Řízení informační bezpečnosti

PV 017

Bezpečnost – Security

Stav, kdy se vlastník (aktiva, majetku) chová tak, aby na majetku nedocházelo ke škodám:

* úmyslným
* neúmyslným
* pasivním.

Musíme vědět, co se nesmí dělat a proti čemu se bránit.

Nelze se bránit proti něčemu, co:

* ještě neexistuje
* neznám

Bezpečnost (i bezpečí) je vždy ve stavu mezi 0 a 1.

Bezpečí – Safety

Nástroje security chrání proti ne/úmysl. událostem (fyzické, emoční, politické, finanční, duchovní, sociální, …) a dosáhnu tak bezpečí – safety.

Bezpečí – stav bytí v chráněné oblasti, která byla vytv­ořena nástroji bezpečnosti – security.

Ve stavu bezpečí (safety) se mohou nacházet inf. aktiva, lidé, majetek, …

Technologie: co je to

* je znalost, jak něco dělat
* je to aplikace věd. poznatků pro praktické účely

**Informační technologie:**

manipulace, zpracování, uchování, přenos informací

**Informace:** infce má hodnotu

<=> ten, kdo k ní má přístup má výhody proti tomu, kdo k ní nemá přístup

* hodnota infce:
  + je sdílitelná v rámci organizace
  + absentuje mimo organizaci.

**Cíl Inf. Bez**.: udržuje sdílitelnost uvnitř a absenci mimo

Informační bezpečnost

Je zaměřena na ochranu inf. aktiv. Zahrnuje:

* TG, standardy, politiky, procesy

**Koncept bezpečné informace**

<=>, pokud je zajištěná:

* ***důvěrnost*** (Confidentality)
  + přístup pouze oprávněným (autori­zo­vaným), zbránit neoprávněným
* ***celistvost*** (Integrity)
  + integrita dat – nesmí být neřízeně mě­ně­na (změna: úmyslná i ne­ú­my­slná)
* ***dostupnost*** (Availability)
  + zdrojů obecně: informací, služeb, HW sys­témů, komunikace, …

CIA je ovlivněna: technickými problémy, přírodou, lidmi – nejslabší článek

**Další pojmy:**

***autentizace***: ověř. identity uživ. služeb (osoba, SW) nebo původce zprávy. Metody: čím je, co má, co ví, co umí.

* ***autorizace*** následuje po autentizaci; autor. je proces povolení přístupu k inf., službám, HW, …
* prokazatelnost ??, nepopiratelnost ??

Protiklady a paradoxy uvnitř InfBez:

**Vlastnosti bitů**

* bity jsou všechny stejné
* snadno ho změním
* snadno ho zkopíruji

**Použitelnost technologií**

* používám chybující rozmanité TG
* ty použít i útočníci

**TG vs bezpečnost (i obecně)**

ISMS musí zohledňovat vlastní cíle organizace.

V zásadě to jde proti sobě a útočník má vždy náskok:

* TG je *umožňovač*: jak něco dělat
* bezpečnost je *zabraňovač*: jak něco nedělat.

**Nutnost systémového, komplex. řešení**

Nutné použít inžen. řešení, které bude funkcí kontextu – vybudovat systém ISMS, což není triviální problém:

* pochopit všechny TG
* identifikovat potřeby stran
* pokrýt všechny procesy.

Zajištění inf. bezp. je komplexní problém.

Je dobré používat nějaký standard. Jedno jaký, ale ten pak systematicky.

**Prevence vs detekce**

* nutné vyvážit
* opět funkce kontextu

Základní bezpečnostní paradigma

Aktivum (v IT)

Vše, co:

- pro vlastníka má nějakou hodnotu

- co přinese nějaký výnos:

* data: pers., účetní, o provozu, …
* HW a SW; inf. systém nebo služba
* lidské zdroje
* licence, patenty, pověst, obch. značka
* ISMS, QMS, návody, prac. postupy, …

a pro útočníka má smysl snížit jeho hodnotu – realizovat negativní dopad.

Hmotná x nehmotná (tangible x intangible)

A. musí být individuálně identifikovatelné

Poškozené, ukradené A. lze nahradit jen s vynaložením času, peněz, úsilí, …

Specifická jsou *citlivá inf. aktiva* s nepominutelnou hodnotou. Klasifikují se jako:

* důvěrná: nezveřejňují se vně org. (platy, vni. předpisy, …)
* tajná: nezveř. se ani uvnitř org.: mohlo by narušit její zájmy
* přísně tajná: nezveř. se ani uvnitř org.: mohlo by vážně poškodit její zájmy

Zák. o KybBezp: Klasifikace aktiv:

**Dle důvěrnosti:**

* Nízká: A. veřejně přístupná; Ochrana žádná
* Střední: většinou KH; Ochrana řízením přístu­pu; není ze zák. vyžadována
* Vysoká: Ochrana pož. zákonem nebo jinými předpisy, SoD: zaznamenává se přístup, šifrují se
* Kritická: Strat. obch. tajemství, citl. os. data; Ochrana nadstand.: evidence přistupujících osob

**Dle integrity:** Stejné jako u důvěrnosti

**Dle dostupnosti:**

**Nízká**: narušení není vážné; toler. výpadek > 1 týden

**Střední**: narušení < 1 prac. den: běžné metody záloh.

**Vysoká**: pro důležitá aktiva; narušení < 1 hod; využívají se zálohy i tech. syst.

**Kritická**: pro krit. aktiva, narušení < minuty; obnova dostupnosti nutně automatizovaná

Zranitelnost

Specifická slabina:

* v ochraně aktiva nebo aktiva jako takového,
* využitelná ke způsobení škod.

Slabina může být:

* už v návrhu, v implementaci, v provozu.

**Nacházíme je:**

* ve fyzickém uspořádání (srv na chodbě)
* v organ. schématech (špatně def. odp. a prvce)
* v admin. opatřeních (slabá hesla)
* v person. politice (špatná školení)
* v tech. a log. opatřeních (neál. srvr)
* v HW, SW, datech (nestrukturovaná data)
* v návrhu arch. systému
* v ISMS (chybně vedený)
* všude.

Hrozba

Možné nebezpečí vzniku škody na aktivech (CIA).

Vnější x vnitřní hrozba.

Podmínkou existence hrozby je:

* existence možného útočníka
* existence zranitelnosti.

**Typy útočníků**:

* #1: nespokojený zaměstnanec, často profík
* amatér, náhodný útočník
* hacker, vandal, hračička: často má znalosti, ale ne zázemí
* profesionál-kriminálník: často se zázemím, motivovaný
* bohatá a znalá autorita.

Míry pro klasifikaci útočníků:

* slabí (stačí jen slabá opatření)
* středně silní (středně silná opatření)
* silní (nutná silná opatření)

**Typy hrozeb:**

* **odhalení**: špehování, kryptoanalýza, moni­to­rování komunikace
* **podvod**: hoax, malware, falš. identity, maškaráda (útočník vystupuje jako legitimní uživatel)
* **narušení**: modifikace dat, procesu, komunikace
* **přisvojení**: krádež dat, narušení dostupnosti (neopráv. použití služeb).

*Hoax* nevyžádaný e-mail, který uživatele varuje před virem, prosí o pomoc, informuje o nebezpečí, snaží se pobavit … Většinou obsahuje i výzvu žádající další rozeslání. (Obtěžuje, nebezp. rady, přeposílá adresy, …)

Riziko

Něco, co hrozí a nevíme, jak to dopadne.

Stále vznikají nová.

**Užší smysl**: *pravděpodobnost uplatnění hrozby*.

Tedy: pravděpodobnost, že útočník využije zranitelnost, zaútočí a způsobí negativní dopad.

**Širší smysl**: (*úroveň rizika)* = pravděpodobnost útoku \* dopad útoku

Každé identifikované riziko má mít svého vlastníka.

Riziko je třeba:

* identifikovat
* analyzovat
* vyhodnotit (určit jeho *úroveň*).

Rizika se vyhodnocují systematicky pomocí tabulek.

**Pro malé a střední firmy**: ex. katalogy typických aktiv, jejich zranitelností a hrozeb (např. normy 27 k)

Když to jinak nejde, je třeba zvolit kompromis:

* každopádně ošetřit všechna aktiva.
* alespoň význam. hrozby a význam. zranitelnosti.

**Pro velké firmy**: outsourcovat nebo znalostní SW aplikace (drahé).

Útok

Realizace hrozby

Událost, kdy útočník využije zranitelnost s cílem způsobit škodu (negativní dopad)

**Kategorizace útoků dle oblasti původce útoku:**

* přírodní vlivy
* externí útoky
* interní útoky
* neúmyslné lidské chyby.

Dopad (negativní) – co je to

Škoda způsobená útokem

Bezpečnostní cíl – co je to

Dosažení požadované minimální hladiny inf. bez­pečnosti, = min. hladiny rizika v oblastech: dův., integ., dost., nepopir., spolehlivosti, autentičnosti, …

Bezp. opatření/funkce (sec. enforcing function)

Provedená akce relevantní jisté hrozbě.

Snižuje na akceptovatelnou hodnotu:

* buď pravděpodobnost uplatnění hrozby (riziko)
* nebo výši dopadu.

Typy opatření dle koncepce opatření:

* preventivní:

hlavně velká rizika, opatř. jsou drahá, eliminují dopad útoku, často omezují činnost organizace

ISMS je v podstatě jedno velké prev. opatření

* heuristické (met. zk. a omylů), nápravná:

pro střední rizika: audity, průb. řízení rizik, určení zbytk. rizik, zálohy, …

* detekční a opravné:

povoluje riziko a pak ho řeší:

plán zach. činnosti po Bezp. Inc.

Typy opatření dle TG implementace:

* **administrativní**: standardy pro návrh, kódování, testování a údržbu SW, směrnice pro tvorbu hesel, leg. předpisy, licenční politiky, výpovědi ze zam.
* **logická**: funkce řízení přístupu, dig. podpis, antivir, šifrování
* **technická**: tokeny, ID karty, šifrovače, archiv. paměť, …
* **fyzická**: trezory, zamčené. dveře, generátor, EPS,

Typy opatření dle oblasti nasazení:

* **správa bezpečnosti** (politiky, návody, standardy)
* **TG bezpečnost** (arch. systémů, mix HW, SW a

firmware)

* **bezpečnost provozu** (pravidla provozu)

**Typické opatření je kombinací více typů.**

**Cena opatření:** 1–20 % ceny aktiva

Bezpečnostní mechanismus

Technologie provedení opatření:

* fyzický: zamykání, trezory, gener. energie, …
* technický: token
* logický: antivir
* administrativní: řízení přístupu, hesla, školení, …

Platformy pro uplatnění inf. bezpečnosti:

Aplikační bezpečnost

Síťová bezpečnost

Internetovská bezpečnost

CIIP: Critical Infor. Infrastr. Protection:

Kybernetický prostor a bezpečnost

Kyb. prostor je komplexní virtuální # vč. lidí, aktivit, organizací, připojených sítí, …

Kybern. bezp. – bezpečnost v celém kyberprostoru

**Vyžaduje**:

* koordinaci a spolupráci
* sdílení infcí o incidentech
* důvěryhodnost:

**mezi** (kart. součin):

* veř. subjekty
* soukr. subjekty
* státy.

Často se chápe inf. bezp. a kyber. bezp jako synonyma

V kyberprostoru:

* ex. bezp. problémy; jejich řešení zde není pokryto
* protože zde ex. velké množství subjektů s různými, nesourodými zájmy
* ex. tato základní rizika:
  + sociální inženýrství
  + hackování
  + malware, …

Bussiness continuity – udržení podnik. procesů

Je na to norma BS 25999

Neřeší jen TG hrozby, ale i přírodní

Cílem je hlavně zajištění dostupnosti zdrojů a služeb.

Absolutní bezpečnost - poznámky

1. Ex. jen u nevyvíjecí se společnosti bez procesů.
2. Každý bezp. algoritmus je možné prolomit,

i když jen hrubou silou a za dlouhý čas.

1. Nástroje musí odpovídat hrozbám podnik. cílů
2. Zlepšování je nekončící proces
3. Použití heurist. metody je racion. a důvodné
4. Je nutné akceptovat existenci zbytkových rizik

Politiky

Organ. může mít více politik:

* všeobecnou
* personální
* zajištění kontin. činností, …

Někdy nezávislé, někdy hierarchicky uspoř.

Bezp Pol – co je to

Soubor pravidel,

specifikujících účinná bezp. opatření,

vhodnými mechanismy,

s cílem dosažení požadované úrovně rizik,

v oblasti informační bezpečnosti.

Typová struktura bezp. politik

1. **Úvodní shrnutí:**

* zákl. hesla
* def. pojmů

1. **Důvody zavedení politiky:**

* podstatné hrozby
* možné škody
* dosavadní incidenty

1. **Řešená oblast, vazby na jiné p-ky**
2. **Cíle:**

* zvládají se rizika
* chrání se důvěrnost
* zajišťuje se integrita
* web. služby vyhovují standardům, ,…

1. **Vlastní pravidla a zásady:**

* sledují se rizika, reaguje se na ně
* některá rizika se tolerují
* vědomí závažnosti
* zajišťují se finance
* reálně se pracuje s možnými podvody
* vydávají se zprávy
* aplikují se leg. požad.
* netoleruje se protipráv. jedn.

1. **Odpovědnosti, organ. struktura:**

* nejvyš. mngt
* bezp. mnžr.
* každý zam.

1. **Klíč. výstupy:**

* incidenty nezpůsobí škody
* škody bude v akcept. mezích
* zákazníci budou v klidu

1. **Související p-ky**

* politika ISMS
* řízení přístupu
* čistého stolu a displeje
* používání SW
* zálohování
* výměny infcí mezi organizacemi
* používání eln. k-cí a síť. služeb
* mobil. zař.
* používání licencí
* práce z domova
* likvidace SW

Hierarchie BP-k

**BP organizace, celková**

* souhrn zásad

**BP specifické**

* viz několik řádků výše

Bezpečnostní politika obecně

Je nezávislá na TG IT

Je koncepční na 5–10 let

Obsah politiky:

* co se chrání
* proti čemu
* s jakým cílem
* jakými opatřeními
* jakými mechanismy.

**Způsoby editace**

* běžné je neformálně – jen pro malé firmy
* semi-formálně: vyšší úroveň důvěryhodnosti
* formální logicko-matem. jazyky – výjimečné.

Důvěrný strukturovaný dokument schválený VM.

Politika je **důvěryhodná** <=>

prokazatelně dosáhne požad. úrovně ochrany aktiv

Důl. podm.: certifikace

Tvorba BP

Iterativní proces

Konceptuální dokument

Ex. šablony (27k)

Postupně se upřesňují náklady tvorby

Tvorba se monitoruje

Fin. verze zahrnuje výstupy z:

* ohodnocení rizik
* prohlášení o aplikovatelnosti: SoA

Bezpečnostní zásady

* separace odpovědností:

auditor od výkonu

správci různých syst. od sebe

* dublování autorizace (přístup mají !dva)
* protokolovací systémy:

odolný proti falšování

pravidelně kontrolovaný

Mechanismy dubl. autorizace

* dělení krptg klíčů na 2 části
* 2 různé klíče: pomocí XOR se vypočte třetí
* současná autentizace více osob (nutný protokol)

Měnící se charakter hrozeb:

* zvládnutá ochrana proti fyzickým útokům
* zvládají se ochrany proti syntaktickým útokům
* nárůst sémantických útoků:
  + profík neútočí na HW a SW, ale na lidi
  + šíří se věrohodné bludy
  + šíří se extrémně rychle
  + KTG je při sém. útoku mimo hru
  + řešení musí mít sociální charakter
  + je nutné povýšit InfSec na CyberSec.

E-commerce

TG, které usnadňují byznys, usnadňují i podvody

Co lze přehlédnout v reálném světě,

může být velkým rizikem v *e-commerce* systému

Zásadní rozpor mezi:

* globální působností podvodníků a
* lokální působností jurisdikce

Rychlé šíření podvodných know-how.

Důvěryhodnost nepopiratelnosti

Reálně podepsaný dokument (u notáře) zaručuje, že podepisující člověk dokument:

* četl
* odsouhlasil
* vlastnoručně podepsal.

Digitálně podepsaný dokument **zaručuje** jen to, že:

pro podpis byl použit soukr. klíč podepisující osoby.

(Použitý kryptologický algoritmus bývá vyhovující.)

Digitálně podepsaný dokument **nezaručuje:**

* že podepisující osoba podepis. dok. četla
* že troj. kůň nepodvrhl k podpisu jiný dokument
* nezneužití HW a SW sloužícího k podpisu

(podepis. osoba určitě nepočítala hash).

Problém pro budoucno: zajistit, aby počítač, na kterém se podepisuje, byl zabezpečený.

Enormní nárůst složitosti

Např. ve windows je standardně pro jednu akci potřeba řádově 104 až 106 instrukcí.

Standardy

Standard: co je to

* ustavený dohodou
* odsouhlasený autoritou
* poskytuje pravidla, návody, char-ky činností

a jejich výsledků

* pro opakované a všeobecné použití
* s cílem dosáhnout optimální stupeň pořádku
* v daném kontextu.

Pojmy:

* anglofonní: *standard*
* němčina a okolí: *norma*

***de facto st.:***

* st. na bázi konsensu profes. komunity
* otevřená, svobodná, prac. dobrovolně, z dotací
* *de f. st*. je liberální pohled na svět

Příklady *de f.* st-dů

**standardy RFC**

*Request for comments*

**st-dy pro internet**

(název st-dů dán historicky)

* v pozadí je ISOC (I-net Society)

členové: 150 institucí, 6000 fyz. osob

* v pozadí je i IAB: I-net Activity Board

rada pro I-net, manažersky spravuje I-net

13 fyz. osob jako členové

dohled nad archit. protokolů

* IAB delegovala vývoj na IETF

I-net engineering task force

(komise pro tech. problémy)

**standardy sdružení OWASP**

*Open Web Application Security Project*

**st-dy pro bezp. web aplikací:**

* vývoj, testy, provoz, …
* kritéria záruk za bezpečnost

**standardy COBIT**

*Control objectives for Inf. and related TG*

vydává ISACA

*Inform. systems audit and control association*

profes. sdružení auditorů IT

* COBIT je vedle ISO
* **doplňuje ISO pro řízení IT**
* má stejné cíle jako ISO (27k)
* ISO spíše veř. sektor
* **COBIT spíše na aplikace:**

34 procesů

230 nástrojů řízení

**Standards of Good Practice**

vydává ISF, *Intrnl Security Forum*

Nezávislá, nezisk.

**praktiky, metodologie měření a rozvoje InfBezp**

volně dostupný st-d:

odvozen od COBIT a ISO 27 k.

zaměřen na metodologii InfBezp

**Firemní proprietární st-dy**

**PKCS: Publ. Key Cryptogr. St.**

* obvykle patentové techniky
* cíl udržet trh silnou společností
* často hrají silnou roli:

***de iure st.***

* schválený autoritou (státní)
* lze jej vymáhat legislativně
* *de i. st*. je silně konzerv. pohled na svět

např. st-dy ISO, IEC, *Intern. Electrotech. Commisson*

konzervativci do *de i. st-dů* často přebírají:

* vyzrálé *de f. st*.
* ale jen to, co chtějí
* a to, co stíhají

Oblasti zájmu *de i. st*-dů

*InfBezp* je součástí všech výše uvedených

Všechny organ. jsou celosvětové a spolupracují:

Univerzálně bez portfeje: ISO, 160 členů

Elektronika a elektrotechnika: ISO, IEC

Komunikace: ISO, ITU-T (původně CCIT)

*Int. Telecomm. Union, T:* sektor standardizace

Evropské *de i*. st. orgány

CEN, Comité Eur. do Norm.

CENEL - … Eléctotechnique:

jako IEC, ale na Evr. úrovni

ETSI: Eur. Telecomm. st. institute

Národní *de i. st*. orgány

Reprezentují stát v ISO

St-dy silných nár. orgánů jsou uznávány mezinárodně:

ANSI: USA; BSI: UK; DIN: SRN;

AFNOR: Francie

ČNI – jen překládá, jinak nemá sílu

Významné postavení USA jako TG lídra:

***IEEE*** (Inst. of electrical and electronics engineers)

* profesní orgán
* jeho st. mají int. dopad
* např. pro LAN: IEEE 802.xxx

***NIST*** (Nat. Inst. for St. and TG)

* federální orgán
* vydává FIPS (Feder. Inform. Processing Stds)

vysoce kvalitní normy

* vydává i Special publications (SP):

SP 800 Computer Sec.: rozsáhlá rodina

* + SP 1800 Cybersec. practice guide
  + SP 500 Comp. systems TG

***ANSI (***Amer. Natnl St-s Inst.)

* zástupce USA v ISO
* dělá hlavně bank. sektor

Závaznost standardů – poznámky

žádný druh není leg. závazný

jen přes zákon – většinou se použije *de i. st*.

mnoho standardů = smrt pokroku

Certifikace – poznámky

!! *Compliance* (vyhovění*)* vs. *Certification !!*

Compl. – deklarace výrobce

Některé standardy jsou obtížně certifikovatelné

Nikoliv ale např. st-dy o algoritmech

Standardizace – poznámky

Někdy ex. více pohledů na to, co je správně

St. s mnoha volnými par. se obtížně certifikuje

Problém s překlady

Někdy produkt vyhovuje jen podst. části st-du

Silný výrobce může prosazovat vlastní standardy

Normalizace ISO

Odpovědnost za tvorbu st. mají tzv. tech. výbory, TC

Ty si samy určují program pro splnění cíle

TC´s mají podvýbory, subcommittees

ty mají pracovní skupiny, WG´s

evoluce (TC – SC – WG) trvá ≈ 5 let:

nyní pro IT velmi brzdící faktor

Životní cyklus:

1. NWI: Návrh nové prac. položky

jmenování odp. editora

1. WG: postupné návrhy v rámci WG
2. SC: návrh st-du v rámci SC

odsouhlasuje se v SC

1. TC: návrh intl st-du

odsouhlasuje se v TC

1. ISO: konečný návrh intl st-du

každé projednávání a hlasování trvá 2–6 měsíců

každý st. se po 5 letech přezkoumává

pokud se neodhalí vada dřív:

pak se vydá *Defect System Report*

ISO Technical reports

mají obv. metodický charakter

věcně skoro stejně významné jako st-dy

příklad: ISO/TR 13335 Směr. pro správu InfSec

**Typ 1**

* když není v TC podpora pro vydání standardu
* názory jedn. členů nejsou shodné
* po 3 letech se musí revidovat a rozhodnout, co dál

**Typ 2**

* když se předmět standardu stále vyvíjí
* předp. se, že v bud. se schválí jako st.
* opět: po 3 letech revidovat, a rozhodnout, co dál

**Typ 3**

* když předmět standardu nepodléhá standardizaci,

ale návrh je významný a připravený

* předp. se, že v bud. se schválí jako st.
* po 3 letech se nemusí revidovat, pokud

v něm nejsou nedostatky

ISO 27000

* celosv. zákl. standard pro InfSec
* rodina celkem asi 40 norem
* vydává ISO/IEC/JTC1/SC27/WG1

*JTC – Joint techn. committee 1*

**27001**

*… - Requirements*

požadavky na funkcionalitu a vlastnosti systému

původně UK st. BS 7779-2

co se musí nebo má dělat

nezávislý na spec. TG

pro všechny a všech velikostí

sepisuje seznam cílů

vše je otevř. a může být doplněno vlastními položkami

lze na něj certifikovat

**27002**

*Code of practice:*

navrhovat, impl., udržovat, vylepšovat opatření

intl. uznávané *best practices*

zdroj návodů, musí být použit

návrh řízení rzk se musí porovnat se seznamem v 27001

**ISO/IEC/JTC1/SC27/WG1, 2, 3**

vydává i další st-dy a TR:

* dig. podpisy
* detekční systémy
* řízení reakcí na události
* autentizace entit
* správa hesel
* šifr. algoritmy
* funkční požadavky
* bankovní operace: šifr., biometrika, …

**Evropské iniciativy jsou slabé**

Právní principy, axiomy

* je dán morálkou, kulturou
* společný pro kulturně blízké státy
* je základem práva
* nelze ho prohlásit za neplatný
* není expl. obsažen v zákonech

rozumí se „samo sebou“, v zák. je imanentně

* příklady:
  + k nemožnému se nelze zavázat
  + zákon není retroaktivní
  + neznalost zákona neomlouvá
  + smlouvy se mají dodržovat
  + spec. úprava ruší obec. úpravu
  + není trestu bez zákona
  + ne dvakrát o tomtéž

181/2014 Sb. o kyber. bezpečnosti

Cíl: zajištění bezp. fung. inf. společnosti

Nedotýká se uživatelů ani poskytovatelů obsahu

Dotýká se správců special. inf. a komunik. systémů

Nezasahuje do obsahu, chrání proti bezp. incidentům

Požadavky na zabezp. kritické inform. infrastruktury

Systém obsahuje:

* bezp. opatření
* detekci událostí
* hlášení incidentů
* reakční opatření
* činnost dohled. pracovišť
* spolupr. CERT a veř. subjektů

NÚKIB vydává vyhlášky

Další relevantní zákony

* 106/1999 o svobodném přístupu k inf.
* 101/2000 o ochraně os. údajů
* 240/2000 o kriz. řízení
* 365/2000 o inf. systémech veř. správy
* 480/2000 o některých službách inf. společnosti
* 127/2005 o elektronických komunikacích

Řízení rizik, risk mngmt

Obecně

Rizika se objevují z růz. důvodů:

* změna byznys modelu
* nevyhovíme zákonu
* nízká kvalita návrhu, provozu aplikací
* z přírody

Rizika nelze hledat jen z pohledu aktiv,

ale i z možných scénářů, co se kolem nich děje kontext): komplex procesů.

***Kontext*** znalost vně. a vni. souvislostí, zasvěcenost do [problematiky](http://slovnik-cizich-slov.abz.cz/web.php/slovo/problematika), přístup k [informacím](http://slovnik-cizich-slov.abz.cz/web.php/slovo/informace)

***Řízení rizik:***

* nejen v IT, v celé byznys aktivitě
* velmi důl. manaž. funkce
* **pro InfBez je v 27005**
* lze aplikovat na:
  + celou org., část
  + na spec. inf. systém nebo data
  + na spec. byznys/TG proces

Procesy řízení rizik

1. **Kontext** (jakoby P-ka v EnMS)

* účel řízení rzk
* hranice sprav. oblasti
* zajištění zdrojů (všech a na vše)
* kritéria pro všechna hodnocení

(aktiv, dopadů, bzns ztrát, provozu)

* organizace (řízení rzk) a odpovědností

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Pravď. real. hrozby | Výše dopadu | **L** | **M** | **H** |
| Zanedbatelný:  tisíce Kč | Zvládnutelný: desetitisíce Kč | Katastrofický:  statisíce Kč |
| **L** | Jednou za dekádu | VL = LL | L = LM | M = LH |
| **M** | Jednou za rok | L = ML | M = MM | H = MH |
| **H** | Jednou za den | M = HL | H = HM | VH = HH |

*Úroveň rizika* a následná opatření:

***VH*** katastrof.: nutné odstranit nebo prevencí snížit

***H*** vysoké: akční plán real. opatření, prev. snížit

***M*** běžné: stačí jmenovat odp. osobu/roli

***L*** akcept-lné: rutinní proced., ev. ošetřit pojištěním

***VL*** zanedbatelné, neřešit

1. **Ohodnocení rizik (assessment):**
   1. identifikace rizik:

ident.: aktiv, zranitelností, hrozeb, dopadů

(využívat scénáře možných útoků)

* 1. analýza rizik: určení velkosti

kvalitativně: prvotní, ale obtížně použit.

kvantitativně: pro hl. rizika, výsl. „součinů“

* 1. vyhodnocení (evaluation) rizik:

aplikace metrik a součinů a porovnání s kritérii

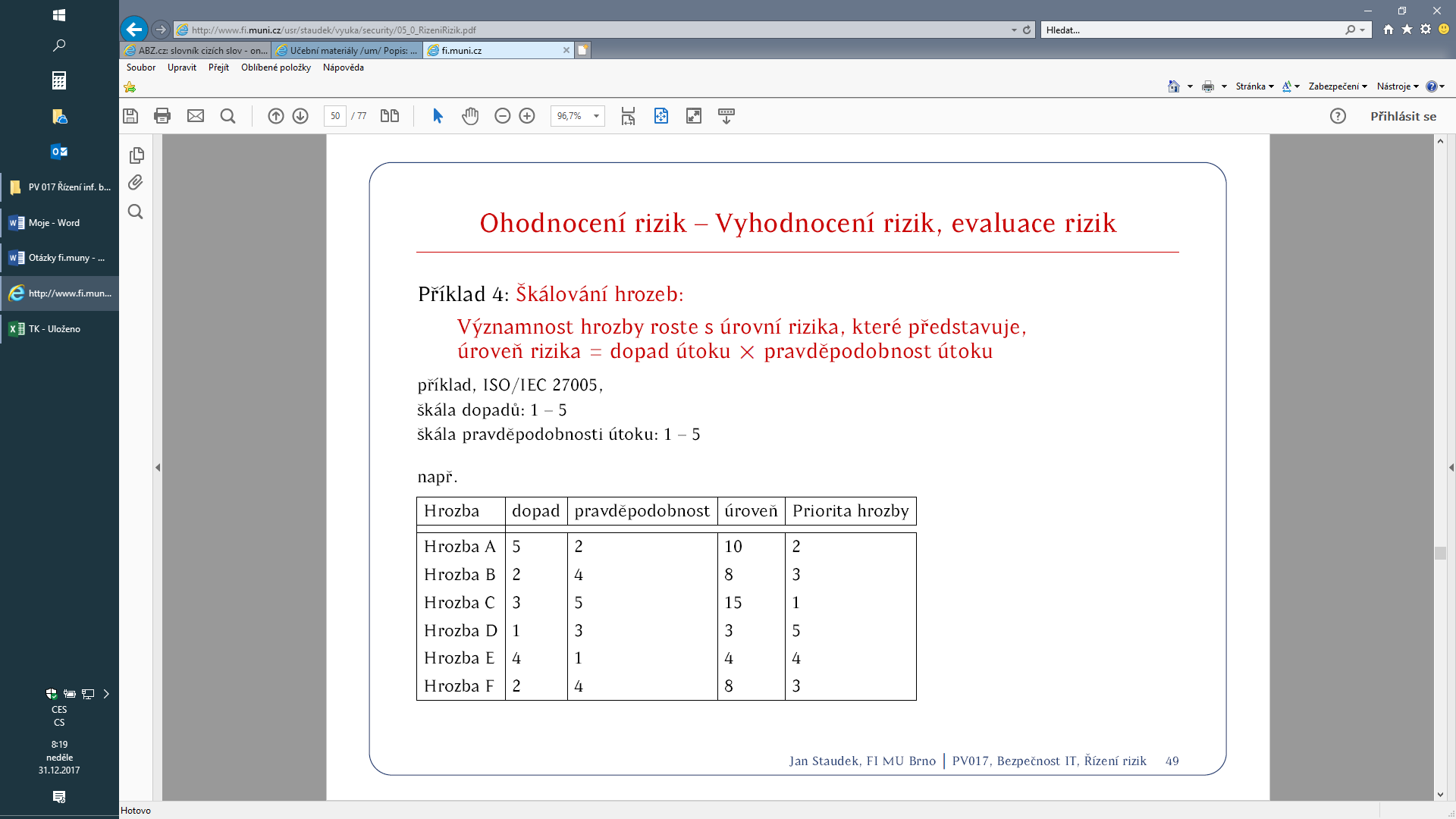
využívat škálovacích stupnic

zahrnout všechny škody, i nepřímé

27005, NIST SP 800: návody škál. stupnic

svou trochu jinou metodiku má i ZKB

i návody kart. tabulek i více dimenzí



**Metody hodnocení**:

* + elementární: převzetí na základě analogie
  + neformální: jak co kdo ví, nestrukt.
  + formální: stnd. strukt. metody/nástroje
  + kombinace: jak pro co (ekon. hledisko!)

**Výstup ohodnocení**:

Prohlášení o aplikovatelnosti,

***Statement of Applicability, SoA:***

Obsah:

* + seznam ohodnocených rizik dle priorit
  + seznam a zdůvodnění opatření, vč. cen
  + požad. důkazy o implementaci
  + požad. důkazy redukce rizik

Vlastnosti SoA:

* + zákl. dok. ISMS, tvoří jádro manuálu
  + prav. se přezkoumává
  + podepsaný vlastníkem oblasti jeho použití
  + použitelný pro k-ci s 3. stranami

(podepsat NDA), [non-disclosure](https://cs.wiktionary.org/w/index.php?title=nondisclosure&action=edit&redlink=1) [agree­m.](https://cs.wiktionary.org/wiki/agreement),

nebo rozdělit na dův. a veř. část)

1. **Zvládnutí rizik (risk treatment)**

Plné odstranění r. je nemožné nebo neekon.:

* vždy se potlačuje největší riziko
* na rozumnou míru
* za nejmenší cenu
* s nejmenším dopadem na ostatní b. procesy

Aplikuje se:

* modifikace rizika
* opatření snižující rizika

Existuje:

* HMG impl. opatření
* Výčet zbytk. rizik

**Plán zvládání rizik má 7 zákl. kroků:**

1. seřazení rizik
2. soupis opatření, jejich analýza
3. analýza nákladů
4. výběr nejvhodnějších opatření
5. přidělení odp. za jejich impl.
6. implementace
7. vyhodnocení

**Plán zvládání rizik musí být:**

* dokumentovaný
* pro daný kontext
* popsaný formálně
* se stanovením odpovědnosti

**Pro každé riziko plán obsahuje:**

* akceptovatelnou úroveň rizika
* všechny možnosti jeho zvládnutí
* která možnost je použita
* již ex. relevantní opatření
* příp. dodatečná opatření
* HMG
* reference na SoA
* zajištění dostupnosti zdrojů
* školení a zvyš. vědomí záv.
* podpis vlastníků rizik
* metodu PDCA

**Cíle plánu:**

* která lze eliminovat
* která snížit na akcept. úroveň
* určí akcept. rizika
* která se přenesou nebo pojistí

1. **Akceptace rizik:**

Management:

* odsouhlasí Plánu zvládání rzk dle stan. kritérií
* odsouhlasí zbytk. rizika jako akceptovatelná
* odůvodní ta akceptovaná, která nejsou standardní

1. **Komunikace rizik: všem, kdo:**

je mohou ovlivnit nebo

jími být ovlivněni

* shromažďuje infce o rzk
* prezentuje výsledky
* podpora rozhodování
* získávání nových znalostí
* prezentuje odpovědnosti
* zlepšuje bezp. uvědomění
* organ. školení

1. **Monitor. a přezk. (rizik a procesu řízení r.)**

Monitorování (dle paradigmatu):

* nová aktiva
* úpravy hodnot aktiv
* nové hrozby
* nové nebo zvýšené zranitelnosti
* změny dopadů/škod
* incidenty, skoro-incidenty

Monitoruje se, protože se mění:

* právní kontext
* konkurenční kontext
* přístup k rizikům
* a mnoho dalšího

Procesy řízení rizik

Často jsou to opakované iterační postupy.

Org. by měla udržovat akt. dtb:

* IT aktiv
* jejich vlastnictví
* rizik
* jejich pravď.
* atd.
* ex. na to nástroje

InfBezp v organizaci

Vrchol. vedení:

* správní rada/představenstvo
* výkonné vedení/představenstvo

(board of directors)

* + výkonný ředitel

(***CEO***, chief executive off.)

* + finanční ředitel
  + provozní ř.
  + obchodní ř.
* **střední mngt**
  + ředitel odb. IT (***CIO***)

*chief inform. officer*

manaž. inf. bezp.: ***CISO***

chief inf. sec. officer

* + ředitelné dalších organ. souč.
* ***řídící výbor*** (inf. bezpečnosti)
  + ustaven vrch. vedením
  + členové napříč organizací
  + členem je bezp. architekt
  + členem je i (více) CISO
  + zasedá 2-4x ročně
  + závěry jdou na výkon. mngt
  + odpovědnosti značně široké
* ***lokální správci*** (inf. bezpečnosti)
* ***admini*** systémů
* **int. auditoři**

CISO

Postavení:

* CEO/představitel vedení: role daná statutem org.
* CISO – bezp. manažer: role daná statutem org.
* šéf projektu ISMS – samost. role

Ustavuje ho *řídící výbor InfSec*

Nesmí být souč. int. aud.

Musí znát byznys procesy

Pozice např.:

* optimálně podřízen přímo CEO
* z nějakého oddělení
* lze část. úvazek

Náplň práce

* dělá seznam zaint. stran (státní správa, hasiči, ..)
* jejich seznam požadavků
* udržuje kontakty na úřady a zájm. skupiny
* průběžně posuzuje kvalitu ISMS
* sleduje leg. a sml. požadavky
* průb. monitoruje systém
* navrhuje prac. verze dok-ce
* odpovídá za aktual. dok-ce
* koordinuje procesy řízení rizik
* navrhuje HMG implementace
* navrhuje opatření
* provádí poč. posouzení rizik
* identifikuje změny rizik
* podílí se na školení a plánu výchovy
* navrhuje discipl. řízení
* definuje komun. kanály
* připravuje komun. zázemí pro katastrofy
* spolupracuje na formulaci cílů
* vytváří BP, její cíle, strategie, oblasti působení
* měří a sděluje výsledky měření efekt. ISMS
* navrhuje vylepšení a opravy
* podává zprávy o impl. opatřeních
* odpovídá za provedení opravných prací
* informuje o impl. ISMS
* informuje o BInc, problémech, akt. hrozbách
* eviduje bezp. události
* koordinuje reakce, vypracovává zprávy
* připravuje důkazy po BI pro právníky
* analyzuje incidenty
* spoluvytváří plán zach. činnosti po BI
* testuje chování po incidentech
* schvaluje metody ochran mobil. zařízení a k-cí
* navrhuje metody šifrování
* navrhuje pravidla pro práci při vzdál. připojení
* definuje pipy bezp. vývoje
* analyzuje protokoly činností (logy)
* komunikuje s vrch. vedením
* odpovídá za oponování dok-tů
* navrhuje metody autentizace, politiku hesel

Generické role odpovědností

* řídící výbor – viz výše
* oddělení IT:
  + zajišťuje provoz systémů
  + bezp. serveroven
  + spolupráce při identif. hrozeb
  + hodnocení rizik
  + řízení projektů, revizí, …
* lok. admini:
  + evidence uživatelů systémů
  + monitorování systémů
  + příprava bezp. procedur
  + zálohování dat
  + návrhy aplik. bezpečnosti
  + implem. vni. opatření
  + test. nouz. plánů

**Klasifikace adminů**

* správci systémů
* správci sítí
* správci areálů
* uživatelé IT
* třetí strany

Účel bezpečnostního auditu

Provádí se v rámci tzv. správy (řízení) bezpečnosti

Nezávislý na exekutivě, nezáv. auditor (separace odp.)

* kontrola definic bezp. procedur
* detekce neošetřených zranitelností
* audit procedur po incidentech: jak, co, kdo, …
* postupy IA musí být součástí systému

Metody hodnocení objektu při auditu.

**Vyšetřování**

* proces kontrolování, studování nebo analýzy
* jednoho nebo více přezkoumávaných objektů
* na všech úrovních (specifikace, mechanismy, procesy)
* cíl: porozumět, objasnit nebo získat důkazy
* lze podporovat automatizovanými nástroji
* typy: všeobecné, cílené, detailní, reprezentativní, úplné

**Interview**

* vedení rozhovorů s jednotl. nebo skup. v organizaci
* cíl: porozumět, objasnit nebo zjistit, získat důkazy
* nelze automatizovat
* typy: všeobecné, cílené, detailní

**Test**

* proces cvičného provozování jednoho nebo více přezkoumávaných objektů za určitých podmínek
* cíl: porovnání skutečného a očekávaného chování
* musí být provedeno kvalifikovanými odborníky, musí být reprodukovatelné, opakovatelné
* lze podporovat automatizovanými nástroji

Řízení reakcí

Bezpečnostní událost

Změna denních operací inf. služeb ukazující, že

* bezp. p-ka byla narušena nebo
* bezp. opatření selhala nebo
* nastala neznámá situace.

Nemusí nutně znamenat:

* úspěšný útok, ani
* vznik škody.

Může to být

* náhodná chyba
* systém zpomalující zálohování
* hloupost uživatele.

Každá BU musí být dokumentována.

Bezpečnostní incident vs. útok

Podmnožina bezp. událostí

Bezp. inc, je bezp. ud., která:

* s vysokou pravď. ohrožuje podnik. činnosti
* a ohrožuje InfBezp.

**Kategorizace BI (na přímé a nepřímé):**

* přímé útoky:

D/DoS

Neaut. přístup (příklady sl. 12)

Zlomyslný SW

Nepatřičné užívání (stahování hack. nástrojů,

používání firem. mailu pro spam,

web. stránky na firem. stroji,

distribuce pirát. souborů)

* nepřímé útoky:

sběr in-fcí: rekognoskace prostředí

(topologie sítí, zranitelnosti, kopírování DNS

zá­zna­mů, testování adres pingem, prohledávání

portů)

porozumění službám

**Kategorizace dle ZKB**

pojem ***infekce***

**Kategorizace dle 27k**

IV: velmi vážný: nouzový stav

útok na velmi důl. IS

velmi vážné obch. ztráty

význ. soc. dopady

III: vážný – kritický stav

II: méně vážný – spíše varování

I: malý – jen podnět k zamyšlení.

**Kategorizace dle hrozeb**

* živly
* sociální nepokoje
* fyzické poškození (úmyslně, náhodně)
* selhání infrastr. (EE, UZS, EPS, HVAC, …)
* elmag. vyzařováním
* technická selhání (vlastních systémů)
* malwarem
* technický útok (přes sítě na zranitelnosti)
* kompro in-fcí (poškození náhodně nebo úmysl.)
* porušení prav. chování (autor. práva, „letadla“)
* útok škodlivým obsahem

Správa/řízení BI

**Cíle správy reakcí:**

1. minimalizace přímého negativního dopad

(zastavit šíření škody, odstavit zdroj útoku)

1. získat poučení, zefektivnit ochrany

(anal. útoku, příčiny, f-ce ochran, zpráva)

**Fáze procesů správy**

**ISIRT:** *Inf. Security Incident Response Team*

* plán a příprava
  + politiky
  + ustavení ISIRT, začl. do org. sch.
  + tech. podpora ISIRT
  + školení a tréninky
  + testování systému řízení BI
* detekce a zprac. zprávy o vlastním BU
* posouzení a vydání rozhodnutí:

byla BU BI-tem?

* plná odpovědnost ISIRT:

1. identif. iniciál. reakce

(dostavení systémů, sítí, služeb)

1. minim. dopadů na podnik. procesy

(infce > mangmntu)

1. identif. zdroje útoku
2. klasifikace BI
3. rozhodnutí o závažnosti
4. příp. spustit kriz. plán
5. obnova normální fce
6. vyprac. záznamu o útoku a reakci

(detailně se všemi odpov., časy, důvody, …

vše, co si dokážu přednstavit)

* poučení z BI
  + příp. další vyšetřování
  + identif. dalšího vylepšení
  + implementace vylepšení
  + přezkoumání dotč. systémů, dok-cí

**Diagram postupu reakce na BU/I**

**(disaster recovery?)**

1. **Detekce a reportování**

* **detekce** bezpečnostní události
* informování – **reportování** standardizovaným **formulářem:**

popíše BI tak, jak ji vidí

* jestliže exituje **Point** **of Contact** (24/7): předává se ta zpráva jim  
  pokud neexistuje PoC, tak se **zpráva předává ISIRT**u

1. **Ohodnocení a rozhodnutí**

* pokud existuje PoC, tak šetří práci kvalifikovaným ISIRTu,
* pokud se o události dá jednoznačně rozhodnout, jestli je BI nebo ne;

pokud si není jistý, tak to taky předávání

* **ISIRT posoudí**, jestli jde o planý poplach nebo jestli je to incident

1. **Reakce**

* pokud se posoudí, že jde o BI a samotný **ISIRT** to nezvládá, nasadí **činnost super školeného bezpečnostního týmu** – spuštění procesů podle předem připraveného **krizového plánu**
* **zdokumentuje se**

1. **Vylepšení**

Tři týmy/fáze pro reakci na útok

1. zásah ***týmu první reakce***
   * běžní provoz. prac.
   * ambulantní zásah
   * inf-ce odp. osobě
2. nástup týmu na řešení incidentu (***ISIRT***)
   * klasifikace BI
   * spuštění kriz. plánu
   * zkušení pracovníci, slouží 24/7
   * uvádějí IS do prov. v omez. podm.
3. nástup ***týmu obnovy***
   * specialisté
   * speciální zručnosti
   * spec. vybavení
   * obnova IT
   * záznam o BI

Pojmy

Vyšetřování bezp. ud.

Týmy se všelijak jmenují:

ISIRT: Inf. Sec. Incident Response Team

CERT: Computer Emergency Response Team

CSIRT: Comp. Sec. Inc. Resp. Team

Asi stálý orgán organizace:

* jak zjišťovat, hlásit a posuzovat BI
* jak reagovat na BI a krizově řídit akce po BI
* jak detekovat, hodnotit a řešit zranitelnosti
* jak pomocí výše ... zlepšovat InfBez a kriz. řízení

Aplikační bezpečnost

**Aplikace**:

* (balík) SW se spec. účelem, často komunikující s uživatelem nebo technologiemi
* já: pracuje v reálném čase
* personalistika, účto, zprac. textu, firewall, antiviry, AutoCad, vlastní aplikace, …

**Trojí ochrana aplikací**:

* před jejich vlastními vadami
* před změnami v důsledku používání (záplaty?)
* před vadami při použití v jiném kontextu

**Apl. bezpečnost neřeší:**

* její bezpečné programování
* fyzickou a síťovou bezpečnost
* tvorbu opatření

**Apl. bezpečnost řeší:**

* vlastní aplik. syst. (procesy, komponenty, SW)
* data (aplikační, uživatelská, konfigurační,

zdrojové kódy, …)

* řízené TG, procesy, subjekty.

Aplik. bezpečnost dle 27k

Procesně orient., TG nezávislá opatření

Pro každou aplikaci:

* ohodnocení rizik – základ
* identif. opatření – v SoA
* definuje se Plán zvládání rizik:

hlavní dok. pro implementaci opatření

Příklady opatření

* oddělení odpov. za návrh, vývoj a testování
* oddělení prostředí testování:

vývoj testů, akceptace, provoz

* autom. registrace a deregistrace
* přidělování nejmen. potřebných práv uživatelů
* kvalitní politika hesel
* skupinové účty moc nebrat
* protokolování událostí
* školení před udělením práva užití
* omezit přístupy k rozhraní s OS, ke zdroj. textům
* přísné změnové řízení
* oddělení síťových prostředí
* ochrana síťových transakcí
* analýza požadavků InfSec

Příklady útoků na aplikace

* útok na autentizaci
* získání cookies klienta
* ovlivnění SQL příkazu
* změna dat z prohlížeče uživatele na aplik. server
* přetok bufferu
* ???

SDLC – Syst. develpm. life cycle

Řešení inf. bezp. je součástí LC

Životní cyklus inf. systému

1. **Zahájení**:

účel, oblast, anal. potřeb, studie proved.,

předb. ohodnocení rizik:

* + dostup z inetu?
  + i neautor. uživatelé?
  + budou data citlivá?
  + bude se používat dtb řešení?
  + bude apl. komunik. s jinými ext. apl?
  + charky útočníků
  + bude více úrovní oprávnění přístupu?
  + ex. zákonná omezení?

1. **Návrh** (architektury systému);
   * modelují se všechny hrozby
   * vč. Plánu zvládání rizik
2. **Vývoj nebo zakoupení**:

* posuzuje se s požadavky, vč. bezpečnosti;
* metody bezp. programování

(např. validace vstupů, silná hesla,

bezp. postupy při zapomenutí hesla)

* používají se ident. rizika

1. **Testování** (jsou splněné požadavky?)

* provádí se bezp. testy:
  + grey box: ze strany ne/autor. uživatele
  + white box: chyby a zran. ve zdrojáku

1. **Zprovoznění**, provoz a údržba:

* na spec. HW, doplněno o další SW:
* mohou se změnit organ. procesy,

politiky, procedury

* black box testy

1. **Likvidace**/přesun infcí, HW, SW

sanitizace (čištění, sterilizace HW a SW)

ISMS dle 27k

Co je to vlastně ISMS:

Je to *systém řízení*:

* dokumentovaný, syst. řízený, implementovaný
* trvale přezk., audit. a kontrolovaný
* trvale akt.
* důvěryhodný (důkazem je certifikace)

Cíl

Procesní řízení InfBezp:

* návrh
* implementace,
* zavedení do provozu,
* provozování,
* monitorování
* přezkoumávání
* udržování
* zajišťování úrovně záruk za kvalitu

27001: jak navrhnout ISMS a co má dělat

(odrážky se týkají vlastního ISMS):

* ustavení a správa
* zavádění a provoz
* monitorování a přezkum
* udržování a zdokonalování
* správa dokumentů
* odpov. vedení
* přezkum 3. stranou
* aktualizace

**27002: kodex nejlepších praktik: kuchařka**

historie: asi 15 let

4 vrstvá struktura dok-ce – viz sam. list

**Vrstva 1:** stabil. strateg. vrstva, schvaluje vrchol

* Zájm. oblasti – scope, dle kontextu
* Inf P-ka celková – hl. strategie
* Vazba na další politiky
* Zpráva o hodnocení rizik
* SoA
* Plán zvládání rizik
* Manuál ISMS

**Vrstva 2:** schvaluje výkon. mangment, občas se mění

* procedury impl.
* Popis řídící struktury
* Definice rolí a odpovědností (přes vš. politiky)
* role 3. stran do smluv)
* řízení přístupu
* Procedura reakce na BU a BI
* BP dodavatelů
* Procedury řídící správu a inspekci ISMS
* Legisl. a sml. závazky
* nižší politiky a jejich implementace

**Vrstva 3**: schval. CISO, mngt provozu, rel. časté změny

* prac. instrukce
* uplatňování politik
* měření účinn. opatření
* popis akceptovatel. používání aktiv (formou politiky)
* zranitelnosti, hrozby a rizika pro tato aktiva
* ***Politika řízení přístupu***
* Procedury, zprávy IT

(změnová řízení, zálohování, síť. bezp., likvidace dat, monitorování)

* pipy bezp. inženýrství (ladění, testy, akceptace, …)
* vytváří je vlastníci procesů, mění se rel. často

**Vrstva 4**: schval. CISO, mngt provozu, časté změny

* šablony: záznamy, formuláře, …

Dokumentace doporučená

* Správa dokumentů
* Nástroje pro správu protokolů
* proces IA
* proces opravné akce
* P-ka BYOD (bring your own device)
* p-ka vzdálené práce
* p-ka klasifikace infcí
* p-ka hesel
* p-ka likvidace a destrukce
* p-ka čistého stolu a monitoru
* p-ka změn. řízení
* p-ka zálohování
* p-ka dopadů činnosti na IB
* plán cvičení a testování
* plán údržby
* plán oponentur
* strategie zachování činnosti

Vztah P-ky InfBezp a ISMS??

Něco požaduje 27001 a něco 27002

*??!! vztah mezi oběma p-kami nikdo neurčuje*

*(nad, vedle, pod)*

Záznamy požadované

* zápisy ze schůzí
* zprávy specialistů
* seznamy (aktiv, hrozeb, ...)
* výsledky auditů, testování
* dokumentace BU a BI
* (oponentní) zprávy
* pgm plnění školení
* výsledky měření a monit. vč. KPI
* pgm IA, výsledky IA
* závěry z oponentur (jednání mngmentu)
* výsledky opravných akcí
* logy uživ. aktivit, BU, …

Generické problémy budování ISMS

* není to TG problém, ale manažerský
* vyvolá změny v řídících procesech
* vědomí závažnosti mngmentu – nutný důkaz
* hledá se ochrana i proti dosud nereal. útokům
* útočníkovi stačí jediná zranitelnost a čeká na lepší útočný nástroj
* k dokonalosti přes komplex mnoha nástrojů
* nutné dostatečné finanční zdroje
* většina investic při budování ISMS nejde do IT, ale do školení, vývoje politik a procedur, …
* nutné PDCA.

Proč používat 27002:

* specif. nejlepších praktik, návod
* specifikuje ISMS netechnickou a nejurisd. cestou
* úplně a systematicky
* validita prokázána mnoha implementacemi
* externě certifikovatelný
* navazuje na 9001 a spol.

Proč se zavádí v urč. organizaci:

1. Rozhodl tak zákon
2. Rozhodl tak vlastník, zákazník, správní rada, …
3. Získání konkurenční výhody – zvýšení důvěryhodnosti
4. Jiné vnitřní pohnutky

Tři možné cesty k ISMS:

1. amatér. aktivity zaměstnanců:

\* dlouhá cesta do pekel

1. bezpečn. tým podle vzorů a prototypů:

\* rychlé, přim. nákl-dy, lze dobře vylepšovat

1. bezpečnostní manažer + outsourcing:

\* rychlé, drahé, obtížně se vylepšuje

PDCA

**Plan**: Plánuj

porozumění problému, definice, kroky, cíle v kontextu, metody, procedury, HMG, kritéria, metody ověř., SoA, výběr opatření, ..

**Do**: Dělej

impl. plánu, opatření, politik, zaškolení, zajištění zdrojů, vazby na jiné syst.

**Check**: kontroluj

měř účinn., kontroluj, zaznamenávej, ověřuj, analyzuj, dělej grafy, testuj, zprávy pro mngmt,…

**Act**: úpravy záměru

finál. fáze: jednej podle dosav. výsledků

úpravy záměru a vlastního provedení

identifikace vylepšení

(všude dost nejasně vysvětlený krok)

Implementace ISMS

Implementaci řeší **27003**: samotnou n. i její integraci

Fáze:

1. **Zahájení**
   * rozhodnutí vedení
2. **Def. oblastí působnosti, formulace politiky**
3. **Analýzy**
   * anal. požadavků organ.
   * Ohodnocení rizik;
   * Plán zvládání rizik
4. **Návrh ISMS a jeho implementace**

**Implementace jako *projekt*:**

(jedinečná soust. činností, jasný cíl, začátek, konec, hmg, vyžaduje spolupráci, potřebuji lidi, čas, peníze, materiál, schopnosti, riziko neúspěchu, složen z úkolů)

**3 dim projektu:**

**co, kdy, za kolik** (jako u SoD)

* pův. 27k předepisovala PDCA; nyní to nechává volné, ale s ohledem na 9001 apod. doporučuje
* Klíčový je šéf projektu impl. ISMS: manager!
* Nad ním je „představitel vedení“, jeden ze CEO
* Na startu vydat

*Seznam aktuál. relev. bezp. problémů*

* Nutná dobrá „politická“ příprava
* Proces impl. musí být specifikován v BezpPol

Musí být schopen auditu ve 4 prostředích:

* vývojové
* testovací
* akceptační
* provozní

*Viz dva obr. na samostatných stranách*

Dokumentace ISMS

Sestavení je čas. náročné

Musí být:

* úplná a vyčerpávající
* v souladu s 27k
* v nál. formě a stylu
* dostupná a chráněná
* systematicky řízená

Certifikace

Analog 9001, …

Postup:

* zájemce o certifikát v dotazníku popíše svůj stav
* uzavře se smlouva
* auditoři absolvují seznamovací interview
* auditoři zanalyzují dokci
* auditoři zanalyzují shodu doke s prostředím a provozovaným ISMS
* dozor a recert. audity

Pro dobrý proces certifikace:

* úplnou dokci
* dostupné zprávy z IA a testů
* otevřenost všech vůči auditorům
* otevřenost VV

Testování

Typy: ext. nebo int. audit

**Testy podle koncepce:**

* **myšlenkové**: logické testování na papíře
* **reálné**: penetrační testy, ztráty energie, …
* **scénářově** orient. testy

Měření a metriky

Obsaženo v **27004**

Aplikace PDCA pro metriky a měření: jasné

**Cíl**:

* inf-ce o účinnosti ISMS
* návrhy opatření

**Poskytuje data**:

* jako důkazy zlepšení
* nápady pro zlepšení

**Potřebujeme**:

1. metriky
2. metodiky měření
3. metody analýz a vyhodnocování

Návrh

* výběr objektů a procesů měření

(vše má nějakou svoji vlastnost, kterou

mohu kval. nebo kvant. ohodnotit)

* intrvw se zaint. stranami
* první verze metrik
* další intrvw
* definice:
  + metriky
  + metody měření
  + analyt. model
  + KPI
  + kritéria (pro zjištění výsledků)
* vlastní měření

(získání vlastností o objektu měření)

* agregace a analýza dat
* převedení od formy pro prezentaci

Metriky – vhodné vlastnosti

Musí být SMART

Použít pravidlo 20/80

Měly by být automatizovatelné

Volit vhodnou četnost měření

Nemusí být nutně objektivní:

* výsledek intrvw
* hodnocení růstu bezp. povědomí

Nemusí mít nutně diskrétní hodnoty:

* výsledek toho, co lidé říkají

Lze využít stáv. zdroje:

* statistiky z helpdesku
* reakce zákazníků
* frekvence řešení problémů na úrovni mngmtu

Stupnice – definice pojmu

* uspořádaná množina:

spojitých nebo

diskrétních

hodnot vlastností

* nebo množina kategorií vlastností.

Typy stupnic

* **nominální, „pojmenovávací“:**
  + většinou kategorie vlastností

(útok externí/interní,

zranitelnost syst./admin/osob. selhání)

* + je kvalitativní
  + posuzujeme stejnost hodnot

(stupnice a objektu)

* + sledujeme četnost dané kvality
  + nelze prov. aritm. operace
* **ordinální, pořadnicová**
  + míra nějaké vlastnosti

(velký, zanedbatelný, katastrofický)

* + hodnoty je možné seřadit
  + je kvantitativní
  + úseky mezi stupni nemusí být stejné
  + stupnice nemá ani ***0*** ani ***1*** prvek
* **intervalová**
  + spočitatelná míra nějaké vlastnosti

(doba 1. reakce na BI)

* + lze spočítat, o kolik je jedna hodnota

větší než jiná

* + úseky na stupnici jsou stejné
  + je kvantitativní
  + (? polohu ***0*** volíme, ***1*** má inher., gener.)
* **racionální, poměrová**
  + spočitatelná míra nějaké vlastnosti
  + (hodnota aktiva; počet přímých útoků)
  + je kvantitativní
  + lze navíc spočítat, kolikrát je jedna hodn. větší než jiná
  + ***0*** je dána nepřítomností vlastnosti
  + pouze kladné hodnoty

**Lze vymyslet i něco jako měř. plán**

Prezentace výsledků – poznámky

* Systém a způsob určuje bezp. pol.
* Roční, Q, měsíční reporty
* Kdo jaké dělá a komu (které roli) předává

Shrnutí kroků k dosažení výsledku měření

Základní metriky a metody

Metrika je vždy dána vlastností objektu a metodou

Metoda: generický popis sledu operací pro zjištění vlastností objektu

Povaha operací:

* subjektivní
* objektivní

Operace: čítání výskytů, sled. času, audit, intrvw, …

Příklad odvozené metriky

* Cíl: vědomí zaměstn. o InfBez
* Základ. metrika:

počet zam. zařazených do školení

počet zam. úspěšných ve školení

**Odvoz. metrika**: ***trend*** v průběhu roku

**Kritéria**: aspoň 80 % úspěšných

Možné metriky dle 27004 (vždy + trendy)

* statistiky změn IT:
  + počty změn z důvodu nových rizik
  + počty návratů k předchozím řešením
  + počty ne/úspěš. změn vůči všem
* vyzrávání IT procesů
  + poločas aplikace bezp. záplat
* stat. dopadů malwaru
* stat. z ext. auditů:
  + počty doporučení
  + vážná odhalení dle závažnosti
  + akceptace doporučení
* stat. z int. auditů
* stat. z helpdesku:
  + počty a typy dotazů
  + počty žádostí o změnu hesla
* stat. bezp. incidentů:
  + průniky, pishingy
  + detekce a efekt. náprav
* stat. z firewallů:
  + přístupy na zakázané zdroje
  + počty hack. útoků
* stat. zranitelností:
  + počty zranit. míst
  + počty jejich objevů, likvidací
  + rychlost oprav záplatami
* M. pro aplikační bezpečnost
  + hodnocení přístup. práv uživatelů
  + omezování přístupu
  + separace prostředí: vývojového, …
  + počty BU a BI
  + přejímací testování systému

Účastníci měření:

* **klienti** měření: komu jsou výsl. měření určeny
* **vlastníci informací:** o měřených objektech
* **měřiči:** měří, shromažďují a uchovávají data
* **hodnotitel měření**: nejč. CISO:

validuje metodu a výsledky

* **interpretátoři:** manažeři odp. za ISMS

rovněž zveřejňují výsl.

Příklad měření:

Název: Obnova ze zálohy

Ev. číslo m. : xxxaaa

Cíl: důkaz, že obn. proběhne do 48 h

Měř. objekt: Záloh. procesy (zajišť. I a A)

Politika zálohování

Výčet obj. měření: O1: Správa požad. na obnovu

O2: Záznamy záloh. systému

Vlastnosti: O1: Požadavky na obnovu

O2: Čas startu a ukonč. obnovy

Metriky: Počet požadavků

Čas startu a ukončení

Počet provedených obnov

Metody: Načítání za měsíc

Záznam časů

Načítání obnov

Typy metod: Všechny jsou objektivní

Stupnice: int., nominální

y-m-d-t, intervalová

int., poměrová

Odvozené metriky: dovedu si představit

Měřící funkce: co se jak dělí, násobí, odečítá

KPI: různé poměry

Analytický model: různé barvy výsečí kol. grafu

Rozhod. kritéria: provést 100 % požad. na obnovu

všechny obnovy do 48 hod.

Interpr. indikátorů: vždy zjistit důvody, do zprávy

Účastníci: bezp. manž, IT odd.,

správce zál. syst., mnžr. ISMS

HMG: dovedu si představit

Zpráva: kol. grafy + koment.

Hodnocení InfBez

ISO 15408

Vyhodnocovací kritéria InfBezp:

1: Úvod a obecný model

2: Požadavky na bezp. **funkcionality**

3: Požadavky na bezp. **záruky**

Původně nazván CC (označení se často používá):

* Standardizovaný
* Uznávaný
* Opakovatelný
* Repro­du­kovatelný

Hodnotící kritéria:

Seznam podmínek, které musí plnit hodnocený produkt:

ToE: (*Target of Evaluation*):

ad 1: požadavky na model

ad 2: SFR – Security Functional Requirements

ad 3: SAR – Security Assurance Requirements

Určena pro:

* zadavatele veř. zakázek
* zákazníky: veř. zakázek
* uživ. sdružení pro specifikaci požadavků na bezp.
* zadavatele vývoje (vodítko, bezp. cíl), vývojáře
* hodnotitele produktů.

Předmět hodnocení: dva typy

(Předmětem hodnocení není systém řízení, ale: …)

* **produkt:** výrobek s konkrétním módem užívání
  + neznáme přesné požadavky uživatele
  + neznáme prostředí, kde bude p. užíván

(nutné zohlednit vš. uživatele #)

* **systém**: jedineč. kombinace produktů plnící urč. f-ci
  + požad. na funkč. a záruky jsou zadány
  + známe prostředí a co uživ. požaduje
  + deskripce požadavků je ale složitá

hodnocení jednorázové a drahé

Metody hodnocení: dvě koncepčně odlišné

* **produktově**/systémově orientované (investigativní)
  + zkoumá se jedn. produkt
  + indiv. pro každý produkt
* **procesně** orientované (auditní postup)
  + zkoumá se proces, dok-ce …
  + levnější, opakovatelné
  + doporučuje se i v 15408

Protection profile, PP

* je specifikační dokument spol. critérií, CC
* vytváří jej uživ. nebo komunita uživatelů
* specifikuje požadavky na bezpečnost:
  + pro jisté prostředí
  + pro jistou třídu zařízení (čip. karty, firewally)
  + v jistém prostředí a účelu
* může to být šablona pro def. bezp. cíle
* lze vyrábět jistý výrobek:
  + vyhovující specifickému PP
  + nebo stejný výr. s jiným PP.

Security target, ST

* také je specifikační dok. spol. critérií, CC
* vytváří ho výrobce/vývojář
* identifikuje bezpečn. vlastnosti cíle hodnocení (ToE)
* dosažitelný i přes více PP
* ST je mnohdy rekl. materiálem výrobce
* je možné hodnotit, zda ST vyhovuje zadanému PP

Security Functional Requirements (SFRs)

* specifikuje bezpečn. funkce spec. produktu
* v normě ex. katalog těchto funkcí, nepovinné
* Například:

SFR může spec. požadavky na autentizaci uživatele

(čipové karty, bank. webu)

* výrobek (TOE) se hodnotí podle toho,

jak splňuje SFR deklarované v ST

Security Assurance Requirements (SARs)

* popisuje měření během vývoje a hodnocení produktu
* k zajištění souladu s prohlášením o SFR
* Například:

aby všechny zdrojové kódy byly zdrženy

v organizačním systému.

Výstupem SAR jsou stupně EAL

*Evaluation assurance level*

**Co EAL hodnotí:**

* kvalitu specifikace
* doprovodnou dokumentaci
* správu konfigurace
* vývoj a testování
* kvalitu dodávky a implementace
* způsob provozu
* zranitelnost
* zajištění údržby
* udává hloubku hodnocení
* podporu životního cyklu
* nehodnotí sílu bezp. mechanismů!!

Jedn. stupně se liší hloubkou a důkladností procedur ověření. Každé úrovni odpovídá balík spec. požadavků.

**Požadovanou EAL si musí určit zákazník sám.**

**To norma neřeší.**

Stupně EAL:

**EAL1**

* nízká odolnost, nízké škody
* funkčně testovaný TOE
* bezchybný provoz v souladu s dok-cí
* hodnocení PP, ST bez účasti vývojáře
* za min. náklady
* příklad: evidence majetku

**EAL2**

* odolnost, škody: nízké
* strukturálně testovaný TOE
* nízká až střední záruka za bezpečnost
* není dostupná kompl. informace o vývoji,
* ale vývojář poskytne specifikace
* EAL1 + ověření výsledků testů vývojáře
* příklad: účto. SW, InfoSysDEA

**EAL3**

* odolnost, škody: znatelné
* metodicky testovaný a kontrolovaný TOE
* EAL2 +

přísněší testy bezpečn. funkcí

kontrola vývojového #

* příklad: bank. SW pro I-net banking

**EAL4**

* metodicky navrhnutý, test. a prozkoumaný TOE
* nejvyšší úroveň, kterou je možné dosáhnout zpětně

pro už existující produkt

* EAL3 +

low-level návrh

kontrola některých zdrojových kódů

- příklad: Windows 2000 SP3

**EAL5**

- semi-formálne navrhnutý a testovaný TOE

- prísne uplatnenie dobrej vývojárskej praxe

- EAL4 +

úplná implementácia TOE

analýza skrytých kanálov

semi-formálny návrh

**EAL6**

- EAL5 so semi-formálne overeným návrhom

- EAL5 +

modulárny a vrstvový návrh TOE

štrukturovaná implementácia

- pre ochranu aktív s vysokou hodnotou

vo vysoko rizikovýchh prostrediach

**EAL7**

- EAL6, ale formálne navrhnutý a overený

- formálny model bezpečnostnej politiky

- formálny detailný návrh

- white-box testy

- nezávislé potvrdenie výsledkov všetkých testov

Vlastnosti digitálních důkazů

**Relevancia**

- dokázať, že získaný materiál sa vzťahuje k šetreniu

- obsahuje informácie k vyšetrovaniu konkrétnej BU

- sú dobré dôvody pre to, aby bol získaný

**Reprodukovatelnsot**

- všetky procesy použité pri manipulácii s poten­cionálnymi dôkazmi majú byť reprodukovateľné

**Dostatočnosť**

- detektív si musí byť vedomý, že zhromaždil dosta­točné množstvo materiálu umožňujúceho riadne vyšetrovanie, ktoré sa má previesť

**Auditovateľnosť**

- DEFR/DES musí dokumentovať a zdôvodniť svoje akcie, aby nezávislý pozorovateľ mohol zhodnotiť, či boli adekvátne

**Opakovateľnosť**

- získavame rovnaké výsledky pri použití rovnakej metódy testovania, rovnakých nástrojov a za rovnakých podmienok

**Ospravedlniteľnosť**

- DEFR/DES musí zdôvodniť, že použité procesy boli správne a nevyhnutné a iný DEFR/DES by to mal potvrdiť zopakovaním procesov

Role pracující s digitálními důkazy

**DEFR: Digital Evidence First Responder:**

**„detektiv“**

* fyzická osoba, oprávněná, vyškolená a kvalifikovaná jednat jako první na scéně incidentu při shromažďování a získávání digitálních důkazů
* odpovědná za manipulaci s důkazy
* musí zaručit, že shromažďování a získávání důkazů neporušuje legislativní omezení

**DES: Digital Evidence Specialist**

**„vyšetřovatel“**

* fyzická osoba, která může provádět úkoly detektiva a má navíc odborné znalosti, dovednosti a schopnosti zvládnout širokou škálu technických problémů

**DEFR i DES musí**

* dokumentovat všechny své akce
* určit a použít metodu pro stanovení přesnosti a spolehlivosti potenciální digitální důkazové kopie oproti původnímu zdroji

Disaster recovery plan: Plán obnovy

jak postupovat po obnově činnosti IT po BI:

* **Kritéria** definující, co je BI
* **Odpovědnosti** za aktivaci obnovy jako **celku**
* **Odpovědnosti** za aktivaci **dílčích** činností
* **Návody** k provádění činností podle plánu obnovy

Informace – co je to

* široký, mnohoznačný pojem, v různých významech.
* obecně: [údaj](https://cs.wikipedia.org/wiki/%C3%9Adaj) o prostředí, jeho stavu a procesech v něm probíhajících
* inf-ce snižuje nebo odstraňuje [entropii](https://cs.wikipedia.org/wiki/Entropie) [systému](https://cs.wikipedia.org/wiki/Syst%C3%A9m)
* množství informace: jak se přijetím inf-ce změnila míra [neurčitosti](https://cs.wikipedia.org/wiki/Entropie) příjemce inf-ce

Užší významy

* **běžný život**: vědění, které lze předávat
* **věda**: vnímaný údaj o vlastnostech a uspořádání objektu ([negentropie](https://cs.wikipedia.org/w/index.php?title=Negentropie&action=edit&redlink=1" \o "Negentropie (stránka neexistuje)))
* [**informati**](https://cs.wikipedia.org/wiki/Informatika)**ka**: kódovaná data jako protiklad [šumu](https://cs.wikipedia.org/wiki/%C5%A0um)

lze je vysílat, přijímat, uchovávat a zpracovávat technickými prostředky

**množství informace:** rozdíl mezi neurčitostí (entropií) informace (nebo stavu) před a po zprávě.