of signals over wire lines, by radio, optical or other electromagnetic devices, including satellite networks, fixed lines with commuted circuits or packets, and mobile ground networks, networks for the distribution of electrical energy in the extent to transmit signals, networks for radio and television broadcast and networks for cable television, regardless of the type of transmitted information.

Nonconformity

Non-conformity with a request.

Non-repudiation

Capability to prove the occurrence of an alleged event or activity, and originating entities with the objective to solve controversies about the occurrence of an event or an absence of an occurrence, or about the activity and involvement of entities into the events.

Open communication system

It represents (includes) a global computer network including all its functions and supported both by private companies and public institutions.

Open software foundation (OSF)

A not-for-profit organization founded in 1988 under the U.S. National Cooperative Research Act of 1984 to create an open standard for an implementation of the UNIX operating system.

Open-security environment (OSE)

Environment where data and source protection against accidental or intentional acts is achieved by using standard operational procedures.

Operating system

Software which controls programme executions and which can offer various services, e.g. assignment of devices, scheduling, control of input and output and data administration. Examples of operating systems are the MS DOS system, LINUX, UNIX, Solaris, and other.

Síť elektronických komunikací**Neshoda****Nepopiratelnost****Otevřený komunikační systém****Open software foundation (OSF)****Otevřené bezpečnostní prostředí****Operační systém**

Operational documentation

Documentation of the information system of public administration describing the functional and technological features of the information system.

Operator of the information system of public administration.

Subject performing at least some of the activities related to the information system. The administrator of the information system of public administration can commission other subjects unless prohibited by a law.

Operator of the information system of public administration.

Subject who by law determines the objective and means for information processing and is responsible for the information system.

Packet

Block of data transferred in computer networks and using the technology of "packet switching". A packet consists of control data and user data. Control data contain information necessary for packet delivery (destination address, source address, checksums, and information on packet priority). User data contain those data items which should be delivered to the target (destination addressee).

Passive threat

Threat of making an access to data without actually changing the state of the data processing system or the computer network.

Password

Character string used as part of the authentication information. General instrument to authenticate a user signing up to a computer, accessing files, programmes and services.

Password cracker

*Programme designed to crack passwords either by the **Brute force attack** or **dictionary attack**.*

Patch

Update which removes a security problem or unstable behaviour of an application expands its possibilities and enhances its performance.

Peer to peer (P2P)

This is a computer network where individual clients communicate directly. This model is primarily used in interchangeable networks. Total transmission capability grows as a rule with the growing number of users in this model. In the

Provozní dokumentace**Provozovatel informačního systému veřejné správy****Správce informačního systému veřejné správy****Paket****Pasivní hrozba****Heslo****Prolamovač hesel****Záplata****Rovný s rovným**

classic model client-server this is quite the reverse.

Penetration**Proniknutí / průnik**

Unauthorized access to a computer system, network or service.

Penetration testing**Penetrační testování**

Analysis of functions of a computer system and networks with the objective of finding out weak spots in computer security so that these could be removed.

Peripheral equipment**Periferní zařízení**

Equipment controlled by a computer and able to communicate with it, e.g. input/output devices and auxiliary memory.

Pharming**Pharming**

*Fraudulent method used on the Internet to obtain sensitive data from the victim of the attack. The principle is an attack on **DNS** and rewriting the **IP** address which results in redirecting the client to a false address of internet banking, email, social network, etc., after inserting the **URL** into the browser. These pages are as a rule indistinguishable from the real pages of a bank and even experienced users may not recognize this change (unlike the related technique of **phishing**).*

Phishing**Phishing („rybaření“, „rhybaření“, „házení udic“)**

Fraudulent method having the objective of stealing the digital identity of a user, the sign-on names, passwords, bank account numbers and accounts etc. in order to subsequently misuse these (drawing cash from the account, unauthorized access to data etc.). Creation of a fraudulent message distributed mostly by electronic mail trying to elicit the mentioned data from the user. The messages may be masqueraded so as to closely imitate a trustworthy sender. It may be a forged request from a bank whose services the user accesses with a request to send the account number and PIN for a routine check (use of the dialog window purporting to be a bank window – so-called spoofing). Thus the fraudster tries to convince accessing persons that they are at the right address whose security they trust (pages of electronic shops etc.). Also, very often credit card numbers and PINS are stolen in this fashion.

Phone phishing**Telefonní phishing**

This technique uses a false voice automaton (Interactive Voice Response) with a structure similar to the original banking automaton ("For a change of password press 1, for connection to a bank advisor press 2"). The victim is usually asked in an email to call the bank for information verification. Here,

sign-on is requested using a PIN or a password. Some automata subsequently transfer the victim to a contact with the attacker playing the role of a telephone bank advisor which allows for other possibilities for questions.

Phreaker

Person doing "hacking" on the phone, using various tricks manipulating the services of telephone companies.

Phreaking

Denotation for tapping into a somebody else's telephone line in distribution panels, public telephone booths or directly in the ground/below ground telephone lines and thanks to these: (1) it is possible to call anywhere free of charge, (2) surf the internet free of charge, and (3) listen to somebody else's telephone conversations. Payment for the call is of course at the cost of the victim (registered user of the line, or the telephone company). Tapping into a mobile network by using various methods or the manufacture of listening devices is also considered phreaking.

Physical access control

*Use of physical mechanisms to enable control of access (e.g. placing the computer in a locked room). See **Access Control**.*

Physical asset

Asset having a material character.

Piggyback entry**Fyzické řízení přístupu**

Unauthorized access to the system using a legitimate link of an authorized user.

Ping**Fyzické aktivum**

Instrument used in computer networks for testing computer availability over IP networks. Ping measures the time of response and records the volume of lost data (packets).

Ping flood**Zahlcení pingy**

*Simple DoS attack when the attacker floods the victim with requests "ICMP Echo Request" (ping). The attack is successful provided the attacker has a wider bandwidth than the victim, or, the attacker can at the same time cooperate with other attackers. See **ICMP flood**.*

Ping of death**Ping of death**

Type of an attack on a computer which includes an ICMP pack sent in error or an otherwise dangerous packet, e.g. a packet sent larger than the maximum size

of IP packet which collapses the target computer, or, by sending the packet the attacker exceeds the maximum size of IP packets which results in a failure of the system.

Port

It is used for communication using the TCP or UDP protocols. It defines the individual net applications running on one computer. It may take on values in the range 0 – 65535. For example, web pages are usually accessible on port 80, server to send out electronic mail on port 25, ftp server on port 21. These values may be changed and with some network services the administrators sometimes set other than normally used port numbers in order to deceive a potential attacker.

Port Knocking

Denotes a method in computer networks how to gain access from an untrusted computer into a computer or computer network protected by a firewall, without the need to sign on with the computer protected by a firewall and change the setting like an administrator. This way creates a semblance that the firewall is closed to untrusted computers and yet gives a chance of changing the setting by a special secret sequence. The method bypasses abuse of security errors in programmes serving permanently open ports.

Port scanner

Programme to test open ports.

Port**Klepání na porty****Port scanner****Portal**

Information (content regions, pages, applications, and data from external sources) concentrated in one central place which can be accessed using a web browser.

Portál**Pretexting**

One kind of social engineering. It creates and uses fictitious screenplay with the objective of convincing the victim to perform the required action, or to obtain the required information.

Pretexting**Pretty good privacy (PGP)**

Mechanism/programme enabling encryption and signature of data. Most typically it is used for encrypting the content of messages (emails) and for providing these messages with an electronic signature.

Dost dobré soukromí**Privacy**

Privacy is the capability or right of an individual or group to retain information

Soukromí

about themselves. Privacy is also the material or mental space of the subject.

Private IP address

Groups of IP addresses defined under RFC 1918 as reserved for use in internal networks. These IP addresses are not routed from the internet. Here are these ranges: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255 and 192.168.0.0 – 192.168.255.255.

Problem

Primary cause of one or more incidents.

Procedure

Specified manner of executing an activity or process.

Process

Set of mutually related or mutually influencing activities transforming inputs into outputs/

Program

Syntactic unit satisfying the rules of a certain programming language; it consists of descriptions (declarations) and commands or instructions necessary to fulfil some function or solve some task or problem.

Protocol

Agreement or standard which controls or enables a link, communication and data transfer among computers, in general among end devices. Protocols can be implemented by hardware, software, or a combination of both.

Proxy trojan

Masks other computers as infected. Enables the attacker to abuse the infected computer for an access to other computers in the network and thus aids the attacker to hide its identity.

Public domain software

Software that has been placed in the public domain, in other words there is absolutely no ownership such as copyright, trademark, or patent.

Public information system

Information system providing services to the public and having relations to information system of the public administration.

Privátní IP adresa**Problém****Postup****Proces****Program****Protokol****Proxy trojan****Software veřejné domény****Veřejný informační systém**

Public IP address**Veřejná IP adresa**

*IP address which is routable in the **Internet**. Such an address is then accessible from the whole **Internet** network unless prohibited for example by **firewall** or router configuration.*

Public Key Infrastructure (PKI)**Infrastruktura veřejných klíčů**

This in cryptography denotes infrastructure for the management and distribution of public keys from asymmetric cryptography. PKI, thanks to transfer of confidence, enables the use of unfamiliar public keys for the verification of electronic signature without having to verify each individually. The transfer of confidence can be implemented either by means of the certification authority (X.509) or by trusted network (e.g. PGP).

Public sector portal**Portál veřejné správy**

Information system created and operated with the intention of facilitating remote access to, and communication with, the necessary information from the public administration.

Public telecommunication network**Veřejná komunikační síť**

Network of electronic communications serving wholly or predominantly to provide publicly available services of electronic communications and which supports information transfer among the endpoints of the network, or a network of electronic communications through which radio and television broadcast are provided as a service.

Public telephone network**Veřejná telefonní síť**

Network of electronic communications to provide publicly available telephone services and which allows for the transmission of voiced speech as well as other forms of communications, such as facsimiles and data transmissions, among the endpoints of the networks.

Publicly available electronic communications service**Veřejně dostupná služba elektronických komunikací**

Service of electronic communications from whose use no one may be a priori excluded.

Ransom ware**Ransomware**

Programme which encrypts data and offers to decrypt them after a ransom payment (e.g. a virus, Trojan horse).

Record**Záznam**

Document with the record of achieved results or in which proofs about completed activities are provided.

Recovery point objective (RPO)**Bod obnovy dat**

Point in time when data must be recovered after a breakdown.

Recovery time objective (RTO)**Doba obnovy chodu**

Time period during which a minimal level of services and/or products and support systems, applications or functions, must be recovered after a disaster.

Re-dial, Pharming crime ware**Přesměrovávače**

Programmes (subset of Malware) whose task is to redirect users to certain pages instead of those originally intended to be visited. On these pages there is an installation of other Crimeware (virus), or there is a substantial increase in the Internet connection fee (using telephone lines with a higher rate).

Redundancy**Redundance**

General meaning is redundancy, abundance. In IT it is used in the sense of backup. For example, a redundant (backup) power supply, redundant (backup) data.

Regional internet registry (RIR)**Regionální Internetový Registr**

Organization looking after the assignment of public IP address ranges, autonomous systems in its geographical scope. There are five RIRs at present: RIPE NCC – Europe and Near East, ARIN – USA and Canada, APNIC – Asia – Pacific Region, LACNIC – Latin America, AfriNIC – Africa.

Release**Uvolnění**

Aggregate of one or more new or changed configuration items which are put into the operational environment as the result of one or more changes.

Reliability**Spolehlivost**

Attribute of consistent intentional behaviour or results.

Replay, replay attack**Replay, replay útok**

Situation when a copy of a legitimate transaction (data sequence) is intercepted, repeatedly replayed by an unauthorized subject usually with illegal intent (e.g. to open a car with a central lock).

Request**Dotaz**

Request for information, in general as a formal request sent to a database or to a browser, or a signal from one computer to another, or to a server with the request for concrete information or data item.

Request for comment (RFC)

It is used to denote standards describing internet protocols, systems and other items related to internet operation. For example, RFC 5321 describes the SMTP protocol for the exchange and processing of electronic mail.

Request for change

Proposal to make a change of a service, element of a service or a system of service control.

Residual data

Data left behind in a data medium after the erasure of a file or part of it. It need not be, however, only data left after the erasure of disc files, unwanted residual data can be left on the local computer, for example, even by work using a remote connection (VPN). It could be data collected (into a cache), for example, of an application.

Residual risk

Risk remaining even after an application of the appropriate measures.

Resilience

Capability of an organization, system or network to resist threats and brace itself against the influence of outages.

Review

Activity done in order to assess the suitability, adequacy and efficiency of the analysed subject to achieve set objectives.

Risk

(1) Danger, possibility of damage, loss, failure. (2) Effect of uncertainty to achieve objectives. (3) Possibility that a certain threat would utilize vulnerability of an asset or group of assets and cause damage to an organization.

Risk acceptance

Decision to accept risk.

Risk analysis

Process of understanding the nature of risks and establishing a risk level.

Risk assessment

Overall process of risk identification, risk analysis and risk assessment.

Request For Comment (RFC)**Žádost o změnu****Zbytková data****Zbytkové riziko****Odolnost****Přezkoumání****Riziko****Přijetí rizika****Analýza rizik****Posuzování rizika**

Risk attitude

Approach of an organization towards assessing risk and, also, dealing with risk, sharing risk, taking over or refusal of risk.

Postoj k riziku**Risk avoidance**

Decision not to allow an involvement into risk situations, or to exclude these.

Vyhnutí se riziku**Risk communication**

Exchange or sharing of information between the decision-maker and other participating parties.

Komunikace rizika**Risk criteria**

Reference values of parameters which are used to assess risk severity.

Kritéria rizika**Risk estimation****Odhad rizika**

Process to determine values of probability and consequences of risk.

Risk evaluation**Hodnocení rizik**

Process to compare the results of risk analyses with risk criteria to find out if the risk level is acceptable.

Risk identification**Identifikace rizik**

Process of looking for, recognizing, and describing risks.

Risk management**Řízení rizik**

Coordinated activities to manage and control an organization in view of the risks.

Risk management framework**Rámec řízení rizik**

Set of components providing the fundamentals and organizational arrangement for the design, implementation, monitoring, re-analysis and continuous improvement of risk management in the whole organization.

Risk management plan**Plán řízení rizik**

Scheme in the framework of risks specifying access, parts of management and sources to be used for risk management.

Risk management policy**Politika řízení rizik**

Statement on the overall intentions and direction of an organization related to risk management.

Risk management process

Systematic implementation of management policies, procedures and well-established practices for the activities of sharing, consulting, context setting, and finding out, analyzing, evaluating, treating, monitoring and cross-checking risks.

Risk owner

Person or entity with the responsibility and authority to control risk and monitor events which cause the risk.

Risk profile

Description of any set of risks.

Risk reduction

Activity to lower the probability and lessen negative consequences, or both of these parameters linked to risk.

Risk retention

Accepting the burden of a loss or benefit from profit ensuing from a certain risk.

Risk source

Element, which either alone or in combination with other elements, has the internal capability to cause a risk.

Risk transfer

Sharing of costs with another party or sharing of benefits from profit flowing from risk.

Risk treatment**Zvládání rizika, ošetření rizika**

Process to modify (change) a risk.

Role**Role**

Aggregate of specified activities and necessary authorizations for a subject operating in the information or communication system.

Rootkit**Rootkit**

Programmes making it possible for insidious software to mask its presence in a computer. Thus they can hide from the user selected running processes, files on disc or other system data. They exist for Windows, LINUX and UNIX.

Sandbox

Security mechanism serving to separate running processes from the operating system proper. It is used, for example, in testing suspicious software.

Script

Set of instructions written in some formal language which control the workings of devices, programme or system.

Sector criteria

Technological or operational values to determine an element of critical infrastructure in the sectors of energy, water management, food and agriculture, health, transport, communication and information systems, finance market and currencies, emergency services and public administration.

Secure shell (SSH)

A protocol that provides secure remote login utilising an insecure network.

Secure socket layer (SSL)

Protocol or a layer inserted between the transport layer (e.g. TCP/IP) and the application layer (e.g. HTTP) which enables communication security by encryption and authentication of the communicating parties.

Security

Property of an element (e.g. an information system) which is at a certain level protected against losses, or also a state of protection (at a certain level) against losses. IT security covers protection of confidentiality, integrity and availability during processing, storage, distribution and presentation of information.

Security account manager

Administrator for securing the accounts in the Windows operating system, e.g. a database, where user passwords are kept (passwords in Windows NT operating system may be kept, for example, in the directory c:\winnt\repair and c:\winnt\config).

Security aims

State of security which the given system or product has to reach.

Security audit

Independent revision and analysis of records in the data processing system as well as activities for testing of the suitability of system controls, checking compliance with accepted security policy and operational procedures, detection

Sandbox

Security mechanism serving to separate running processes from the operating system proper. It is used, for example, in testing suspicious software.

Skript

Set of instructions written in some formal language which control the workings of devices, programme or system.

Odvětvová kritéria

Technological or operational values to determine an element of critical infrastructure in the sectors of energy, water management, food and agriculture, health, transport, communication and information systems, finance market and currencies, emergency services and public administration.

Secure shell (SSH)

A protocol that provides secure remote login utilising an insecure network.

Secure socket layer (SSL)

Protocol or a layer inserted between the transport layer (e.g. TCP/IP) and the application layer (e.g. HTTP) which enables communication security by encryption and authentication of the communicating parties.

Bezpečnost

Property of an element (e.g. an information system) which is at a certain level protected against losses, or also a state of protection (at a certain level) against losses. IT security covers protection of confidentiality, integrity and availability during processing, storage, distribution and presentation of information.

Správce zabezpečení účtů

Administrator for securing the accounts in the Windows operating system, e.g. a database, where user passwords are kept (passwords in Windows NT operating system may be kept, for example, in the directory c:\winnt\repair and c:\winnt\config).

Bezpečnostní cíle

State of security which the given system or product has to reach.

Bezpečnostní audit

Independent revision and analysis of records in the data processing system as well as activities for testing of the suitability of system controls, checking compliance with accepted security policy and operational procedures, detection

of security infringements and recommendation for any indicated changes in the control, security policy and procedures. Independent testing of the information system activity and records thereof. The objective is to determine if checks are appropriate, if there is compliance with security policy, recommendation of eventual changes in the system of countermeasures. As rule is, it is done by an external or an internal auditor.

Security authority**Bezpečnostní autorita**

Entity responsible for the administration of security policy within the security domain.

Security category**Bezpečnostní kategorie**

Grouping of sensitive information used when controlling data access.

Security classification**Bezpečnostní klasifikace**

Determination which level of protection for data or information is required before access, together with noting this level of protection.

Security clearance**Bezpečnostní prověření**

Clearance given to an individual for accessing data or information on or below the specified security level.

Security domain**Bezpečnostní doména**

Group of users and systems subject to common security policy.

Security event**Bezpečnostní událost**

Event which may result in or cause the infringement of information systems and technologies and rules defined for the protection (security policy).

Security filter**Bezpečnostní filtr**

Trusted computer system enabling security policy for data passing through the system.

Security incident**Bezpečnostní incident**

Infringement or an imminent threat of infringement, of security policies, security principles or standard security rules of operation for the information and communication technologies.

Security information and event management (SIEM)

System whose task is to acquire, analyse and correlate data – events in the network. SIEM systems combine the methods of detection and analysis of abnormal events in the network, provide information usable for network management and operated services.

Security level

Combination of a hierachic security classification and security category, representing sensitivity of an object or security clearance of an individual.

Security manager

Employee role to act as a guarantee for IT security with the definition of responsibility and authority.

Security policy

(1) At the level of an organization, basic document which defines the structure of security risk, responsibility for information protection within an organization, level of information protection. (2) At the system level, a set of rules and practices specifying or regulating how the system (or organization) provides security services in order to protect sensitive or critical system resources.

Security requirements

Requirements put on the information system which follow from laws, instructions, legal amendments, binding standards, internal regulations of an organization; environment where the system operates and the mission it fulfils; necessary for ensuring confidentiality, availability and integrity of information processed in the system.

Security safeguards

Protective measures to ensure security requirements put on the system. May vary in character (physical protection of equipment and information, personnel security – checking of employees, organizational measures – operational rules, and similar).

Security software disabler

It blocks software to secure the PC (Firewall, Antivirus).

Security standards

Set of recommendations and general principles to define, maintain and improve information security inside an organization.

Management bezpečnostních informací a událostí (SIEM)**Bezpečnostní úroveň****Bezpečnostní manažer****Bezpečnostní politika****Bezpečnostní požadavky****Bezpečnostní opatření****Security software disabler****Bezpečnostní standardy**

Security vulnerability

Intentional error or unintended defect or software error in general or in firmware of the communication infrastructure equipment which may be used by a potential attacker for harmful activity. These vulnerabilities are either known or published but yet untreated by the manufacturer, or hidden and undetected. In case of hidden vulnerabilities it is important whether these are detected sooner by the attacker, manufacturer, security analyst or user. Security vulnerabilities are therefore potential security threats. Security vulnerabilities can be eliminated by consequential security patches for the system.

Sensitive data

Protected data having fundamental importance for the operation of an organization. Its leakage, abuse, unauthorized alteration or unavailability would mean damage to the organization, or, as the case may be, the organization would be unable to meet its objectives.

Sensitive information

Information which, on the basis of a decision by the relevant authority, must be protected, because access to it, modification, destruction, or loss would cause a substantial damage to someone or something.

Sensitivity

Measure of importance assigned to information by the owner of the information, describing the need for protection.

Server cluster

Group of network servers used to increase the efficiency of internal processes by distributing load among individual linked components in order to speed up computing processes by using the power of more servers. When one server in the farm fails, another one can replace it.

Service

Activity of the information system meeting the given requirements of an authorized subject related to the function of the operating system.

Service component

Independent component of a service which, when united with other components provides the whole service.

Service continuity

Capability to manage risks and events which could seriously impact services,

Bezpečnostní zranitelnost**Citlivá data****Citlivá informace****Citlivost****Serverová farma****Služba****Prvek služby****Kontinuita služeb**

with the objective of providing continuous services at the agreed levels.

Service level agreement (SLA)

Documented agreement between the service provider and the customer which defines services and their parameters.

Service level declaration (SLD)

*Specification of offered services which can change on the basis of individual agreements according to the actual needs of individual customers. Hence, a more detailed SLA. See **SLA**.*

Service management

Set of capabilities and processes to manage and control the activities and sources of the service provider for the design, handover, delivery and improvement of services so that the requirements placed on them be met.

Service pack

Collection (pack) of several updates which could all be installed at the same time.

Service provider

Any natural or legal person providing some of the services of the information society.

Service request

Request for information, advice, access to service, or for a previously agreed change.

Service requirement

Needs of customers and users of services, including requirements for the service level and the needs of a service provider.

Service set identifier (SSID)

Unique identifier (name) of every wireless (WiFi) computer network.

Sexting

Electronic distribution of text messages, photographies or videos with a sexual content. These materials often originate in partner relations. Such materials, however, may represent a risk that one partner, out of various motives, would publish photographies or videos of the other partner.

Dohoda o úrovni služeb (SLA)**Prohlášení o úrovni služeb****Řízení služeb****Aktualizační balík****Poskytovatel služby****Žádost o službu****Požadavky na službu****Service set identifier (SSID)****Sexting**

Shareware

Freely distributed software protected by copyright. In case the user decides to use this software longer than the author permits, the user is obliged to satisfy conditions for use. These can be, for example, payment of a certain financial amount, user registration, etc.

Sharing

Possibility to have a portion at the same time of one or more information sources, memory or devices.

**Simple mail transfer protocol
(SMTP)**

Internet protocol for the transmission of messages of electronic mail. It describes communication among mail servers.

Simulation

Use of a data processing system to extract selected properties in the behaviour of a physical or abstract system.

Sniffer

Programme for the eavesdropping of all the protocols which a computer receives/sends (it is used, for example, for eavesdropping of access names or passwords, numbers of credit cards).

Social engineering

Way of people manipulation in order to perform a certain action or to obtain a certain information.

Social network

Interconnected group of people who interact. It is formed on the basis of interests, family ties or other reasons. This idea is at present often used in connection with internet and the onset of webs which are directly targeted at social networks (Facebook, Lidé.cz etc.), social networks can also form in interest communities around certain web sites, for example at their forums.

Software

Set of programmes used in a computer which execute data processing or a concrete task. Software can be further subdivided into: a) system software – input/output devices, operating systems or graphics operation systems; b) application software – applications, simple utilities or complex programming systems; c) firmware – hardware control programme.

Shareware**Sdílení****Simple mail transfer protocol
(SMTP)****Simulace****Sniffer****Sociální inženýrství****Sociální síť****Software (programové vybavení)**

Software piracy

Unauthorized use, copying or distribution or software.

Spam

Unsolicited mail such as commercials, or another unsolicited message, usually of a commercial character, which is distributed on the Internet. Most often these are offers for aphrodisiacs, medicaments or pornography. Unless the system is adequately protected, unsolicited mail can make up a substantial part of electronic correspondence.

Spamming

Mass distribution of unsolicited messages by electronic means – most often by electronic mail.

Spear phishing

*More sophisticated attack than **Phishing**, which uses prior obtained information about the victim. Thanks to a more focused targeting on a concrete user this method attains higher effect than a standard attack of the **Phishing** type. See **Phishing**.*

Spoofing**Úmyslné oklamání, podvržení**

Activity with the objective of deceiving (misleading) a user or operator usually by sporting a false identity.

Spyware

Programme which secretly monitors the behaviour of an authorized computer or system user. The findings are sent by these programmes continuously (e.g. at every start-up) to the subject which created the programme or distributed it. Such programmes are frequently installed on the target computer together with another programme (utility, computer game), however, they bear no relation to it.

SQL injection

Injection technique which abuses security errors occurring in the database layer of an application. This security error manifests itself by infiltrating unauthorized characters into an SQL command of an authorized user, or by taking over user access, to execute the SQL command.

State of cyber danger

Under cyber danger we understand such a state when there is a large measure of danger to information security in information systems or security of services

Softwarové pirátství**Nevyžádaná pošta****Hromadné rozesílání nevyžádané pošty****Spear phishing (rybaření oštěpem)****Úmyslné oklamání, podvržení****Spyware****SQL injection****Stav kybernetického nebezpečí**

or of electronic communications.

Statement of applicability

Documented statement describing the objectives of measures and the measures which are relevant and applicable for the ISMS of a given organization.

Stealth

Prevention or limitation of object's identification.

Structured query language (SQL)**Structured query language (SQL)**

Standard query language used to work with data in relational databases.

Stuxnet

Computer worm created to attack industrial control systems of the SCADA type used to control large industrial enterprises, for example factories, power generating plants, product lines and even military objects.

Subject

In computer security, an active entity which can access objects.

Subject of critical infrastructure**Subjekt kritické infrastruktury**

Operator of an element of critical infrastructure; if it is an operator of an element of the European critical infrastructure, the operator is considered to be a subject of the European critical infrastructure.

Supervisory control and data acquisition (SCADA)**Dispečerské řízení a sběr dat (SCADA)**

Computer system for the dispatcher control and data acquisition. It could be industrial control systems, or computer systems for monitoring and process control. The processes could be industrial ones (e.g. electrical energy generation, manufacture and purification of fuel), infrastructural (e.g. treatment and distribution of drinking water, taking away and purification of sewage, oil and gas pipes, civilian systems of antiaircraft defence – sirens, and large communication systems), and facilities (e.g. airports, railway stations and hubs).

SYN-cookies**SYN-cookies**

Element of defence against a flooding by packets in the TCP protocol with the attribute SYN. See SYN-Flood.

SYN-flood**SYN-flood**

Cyber attack (Denial of Service type) on a server by flooding with packets in the

TCP protocol. The attacker sends a flood of **TCP/SYN** packets with a forged heading of the sender. The server accepts every such packet as a normal request for a connection. Server then sends out the **SYN-ACK** packet and waits for the **ACK** packet. This however never arrives as the heading of the sender was forged. Such a semi-open request blocks out, for some time, other legitimate requests for a connection. See **DOS, DDOS, SYN-cookie**.

System administrator**Správce systému**

Person responsible for the management and maintenance of a computer system.

System Integrity**Integrita systému**

Quality of a data processing system fulfilling its operational purpose and at the same time preventing unauthorized users from making changes in resources or from using the resources or from improper use of these. Property that a system performs its intended function without disruption, without intentional or accidental non-automated system manipulation.

TCP SYN flood**Zahlcení TCP SYN**

Type of a **DDOS** attack, it sends a flood of **TCP/SYN** packets with a forged heading of the sender. Each such packet is accepted by the server as a normal request for a connection. Server then sends out a **TCP/SYN-ACK** packet and waits for **TCP/ACK**. This however never arrives as the user heading was forged. Thus a half-open request blocks, for some time, other legitimate requests for a connection.

TERENA**TERENA**

Trans-European Research and Education Networking Association, a European international organization supporting activities in the area of internet, infrastructures and services in the academic community.

TF-CSIRT**TF-CSIRT**

International forum enabling the cooperation of **CSIRT** teams on a European level. It is divided into two groups – a closed one which is open only to accredited teams, and an open one which is accessible to all parties interested in the **CSIRT** teams' work. **TF-CSIRT** is one of the activities of the **TERENA** international organization. Working group **TF-CSIRT** meets usually several times per year.

Third party**Třetí strana**

Person or organization independent both of the person or the organization which submits the object to be judged for compliance (product, service) and also independent of the purchaser of the object.

Threat

Potential cause of an unwanted incident which may result in damage to a system or organization.

Hrozba**Threat analysis**

Analysis of activities and events which could negatively affect IT service quality (system of data processing and transfer) and/or data proper.

Analýza hrozeb**Time bomb****Časovaná bomba**

Logical bomb activated at a predetermined time.

Top level domain (TLD)**Doména nejvyšší úrovně**

This is the internet domain at the highest level in the tree of internet domains. In the domain name, top level domain is given at the end (e.g. in nic.cz, cz is the top level domain). Top level domains are fixed by the internet standards organization IANA: a) National TLD (country-code TLD, ccTLD) unites domains in one country. Their name has two letters, with exceptions corresponding to country code per ISO 3166-1, e.g. cz for the Czech Republic; b) Generic TLD (generic TLD, gTLD) is common for a given type of subjects (e.g. aero, biz, com, info, museum, org,...) not tied to one concrete country (with exceptions TLD mil and gov which out of historical reasons are assigned for military and government computer networks in the U.S.A.); c) Infrastructure TLD used for the internal mechanisms of the internet. At present there is just one such TLD: arpa, used by the DNS system.

Top management**Vrcholové vedení**

Person or a group of persons who lead the organization at the highest level.

Torrent**Torrent**

This is a file with the ending .torrent which contains information about one or more files to be downloaded. See BitTorrent.

Traffic analysis**Analýza komunikace / datových přenosů**

Simple and advanced mathematical and visual methods for the analysis of data traffic TCP/IP in a computer network. See Analysis.

Transition**Přechod**

Activity related to a shift of new or altered service into or out of the operational environment.

**Transmission control protocol
(TCP)**

It is one of the basic protocols in the protocol set of the Internet; more precisely it represents the transport layer. Using the TCP, applications on interconnected computers can link up and transmit data over the links. The protocol guarantees a reliable delivery as well as delivery in the right order. TCP also differentiates data for multiple concurrently running applications (e.g. a web server and email server) running on the same computer. TCP is supported by many of the application protocols and applications popular on the internet, including WWW, email and SSH.

Transport layer security (TLS)

A cryptographic protocol that provide communication security over the Internet. They use asymmetric cryptography for authentication of key exchange, symmetric encryption for confidentiality and message authentication codes for message integrity. Several versions of the protocols are in widespread use in applications such as web browsing, electronic mail, Internet faxing, instant messaging and voice-over-IP (VoIP).

Transport layer security (TLS)

A cryptographic protocol that provide communication security over the Internet. They use asymmetric cryptography for authentication of key exchange, symmetric encryption for confidentiality and message authentication codes for message integrity. Several versions of the protocols are in widespread use in applications such as web browsing, electronic mail, Internet faxing, instant messaging and voice-over-IP (VoIP).

Trojan horse

Programme which executes a useful function, taken at face value, but in reality has also some hidden harmful function. Trojan horse does not self-replicate, it is distributed thanks to the visible utility it provides.

Trusted computer system

Data processing system having sufficient computer security to allow for a concurrent access to data to users with different access rights and to data with different security classification and security categories.

Trusted introducer

Authority uniting European security teams of the type CERT/CSIRT. At the same time it also helps in creating the CERT/CSIRT teams and provides for their accreditation and certification. It is operated by the TERENA organization. See TERENA.

**Transmission control protocol
(TCP)****Bezpečnost transportní vrstvy****Transport layer security****Trojský kůň****Důvěryhodný počítačový systém****Trusted introducer**

UDP flood

*This is a type of an attack using the User datagram protocol (**UDP**). The attacker sends out an unspecified number of packets to a random port of the system of the victim. Receiving system of the victim is unable to determine which application requested such a packet, which generates an **ICMP** packet of undeliverability of the **UDP** packet. If more **UDP** packets arrive in the receiving port of the victim, the system may collapse.*

Uniform resource locator (URL)**Uniform resource locator (URL)**

Source identifier describing the location of a concrete source, including a protocol, serving to link to this source. The best known such an example is <http://www.somedomain.somewhere>.

Universal unique identifier (UUID)**Universální unikátní identifikátor**

*An identifier standard used in software construction, standardized by the Open Software Foundation (**OSF**) as part of the Distributed Computing Environment (**DCE**).*

URL trojan**URL trojan**

*It redirects infected computers connected via the dial-in Internet connection to more expensive rates. See **Dialer** and **Trojan horse**.*

User**Uživatel**

Any natural or legal person using a service of the information society in order to look for, or make access to, information.

User datagram protocol (UDP)**User datagram protocol (UDP)**

An Internet networking protocol for connectionless communications (RFC 768).

User identification**Identifikace / ID uživatele**

Character string or a formula used by a data processing system for user identification.

User profile**Uživatelský profil**

Description of a user typically used for access control. It may include data such as user ID, user name, password, access rights and other attributes.

Virtual local area network (VLAN)**Virtuální lokální síť**

*Logically independent network in the framework of one or more devices. Virtual networks can be defined as the domains of all-directional broadcast (See **LAN**) with the objective of making the logical network organization independent of the physical network.*

Virtual private network (VPN)**Virtuální privátní síť**

This is a private computer network allowing for the connection of remote users to the targeted LAN via the Internet. Security is tackled using an encrypted tunnel between two points (or among one and several points). Identity of both parties is verified using digital certificates when making the connection.

Virus**Virus**

Type of malware spreading from one computer to another by attaching itself to other applications. Consequently it may cause unwanted and dangerous activity. Usually it has a built-in mechanism for further distribution or mutations.

Virus analysis**Analýza počítačového viru**

Complex activity including the analysis of computer virus behaviour (how it spreads, hides, damage caused by the virus), analysis of virus code, finding of the virus and its removal from files, or rectification of damage caused by the virus. More also in disassembly, debugger, tracing, code emulation.

Virus signature**Charakteristika viru (signatura viru)**

Unique bit string which sufficiently identifies the virus and which can be used by a scanning programme to detect virus presence.

Vulnerability**Zranitelnost**

Weak spot of an asset or control which can be made use of by a threat.

Vulnerability analysis**Analýza zranitelnosti**

Systematic analysis of a system and operating services in view of security weaknesses and the efficiency of security measures.

Vulnerability assessment**Hodnocení zranitelností**

Process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.

Vulnerability assessment and**Hodnocení zranitelností a řízení****vulnerability management (VA/VM)****zranitelností (VA/VM)**

See Vulnerability assessment and Vulnerability management.

Vulnerability management**Řízení zranitelností**

Cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities. This practice generally refers to software vulnerabilities in computing systems however it can also extend to organizational behaviour and strategic decision-making processes.

Wardriving

Searching for insecure wireless Wi-Fi networks by a person sitting in a means of transport, using a notebook, PDA or smartphone.

Warez

Term from the computer slang denoting copyright-protected creations which are treated in violation of the copyright. Warez is sometimes split into gamez (computer games), appz (applications), crackz (cracks) and also moviez (films). Today, the most frequent way of distribution is mainly the Internet.

Watchdog timer

An electronic timer that is used to detect and recover from computer malfunctions. During normal operation, the computer regularly restarts the watchdog timer to prevent it from elapsing, or "timing out". If, due to a hardware fault or program error, the computer fails to restart the watchdog, the timer will elapse and generate a timeout signal. The timeout signal is used to initiate corrective action or actions. The corrective actions typically include placing the computer system in a safe state and restoring normal system operation.

Web vandalism

Attack which alters (defaces) web pages or causes a service denial (denial-of-service attacks).

Webtapping

Monitoring of web pages which may contain classified or sensitive information, and of people, who have access to them.

White hat

Ethical hacker who is often employed as an expert in computer security, programmer or network administrator. He or she specializes on penetration tests and other testing methodologies to ensure IT security in an organization.

Whois

Internet service to find contact data of the owners of internet domains and IP addresses.

WiFi

Wireless technology for data distribution ("by air"), suitable for the creation of network infrastructures in places where the building of a classical cable network is impossible, difficult or not cost-effective (cultural monuments, sports facilities, fair grounds). Suitably located successive points of access along the route from

Wardriving

Searching for insecure wireless Wi-Fi networks by a person sitting in a means of transport, using a notebook, PDA or smartphone.

Warez

Term from the computer slang denoting copyright-protected creations which are treated in violation of the copyright. Warez is sometimes split into gamez (computer games), appz (applications), crackz (cracks) and also moviez (films). Today, the most frequent way of distribution is mainly the Internet.

Časový hlídáč

An electronic timer that is used to detect and recover from computer malfunctions. During normal operation, the computer regularly restarts the watchdog timer to prevent it from elapsing, or "timing out". If, due to a hardware fault or program error, the computer fails to restart the watchdog, the timer will elapse and generate a timeout signal. The timeout signal is used to initiate corrective action or actions. The corrective actions typically include placing the computer system in a safe state and restoring normal system operation.

Webový vandalizmus

Attack which alters (defaces) web pages or causes a service denial (denial-of-service attacks).

Odposlech webu

Monitoring of web pages which may contain classified or sensitive information, and of people, who have access to them.

White hat

Ethical hacker who is often employed as an expert in computer security, programmer or network administrator. He or she specializes on penetration tests and other testing methodologies to ensure IT security in an organization.

Whois

Internet service to find contact data of the owners of internet domains and IP addresses.

WiFi

Wireless technology for data distribution ("by air"), suitable for the creation of network infrastructures in places where the building of a classical cable network is impossible, difficult or not cost-effective (cultural monuments, sports facilities, fair grounds). Suitably located successive points of access along the route from

the transmitter to the recipient are sufficient for data transmission.

WiMax

Telecommunication technology providing wireless data transmission using various transmission modes, from point-to-multipoint to completely mobile internet access for the transmission.

Wireshark

*Formerly **Ethereal**. Protocol analyzer and packet sniffer which enables eavesdropping of all protocols which the computer receives and sends via an interface. Wireshark can decode the whole packet and show it in a way as sent out by the computer. Its advantage is that it is distributed under a free licence **GNU/GPL**.*

Wiretapping

This is any tapping of a telephone transmission or conversation done without the consent of both parties, by accessing the telephone signal proper.

Workstation

Functional unit, usually with specific computing capabilities, having user input and output devices, e.g. a programmable terminal or a stand-alone computer.

World wide web (WWW)

*Graphically-oriented service of the **Internet** – a system of interconnected hypertext pages using formatted text, graphics, animation and sounds.*

Worm

*Autonomous programme (subset of **Malware**) capable of creating its copies which it then sends out to other computer systems (networks) where these pursue further activities they have been programmed for. Often it may serve to detect security holes in systems or mail programmes.*

X.509

*Standard for systems based on the public key (**PKI**) for simple signatures. X.509 specifies, for example, the format of a certificate, lists of cancelled certificates, parameters of certificates and methods for checking the validity of certificates.*

Zombie

Infected computer which is part of botnet networks.

WiMax**Wireshark****Odposlech****Pracovní stanice****World wide web (WWW)****Červ****X.509****Zombie**

Notes:

Použité zkratky / Abbreviations used

Zkratka Abbreviation	Česky	English
ACI	Informace řízení přístupu	Access control information
ACL	Seznam pro řízení přístupu	Access control list
APT	Pokročilá a trvalá hrozba	Advanced persistent threat
ARP	Protokol ARP	Address resolution protocol
ASIM	Automatické monitorování výskytu bezpečnostního incidentu	Automated security incident measurement
BCM	Řízení kontinuity organizace	Business continuity management
BCMS	Systém řízení kontinuity organizace	Business continuity management system
BIOS	Základní vstupně-výstupní systém	Basic input output system
BSOD	Modrá obrazovka smrti	Blue screen of death
CA	Certifikační autorita	Certification authority
CAPTCHA	Zcela automatizovaný veřejný počítače od lidí	Completely automated public Turing test to tell computers from humans
CAS	Systém řízeného přístupu	Controlled access system
CC	Creative commons	Creative commons
CERT	Skupina pro reakci na počítačové hrozby	Computer emergency response team
CI	Konfigurační položka	Configuration item
CIRC	Schopnost pro reakci na počítačové hrozby	Computer incident response capability
CMDB	Konfigurační databáze	Configuration management database
CNA	Útok na počítačovou síť	Computer network attack
CNE	Vytěžování počítačové sítě	Computer network exploitation
COMPUSEC	Počítačová bezpečnost	Computer security
COMSEC	Bezpečnost komunikací	Communication security
CSIRT	Skupina pro reakce na	Computer security incident

	počítacové bezpečnostní incidenty	response team
CZE	Česká republika	Czech Republic
ČR	Česká republika	Czech Republic
DCE	Distribuované výpočetní prostředí	Distributed computing environment
DDOS	Distribuované odmítnutí služby	Distributed denial of service
DMZ	Demilitarizovaná zóna	Demilitarized zone
DNS	Systém doménových jmen	Domain name system
DNSSEC	Bezpečnostní rozšíření systému doménových jmen	Domain name system security extensions
DOS	Odmítnutí služby	Denial of service
DPI	Podrobná inspekce paketů	Deep packet inspection
ENISA	Agentura pro elektronickou a informační bezpečnost	European network and information security agency
EU	Evropská unie	European union
FIRST	Fórum pro bezpečnostní týmy	Forum for incident response and security teams
FTP	Protokol pro přenos souborů	File transfer protocol
H4H	Hackers for hire	Hackers for hire
HTTP	Protokol pro přenos hypertextových dokumentů	Hypertext transfer protocol
HTTPS	Bezpečnostní nadstavba protokolu pro přenos hypertextových dokumentů	Hypertext transfer protocol secure
IANA	Úřad pro přidělování čísel na Internetu	Internet assigned numbers authority
ICANN	Internetová společnočnost pro přidělování jmen a čísel na internetu	Internet corporation for assigned names and numbers
ICMP	Internet control message protocol	Internet control message protocol
ICT	Informační a komunikační technologie	Information and communication technology
IDS	Systém detekce průniku	Intrusion detection system
INFOSEC	Bezpečnost informací / informačních systémů	Information security

IO	Informační operace	Information operation
IP	Internet protokol	Internet protocol
IPS	Systém prevence průniku	Intrusion prevention system
IRC	Internetové směnové povídání	Internet relay chat
IS	Informační systémy	Information systems
ISMS	Systém řízení bezpečnosti informací	Information security management system
ISP	Poskytovatel služeb internetu	Internet service provider
IT	Informační technologie	Information technology
LAN	Lokální síť	Local area network
LIR	Lokální internetový registr	Local internet registry
MBCO	Minimální úroveň chodu organizace	Minimum business continuity objective
MITM	Člověk uprostřed	Man in the middle
NAT	Překlad síťových adres	Network address translation
NATO	Severoatlantická aliance	North Atlantic Treaty Organization
NATO CCD COE	Kooperativní špičkové centrum kybernetické obrany NATO	NATO Cooperative cyber defence centre of excellence
NATO CDMA	Výkonný úřad kybernetické obrany NATO	NATO Cyber defence management authority
NBAD	Detekce anomálního chování sítě	Network behavior anomaly detection
NCIRC TC	NATO CIRC – Technické centrum	NATO computer incident response capability – Technical centre
NNEC	NATO Network Enabled Capability	NATO Network Enabled Capability
OSE	Otevřené bezpečnostní prostředí	Open security environment
OSF	Open software foundation	Open software foundation
P2P	Rovný s rovným	Peer to peer
PC	Osobní počítač	Personal computer
PGP	Dost dobré soukromí	Pretty good privacy
PKI	Infrastruktura veřejných klíčů	Public key infrastructure
RF	Rádiové vlny	Radio frequency
RFC	Request for comment	Request for comment
RIR	Regionální Internetový Registr	Regional internet registry
RPO	Bod obnovy dat	Recovery point objective

RTD	Doba obnovy chodu	Recovery time objective
SCADA	Dispečerské řízení a sběr dat	Supervisory control and data acquisition
SIEM	Management bezpečnostních informací a událostí	Security information and event management
SLA	Dohoda o úrovni služeb	Service level agreement
SLD	Prohlášení o úrovni služeb	Service level declaration
SMS	Systém řízení služeb	Service management system
SMTP	Simple mail transfer protocol	Simple mail transfer protocol
SQL	Structured query language	Structured query language
SŘBI	Systém řízení bezpečnosti informací	Information security management system
SSH	Secure shell	Secure shell
SSID	Service set identifier	Service set identifier
SSL	Secure socket layer	Secure socket layer
TCP	Transmission control protocol	Transmission control protocol
TERENA	Trans-evropská výzkumná a vzdělávací síťové fórum	Trans-European research and education networking association
TLD	Doména nejvyšší úrovně	Top level domain
TLS	Bezpečnost transportní vrstvy	Transport layer security
UDP	User datagram protocol	User datagram protocol
URL	Uniform resource locator	Uniform resource locator
UUID	Universální unikátní identifikátor	Universal unique identifier
VA/VM	Hodnocení zranitelností a řízení zranitelností	Vulnerability assessment and vulnerability management
VLAN	Virtuální lokální síť	Virtual local area network
VPN	Virtuální privátní síť	Virtual private network
WWW	World wide web	World wide web
XSS	Cross-site scripting	Cross-site scripting

Použité zdroje / Sources used

Česky	English
• ČSN EN ISO 9000:2006 Systémy managementu kvality – Základní principy a slovník	• ISO/IEC 9000:2006 Quality management systems – Fundamentals and vocabulary
• ČSN ISO 31000:2010 Management rizik – Principy a směrnice	• ISO 31000:2010 Risk management – Principles and guidelines
• ČSN ISO/IEC 27000:2010 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník	• ISO/IEC 27000:2010 Information technology – Security techniques – Information security management systems – Overview and vocabulary
• ISO/IEC 27000:2012 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník	• ISO/IEC 27000:2012 Information technology – Security techniques – Information security management systems – Overview and vocabulary
• ČSN ISO/IEC 27005:2009 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací	• ISO/IEC 27005:2009 Information technology – Security techniques – Information security risk management
• http://www.cybersecurity.cz/ ve verzi 25. 10. 2011 a 29. 2. 2012	• http://www.cybersecurity.cz/ in Version 25. 10. 2011 and 29. 2. 2012
• http://www.govcert.cz/ ve verzi 25. 10. 2011	• http://www.govcert.cz/ in Version 25. 10. 2011
• http://www.nic.cz/ ve verzi 01. 03. 2012	• http://www.nic.cz/ in Version 01. 03. 2012
• http://www.wikipedia.org/ ve verzi 01.03.2012	• http://www.wikipedia.org/ in Version 01.03.2012
• ISO/IEC 20000–1:2011 Informační technologie – Management služeb – Část 1: Požadavky na systém–řízení služeb	• ISO/IEC 20000–1:2011 Information technology – Service management – Part 1: Service management system requirements

- ISO/IEC 27003:2010 Informační technologie – Bezpečnostní techniky – Směrnice pro implementaci systému řízení informační bezpečnosti
- ISO/IEC 27031:2011 Informační technologie – Bezpečnostní techniky – Směrnice pro připravenost informační a komunikační technologie pro zabezpečení kontinuity organizace
- ISO/IEC 27033 – Informační technologie – Bezpečnostní techniky – Bezpečnost sítě
- ISO/IEC 27039 (návrh) – Informační technologie – Bezpečnostní techniky – Výběr, uvedení do chodu a provoz systémů pro zjištění vniknutí
- ISO/IEC 27032:2012 Informační technologie – Bezpečnostní technologie – Směrnice pro kybernetickou bezpečnost
- ITIL® výkladový slovník v češtině, v1.0, 29. července 2011 založen na výkladovém slovníku v angličtině v1.0 z 29. 7. 2011
- JTC1/SC27/SD6 Informační technologie – Bezpečnostní techniky – Stálý dokument 6 (SD6): Terminologický slovník IT bezpečnosti
- ISO/IEC 22301:2012 Společenská bezpečnost – Systémy řízení kontinuity organizace – Požadavky
- Kybernetická bezpečnost resortu obrany v letech 2011 až 2013: Pojmový aparát a seznam zkratek, Ministerstvo obrany
- ISO/IEC 27003:2010 Information technology – Security techniques – Information security management system implementation guidance
- ISO/IEC 27031:2011 Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity
- ISO/IEC 27033 – Information technology – Security techniques – Network security
- ISO/IEC 27039 (draft) – Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems
- ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity
- ITIL encyclopedic dictionary in Czech, v1.0, 29 July 2011, based on the encyclopedic dictionary in English v1.0, 29 July 2011
- JTC1/SC27/SD6 Information technology – Security techniques – Standing Document 6 (SD6): Glossary of IT Security Terminology
- ISO/IEC 22301:2012 Societal security – Business continuity management systems – Requirements
- Cyber security of the Defense Department between 2001 and 2013: Concepts and a list of abbreviations, MoD.

- Veřejně dostupné informace (Internet) • Public available sources (Internet)

© Jirásek, Novák, Požár, Praha 2013

Žádná část této publikace nesmí být kopírována a rozmnožována za účelem rozšiřování v jakékoli formě či jakýmkoli způsobem bez písemného souhlasu autorů.

No part of this publication may be copied or duplicated for distribution in any form or in any way without the written permission of the authors.

Výkladový slovník kybernetické bezpečnosti

Cyber Security Glossary

Vydal / Publisher:

Policejní akademie ČR &
Česká pobočka AFCEA

2013

Tištěný náklad / Print run: 700 ks / pcs.

Autoři / Authors:

Petr Jirásek, Luděk Novák, Josef Požár

Editoři / Editors:

Petr Jirásek, Milan Kný

Přeložil do angličtiny / English Translation:

Karel Vavruška

Policejní akademie ČR

Lhotecká 559/7, 143 01 Praha 4

<http://www.polac.cz>

Česká pobočka AFCEA

Dolnoměcholupská 12, 102 00 Praha 10

<http://www.afcea.cz>

ISBN 978–80–7251–397–0



*Druhá aktualizovaná verze slovníku je vydána
Policejní akademii ČR v Praze a Českou pobočkou AFCEA
pod záštitou
Národního centra kybernetické bezpečnosti České republiky a
Národního bezpečnostního úřadu České republiky.*



*The second updated version of the glossary is published by
Police academy of the Czech Republic in Prague and AFCEA Czech Republic
under the auspices of
National Cyber Security Centre of the Czech Republic and
National Security Authority of the Czech Republic.*



ISBN 978-80-7251-397-0
© Jirásek, Novák, Požár, Praha 2013