Bezpečnost informačních systémů

Informační systém a jeho bezpečnost

Informační systém je označení pro soubor technických prostředků (hardwaru a softwaru), které dokážou **poskytovat** nebo **udržovat data** či **informace** pro požadovaný účel jeho uživatelům.

Informační systémy se mohou dělit podle několika skupin podle jejich účelu, přístupnosti nebo stupně automatizace.

Podle přístupnosti:

- **Veřejné**
  - Jsou přístupné veřejnosti
  - Wikipedie, veřejné knihony
- **Neveřejné**
  - Nejsou přístupné veřejnosti, ale pouze určenému okruhu uživatelů
  - Především se jedná o interní systémy firem nebo organizací

Podle účelu:

- **Podnikové**
  - Užívány v podnicích
  - Slouží pro pracovní procesy, pro zaměstnance
- **Osobní**
  - Informační systém, který slouží pro individuální záležitosti
- **Managerské**
  - Netříděné informace zobrazované v grafech, tabulkách nebo reportech
  - Především pro vyšší management firem
- **Knihovní**
  - Správa knih v knihovně
- **Geografické**
  - Systém pro sběr, uchovávání, třídění a analýzu dat, které znázorňují realitu pomocí map nebo topografických údajů
  - Může jít například o katastrální úřad
- **Veřejno správní**
  - Podporuje činnost výkonu výkonu veřejné zprávy

Podle automatizace:

- **Neautomatizované**
  - Systémy, které mají za úkol komunikovat a interagovat s uživatelem
  - Data se v nich dají lehce najít a snaží se a by data byly zobrazeny pro uživatele ve smysluplné formě

    - O zadání informací se tak tedy stará uživatel
- **Automatizované**
    - Systém, který je plně automatizovaný nevyžaduje zásah vnějších sil nebo interakci s uživatelem
    - Pracuje pouze se vstupními daty, ze kterých dokáže vypracovat výsledek, který je uživateli předložen

Takovéto informační systémy by měly mít patřičné zabezpečení proti vnějším útokům nebo špatnému zadaní dat do systému samotným uživatelem. Počítačovou bezpečností se rozumí stav, při kterém je dosaženo **dostupnosti**, **integritě**, **důvěrnosti** a **odpovědnosti**.Tyto čtyři stavy zabraňují ztrátě nebo zneužití našeho systému a dat v něm uložených.

- **Dostupnost** – data jsou dostupná autorizovaným uživatelům.
- **Integrita** - změnu dat smí provádět pouze autorizovaní uživatelé
- **Důvěrnost** - přístup k datům, mají pouze autorizovaní uživatelé
- **Odpovědnost** – uživatelé jsou odpovědní za své aktivity

Ochrana dat a zabezpečení počítače

Data je nutno chránit před kompromitací, modifikací nebo zničením.

- **Kompromitace** - chráníme důvěrnost dat
- **Modifikace** - chráníme data proti neoprávněné změně
- **Zničení** - chráníme data proti úmyslnému či neúmyslnému zničení

Systémy bychom měly ochránit před neoprávněným **fyzickým** i **logickým přístupem,** například **ověřením identity uživatele**, k datům, ke kterým by neměl mít přístup. Ochránit data je třeba i při přenosu na síti. Takovéto bezpečnosti se dá docílit například programy pro ochranu systému jako **antivir** nebo **firewall** a samotné data můžeme ochránit **šifrovacími** nebo **hashovacími funkcemi**.

Celý systém bychom měli také **monitorovat**, aby mohl být útok včas zjištěn, pokud už k průniku do systému dojde.

Hrozby

Hrozba je vlastnost prostředí, která může potencionálně způsobit narušení bezpečnosti našeho systému.

- **Neúmyslné**
    - Porucha hardwaru
    - Přírodní katastrofy
    - Výpadek napájení
    - Selhání obsluhy

- **Úmyslné**
    - Krádež hardwaru, jeho úmyslné poškození nebo zničení
    - Neoprávněná manipulace s daty
    - Krádež software
    - Viry

Útoky a typy útočníků

Všemožné útoky dokáží využít slabin systému a zneužít je pro získání informací nebo získání úplné kontroly nad cílovou informační technologií nebo člověkem. Útoky mohou být provedeny na počítačový systém, ale také na samotného člověka, ze kterého jsou tak vylákány třeba citlivé informace. Při takovýchto útocích může jít o **krádež**, **zneužití** nebo **neoprávněné užití dat**, **sabotáž**, **vydírání** nebo **špionáž**. Útoky mohou být rozděleny také na pasivní a aktivní. U pasivních se používá různých forem odposlechů(**spyware**, **packet sniffing**), které nevzbudí tak velké podezření protože nemanipulují s daty na cílovém systému. U aktivních útoků se útočník aktivně účastní při napadení daného systému, může jít například o **crackování** hesel nebo **DDoS**.

Útočníci mohou mít více úmyslů jak s ukradenými daty nebo napadeným systémem naloží. Můžeme je rozdělit do několika hlavních kategorií.

- **Black hat**
    - Je útočník, který daný systém chce zničit nebo naprosto vyřadit z provozu a snaží se způsobit druhé straně co největší škody jak už finanční nebo datové
- **Gray hat**
    - Je útočník, který útočí za účelem se obohatit
    - Většinou krade data aby je mohl prodat na černém trhu nebo proniká do systémů a po administrátorech poté požaduje určitou částku za opravu dané chyby
- **White hat**
    - Je útočník, který testuje bezpečnost systémů bez jakéhokoliv úmyslu krást nebo ničit data
    - Často se jedná o experty, kteří testují systémy a jsou za to různými korporacemi placeni
    - Užívá se také označení etický hacker

Hesla a biometrika

Hesla slouží pro **autentizaci** uživatele, což znamená jednoznačné určení identity daného uživatele. Autentizace může zahrnovat tři faktory. **Znalost** (heslo, pin, gesto), **Vlastnictví** (certifikát, mobil, karta, doklad totožnosti), **Biometrie** (otisk prstu, rozpoznání obličeje, snímání sítnice). Všech těchto faktorů lze využít třeba i najednou.

Hesla by měly splňovat určité podmínky pro to, aby mohla být označeny jako “silná”. Základními pravidly je užití velkých a malých písmen, číslic a dostatečného počtu znaků. Heslo by se také nemělo objevit na seznamu nejpoužívanějších hesel na internetu a nemělo by obsahovat často používané či předvídatelné fráze či slova.

Biometrika je technika identifikace lidí na základě jejich osobních charakteristik či vlastností. Může jít například o vlastnosti těla nebo chování. Příkladem může být otisk prstu nebo třeba dynamika podpisu. Charakteristiky člověka se odlišují v míře spolehlivosti. Takovéto údaje však leze zapomenout nebo ztratit a nekladou tak požadavky na uživatele, ale je pro ně nutný speciální hardware a software, který nemusí být stoprocentně spolehlivý.

Zálohování a archivace dat

Zálohování je operace, při které se vytváří kopie dat, aby uživatel předešel jejich úplné ztrátě. Uživatel počítá s blízkým využitím zálohovaných dat. Zpravidla se jedná o krátkodobé uchovávání dat.

Archivace je operace, při které se také vytváří kopie dat, ale nepočítá se s tím, že data budou v blizské době využity nebo požadovány. Zpravidla se jedná o dlouhodobé uchovávání dat.

Pravidla pro zálohování

- Je to nejúčinnější způsob ochrany dat
- Pro zálohování se používají specializované zálohovací programy
- Zálohovací programy jsou součástí operačních systémů, programy od jiných výrobců mohou mít větší rychlost a více funkcí
- Je třeba zvolit co nejtrvanlivější médium, které se mohou lišit od potřebné doby uchování dat

Malware a obrana proti němu

Malware je počítačový program, který se šíří bez vědomí uživatele a jeho úkolem je především škodit a šířit se. Přítomností v systému může způsobit zpomalení počítače, změnu informací nebo dat, zobrazování nežádoucího obsahu.

Program může například ovládnout napadený systém, vykonávat akce bez souhlasu uživatele a posílat tak například spam z napadeného počítače nebo se počítač může stát jedním z účastníků při DDoS útocích. Může také například zašifrovat nebo úplně zničit data za jejichž obnovu může požadovat finanční částku. Může také zůstat nezpozorován a dál se šířit v síti a pouze krást informace a posílat je útočníkům.

Antivir

Je software, který má za účel identifikaci, odstranění a eliminaci počítačových virů a jiného škodlivého softwaru. Může procházet soubory na lokálním disku a porovnávat je z databází virů nebo může aktivně monitorovat aktivitu sítě a odchytávat tak hrozby ještě předtím, než vůbec dojde k jejich zápisu na disk. Jedním z příkladů antivirových programů může být AVG, ESET nebo AVAST

Sociální inženýrství

Způsob manipulace lidí za účelem provedení určité akce ovlivňovanou osobu nebo získaní informace od ovlivněné osoby. Může mít několik forem, některé jsou přímé některé méně.

- **Pretexting**
    - Aplikace vymyšleného scénáře s cílem přesvědčit oběť k učinění dané akce nebo k získání potřebné informace
- **Phishing**
    - Jedná se o techniku, kdy je nasazen software, který se tváří jako známá stránka nebo aplikace a pouze čeká, než se nepozorní uživatelé nachytají a zadají své přihlašovací údaje do falešné aplikace.
- **Baiting**
    - Infikované fyzické zařízení je zanecháno na místě, které chce útočník infikovat, s popiskem vzbuzující zvědavost. Když se chce oběť na obsah fyzického zařízení podívat infikuje tak svůj počítač a potencionálně i celý informační systém, ke kterému je připojen.

Typy malwaru

- Backdoor
  - otevře některé porty počítače a naslouchá na nich povelům zvenčí
- Trojský kůň
  - Umožní získat útočníkovi přístup do počítače a pracovat s ním.
  - Password-stealing
    - monitoruje zadaná přihlašovací jména a hesla
  - Destruktivní
    - likvidace dat - mazání, přepisování, šifrování, nebo i zformátování celého disku s daty
  - Dropper
    - Uchovává v sobě jiné viry a po infikaci počítače je vypouští
  - Downloader
    - Stahuje další viry do počítače
  - Proxy
    - Promění infikovaný počítač na mail server a posílá spam
- Dataminer
  - Program, který shromažďuje data o činnosti uživatele počítače
- Keylogger
  - Software, který snímá stisky jednotlivých kláves
- Červ
  - Nevyžadují aktivitu uživatele, čekají v počítači, na to až uživatel nenainstaluje záplatu potřebnou pro ochranu proti červům
  - Velmi agresivní, rychle se replikuje
- Rootkit
  - Běží v jádru operačního systému, skrývá se v něm před antivirovými programy a protože je součástí operačního systému, tak se špatně odstraňuje i detekuje
- Boti
  - Používají se k distribuovaným útokům DoS nebo Spamu
- Logická bomba
  - Typicky ničí data, spouští se při splnění podmínky
- Ransomware
  - omezuje uživatelům přístup k jejich počítačovému systému nebo souborům a požaduje za přístup výkupné

Slavný malware

Christmas Tree

- První síťová epidemie
- Ukazoval obrázek vánočního stromu a přál pěkné vánoce
- Současně se rozesílal uživatelům sítě

Morris Worm

- Jeden z prvních červů, který pro šíření používal internet
- Původním úmyslem bylo spočítat počítače připojené k internetu
- Zahltil počítače připojené k internetu, virus se mohl více replikovat na jeden počítač
- Morris je prvním člověkem, který byl kvůli takovéto věci obviněn

ILOVEYOU

- E-mailový červ
- Rozesílal textový soubor jako přílohu v emailu
- Hledal čísla a hesla od kreditních karet

Stuxnet

- Profesionálně vytvořený červ
- Měl napadat jaderné elektrárny v Íránu, speciálně průmyslové systémy SCADA
- Kaspersky označuje tento vir jako začátek éry kybernetických válek

Etický hacker

Expert v oblasti IT, který je najmut firmou, aby úmyslně zkusil najít slabiny v systému firmy nebo korporace. Poté co je najde může korporace chyby systému opravit.

Slavné jména

Julian Assange

- Zakladatel wikileaks.org

Edward Snowden

- Bývalý zaměstnanec CIA, který odhalil celosvětový systém pro sledování