# 1. přednáška – Úvod do předmětu

***(Data, informace)*** *= data – údaje, text; informace – data v určitém kontextu (význam!)*

**Uložení dat** – disky, pásky (*furt se používaj!*), optická média, flash paměti
**Informační systém** – principy informačních systémů

- architektury:
  - agendové zpracování
  - klient/server *(web. stránky);* = třívrstvá architektura (*prezentační, aplikační, databázová*)
  - multi-tier IS (*vícevrstvá; + API/ap. logika; client, presentation, business service, data*)
  - cloudové IS

## *Útok, zranitelnost*

**Počítačová aktiva** – vše, co lze ohodnotit *(co může mít nějakou cenu)*

- hmotná *(např. HW)* i nehmotná *(např. SW, data)*, může být i vlastnost (dobré jméno, dostupnost, funkčnost); *otázka ocenění*
- podpůrná aktiva – podílející se na provozu *(jenom nástroj)*
- primární aktiva – poskytovaná služba

**Zranitelnost** – **slabé místo**, které je využito jednou či více hrozbami

- známé – opravené/neopravené
- neznámé – skryté/neobjevené
- jednání člověka, technická závada, zásah vyšší moci
- **Kybernetická hrozba** = možnost pokusu o poškození nebo narušení počítačové sítě nebo systému
  - Únik informace, narušení integrity (*integrita = neporušení*), potlačení služby (DoS; *nedostupnost*), nelegitimní použití (*dostane se tam někdo, kdo nemá oprávnění*)

**Hrozby** = *možnosti využití zranitelných míst*

- zdroje:
  - člověk – úmyslně/nedbalost (*zůstane přihlášený, omylem něco pošle, …*);
  - technické chyby (*v kódu*); vyšší moc (*selhání, které nemůžete ovlivnit*)
- zdroje působení – vnitřní/vnější

**Vynaložené prostředky** (*jaké prostředky byste měli vynaložit na ochranu dat?*)

- ochrana dat – semestrální práce vs. PayPal/ČSSZ
- metoda nákladová (*náklady na opatření by neměly přesáhnout možná rizika*)

**Typy hrozeb**

- sociální inženýrství; phishing *(souvisí spolu);* botnet (*síť počítačů infikovaných speciálním SW, řízeným z jednoho centra*); malware (*obecně škodlivý SW*); ransomware (*výkupné za přístup k datům*); spam; podvodné nabídky; hacking; sniffing (*sledování systému*);
- DoS (*Denial od Service*), DDoS (Distributed DoS), ReDoS (Regex DoS; *pomocí regulárních výrazů*),
- šíření závadného obsahu, identity theft, kyberterorismus, kybernetické výplatné či vydírání,
- APT (Advanced Persistent Threat – *počítač dělá nějakou nekalost a vy o tom nevíte*)

→ **Shrnutí**: *Je důležité identifikovat:* Co špatného (nežádoucího) se může stát? Co může selhat?
→ *Ale také:* Jaká je možnost/pravděpodobnost, že se to stane? *(riziko = pravděpodobnost využití zranitelného místa k útoku)*
→ *A:* Jak závažné mohou být účinky/dopady/následky?

# 2. přednáška – Kryptografie

→ = **skrývání informací**
→ jednosměrné *(zašifrování ale ne rozšifrování)* nebo obousměrné
→ symetrické/asymetrické šifrování

**Historie** – Polybiův čtverec *(tab 5x5; abeceda; souřadnice)*; Cézarova šifra *(posunutí v abecedě)*,
- **DES** *(Data Encryption Standard)* – proudová šifra (*stream; písmenko po písmenku, za běhu průběžné šifrování*) s 64bitovým klíčem; považována za nedůvěryhodnou, Triple DES jako náhrada (*šifrování 3x, vyšší odolnost*)
- **AES** *(Advanced ES)* – nástupce DES, používána v současnosti pro šifrování přenosů dat

**DH** (Diffie-Hellmann) bezpečná výměna klíčů (*barva symbolizuje funkci*)
- *Stejná barva; na každé straně se přimíchá vlastní jiná, pošle se druhé straně; každá strana přimíchá zase vlastní barvu → na obou stranách stejná barva*

**Steganografie** – ukrývání informací *na nečekaná místa (ne přímo šifrování)*
- se znalostí způsobu ukrytí lze informace odhalit
- ukládání do formy obrázků, videí, spustitelných souborů, inzeráty

## *Hashovací funkce*

→ cílem hashovací funkce je ***jednosměrné*** zašifrování textu libovolné délky do textu **přesně dané délky** *(obvykle 256-512 bitů)*
→ malá změna na vstupu znamená velkou změnu na výstupu
→ odolnost vůči kolizím (*kolize = dva různé dokumenty mají stejný hash*)
→ znemožnění kryptoanalýzy

**Využití** – kontrola integrity a ověření na dálku, ukládání hesel, autentizace, vyhledávání, jednoznačná identifikace

**MD5** – 128bit hash
- existuje algoritmus pro hledání kolizí (MD4/MD5)
- nevhodný pro ověřování integrity dokumentů

**SHA-1** – 160bit hash
- útok na něj v roce 2005
- již není akceptován v SSL

**SHA-2** – aktuálně doporučovaná verze SHA; SHA-224/SHA-256/SHA-384/SHA-512
- aktuálně používaný pro certifikáty a elektronický podpis

**Rainbow tables** – vypočítané tabulky slov a jejich hashů
- jednoduchá slova lze vyhledat na internetu; nepokrývají nesmyslná slova

---

*Symetrická (obě strany stejný klíč pro šifrování a dešifrování) x*

## *Asymetrická kryptografie*

→ založená nejen na ***privátním*** klíči *(dešifrování)*, ale také na ***veřejném*** *(šifrování)*
→ výpočetně náročná
→ z veřejného klíče neodvodíme privátní; ale z privátního lze vytvořit veřejný
→ data šifrovaná veřejným klíčem lze dešifrovat pouze privátním klíčem
→ **RSA** (*popis, ale nemluvil o tom*)

## *Kryptoanalýza*

→ zjištění původního textu ze šifrovaného textu

→ není použitelná u hashovacích funkcí; Enigma

- **Frekvenční analýza** – použitelná na šifry, kde je substituce vždy pevně daná
    - slovní frekvenční analýza, pokud známe rozdělení šifrovaného textu na slova a máme dostatečný vzorek
- **Znalost původního a šifrovaného textu**
    - využití pro symetrické šifry
    - slouží k odhalení šifrovacího klíče

**Kolize hashovacích funkcí**

- narozeninový paradox (*50% pravděpodobnost, že dva lidi v místnosti mají narozeniny ve stejný den → kolik lidí? = 23*)
- MD5 2^128 odpovídá 2^64;
- (*příklad zpráv se stejným hašovým kódem MD4 – stejná zpráva, ale různá částka v dolarech*)

**Shrnutí** – závislost na kvalitě hashovací funkce

- u symetrické šifry nutné průběžné výměny šifrovacích klíčů
- nezpochybnitelnost asymetrické kryptografie

# 3. přednáška – Autentizace

→ ***ověření totožnosti***; (***identifikace*** *= totožnost, např. xname, RČ;* ***autorizace*** *= oprávnění k činnosti)*

- **heslo** je nejpoužívanější autentizační metodou
- používání silných hesel? pravidelná obměna hesel?

## *Útoky na autentizaci:*

1) **Replay attack** – založen na odposlechu; přehrání komunikačního protokolu
2) **Man-in-the-middle** – narušení přímého běhu (*obrana = šifrování komunikace?*)
3) **Brute-force attack** – hromadné zasílání požadavků; více zapojených počítačů
4) **Slovníkový útok** – slova ze slovníků nebo předdefinovaných seznamů
5) **Shoulder-surfing** (*pohled přes rameno*)
6) **Útoky na integritu** (*ne na samotné heslo, ale na bezpečnost autentizačního protokolu/systém*)
    - na chyby v protokolech
    - code injection
    - chybné/podvržené vstupy naruší integritu systému
    - kontrola musí být prováděna na cílovém systému (ne na straně klienta)

## *Způsoby autentizace*

1) **Prokázání znalosti**
    - heslo, fráze; něco, co **víme**; mohou být snadno sdílena
    - **Hesla** – bud volně čitelná (plain text) nebo v podobě hashe;
        - solení – uživatel, sůl *(několik náhodných bitů)*, uložené heslo = hash(heslo+sůl) → *stejné heslo má pak několik různých zakódovaných variant*
    - **Protokol challenge-response**
        - server odešle sc (server challenge), klient odešle cc (client challenge)
        - klient spočítá odezvu **cr** = hash(**cc+sc**+secret)
        - server spočítá odezvu cr a porovná hodnotu s klientskou hodnotou
        - server spočítá odezvu serveru **sr** = hash(**sc+cc**+secret)
        - klient spočítá sr a porovná s hodnotou získanou ze serveru
2) **Prokázání vlastnictví** – vlastnictví tokenu, karty, telefonu; poštovní adresa; něco, co **máme**
    - **Čipové karty** – privátní klíč; klient podepisuje výzvu serveru; karta zodpovědná za podpis
        - nutné čtečky karet; karty chráněné PIN; MITM útok
    - **SMS/telefon** – jednorázová hesla zasílaná nezávislým kanálem; umístění SMS brány (vzdálená služba/brána); MITM útok

**One-time passwords** *(např. Google Authenticator, HW generátor OTP)*

- **HOTP** (HMAC-based OTP); událostí řízené OTP
    - *(OTP = hash(Tajemství+Počítadlo); (např. tlačítko; přidá, po kolikáté mačkáte tlačítko)*
    - resynchronizace; ověření protistrany
    - SHA1 hash, RFC4226 (redukce SHA1 na čísla)
- **TOTP** (Time-based OTP) počítadlo je nahrazeno časem;
    - časové okno platnosti; resynchronizace

**Předsdílená hesla** – náhodně generovaná hesla

- **S/KEY** – výchozí tajemství W; hash – P1 = H(W), P2 = H(P1), P3 = H(P2); výchozí taj. smazáno
    - na serveru uloženo Pn, klient používá hesla pozpátku od Pn-1
    - *klient pošle pn-1; server si to zahashuje a porovná s hodnotou pn, zapamatuje si pn-1*

**Závěr OTP** → není nutný dodatečný hardware; odolné odposlechu, bez potřeby instalace, jednoduché na použití; autentizace bez internetu,
→ MITM útok
→ omezení – heslo se nesní opakovat, jedinečné sdílené tajemství pro každý systém
→ autentizace třetí stranou (*registrace/přihlášení pomocí googlu, fb, …*)

3) **Prokázání vlastnosti** – něco/něčím **jsme**; specifická vlastnost těla;
   - rozpoznání obličeje, otisk prstu, rozpoznání oční duhovky
   - *FRR – False Reject Rate, FAR – False Accept Rate → kompromis mezi*

**Závěr**

- autentizace heslem – jedinečná, silná hesla
- OTP autentizace (*doplněk ke klasickému heslu*) – jedinečné sdílené tajemství, pro různé systémy
- doporučená vícefaktorová autentizace (*SMS, OTP, …*)
- biometrická autentizace pro kontaktní systémy (*docházkové systémy, mobilní telefon, …*)

# 4. přednáška – Hardwarové a softwarové zranitelnosti

## *HW a SW architektury*

***HW architektura***

**ENIAC** *(„sofistikovanější kalkulačka“; jednoúčelový)*

- 18 tisíc elektronek, 1 500 relé, 70 000 odporů, 2 letecké motory (*chlazení*),
- 30 tun, spotřeba řádově desítky kW (*dnes kolem stovky W*)

**Polovodičové součástky 1957** (*relé → tranzistor*)

- snížení spotřeby, zvýšení rychlosti (desítky-stovky operací za sekundu)
- vznik vyšších jazyků – COBOL, ALGOL
- vzájemná nekompatibilita

**Aktuální architektura** – integrované obvody

- stovky tisíc-miliony operací za sekundu
- magnetická média pro uchování dat, první disky
- jazyky LISP, Pascal
- modularity – sběrnice (*skupina vodičů, konektor – připojení jednotlivých modulů*)

*Porovnání architektur – Von Neumann vs. Harvard*

- *VN sdílená paměť pro program i data; H rozdělená (UEFI systémy; řídící jednotky v autech atd.)*

*Softwarová architektura: (obrázek – HW, nad tím systémový SW, nad tím aplikační SW)*

- *Aby si SW (OS) a HW rozuměl, jsou potřeba drivery (ovladače) – prostředník pro HW, napsán jazykem OS*
- *Aplikace nepracují s HW ale s OS*

**Vývoj hardwarových zařízení**

- původně jednoúčelová elektronická zařízení v podobě automatů
  - zařízení byla tzv. hard-coded, nebylo možné nastavení měnit
- přechod k mikroprocesorovým systémům
  - možnost aktualizovat firmware (ten má vlastní zranitelnosti – *řadič disku odesílající data*),
  - snazší rozšiřování funkcionalit

## *Softwarové zranitelnosti:*

**1) Injektáž (SQL, kódu)**

- *SQL injection*

```
select * from accounts where custID='VSTUP'

VSTUP=15
select * from acc@unts where custID='15'

VSTUP=' or '1'='1
select * from accounts where custID='' or '1'='1'
```

  - *na základě parametru od uživatele (15); pozmění vstup (‘‘ or ‘1‘ = ‘1‘)*
  - *buď znáte ten dotaz (zdrojový kód) nebo ne → blind, zkoušíte hádat*
- *Code injection*
  - *exec(“pgm“.$PARAM)  $PARAM=&& ls*
- pro útočníka je vhodné znát kód programu
- ochrana – důsledná kontrola validity vstupů *(např. otestování, jestli je vstup číslo)*

2) **Útok na uchování spojení v session a autentizaci**
   - *příklad s cookie UISAuth (k cookies se dostane i JavaScript)*
   - předávání session ID v URL
   - chybné ukončení session pro zavření prohlížeče, dlouhý timeout
   - únik databází s hesly
   - ochrana – důsledná kontrola platnosti session, hashování hesel a solení (salted hash)
   - multifaktorová autentizace
3) **XSS – Cross-site scripting**
   - spuštění útočníkova skriptu v prohlížeči jiného uživatele
   - ochrana – kontrola vstupů *(*escaping, validita podle typu vstupu*)*
4) **Útok na oprávnění**
   - *přepsal parametr id v URL (?)*
5) **Chybná konfigurace**
   - výchozí nezabezpečené účty
   - nesmazané instalační skripty
   - chybná konfigurace webového serveru *(výpis adresářů, konfig. souborů; záložní soubory skriptů (.bak) zobrazované klientovi, zapnuté debug info)*
   - nesmazané ukázkové aplikace, výchozí stránky
6) **Vystavení citlivých dat**
   - šifrování citlivých dat databázovými prostředky
   - krádež autentizační databáze
   - ne striktní využívání TLS na všech stránkách (krádež session ID)
7) **Nedostatečná detekce útoků**
   - automatické testování známých útoků automatickým scannerem
   - omezený počet pokusů na přihlášení
   - opakované chybné parametry
8) **Cross-site request forgery**
   - *příklad s profilem v moodlu (na server se odešle požadavek, server zjistí, že je ten uživatel přihlášenej, informaci pošle zpátky)*
9) **Zranitelné komponenty**
   - komponenty fungují s oprávněním aplikace
   - backdoor komponenta
   - důvěryhodnost vydavatele komponenty, analýza kódu
10) **Zranitelné API**
   - moderní aplikace komunikují přes API webové služby
   - zabezpečení vstupu viz SQL injection
   - důsledná kontrola oprávnění na straně serveru
   - reverse engineering (modifikace parametrů při volání služby)

## *Obrana*

1) **WAF** – webový aplikační firewall
   - ochrana před automatickými útoky (SQL injection, XSS, blacklisting)
   - umožnuje ochranu před opravou zranitelnosti v aplikaci
   - první stupeň ochrany webových služeb
2) **Doporučení pro obranu**
   - validace vstupů; běh procesů v izolovaném prostředí; aktualizace SW, WAF; automatizované periodické penetrační testy; ověření všeho, co věřit jde

# 5. přednáška – Zálohování dat

**Zálohování**

- ochrana dat před selháním hardware
- ochrana před modifikací (= archivace, verzování záloh)
- obnova dat – nutná kapacita, kam lze data obnovit

## *Média pro zálohování dat*

**Výběr nosiče** pro uložení záloh:

→ trvanlivost médií
→ náchylnost médií na zničení
→ kapacita média, přístup k datům

1) **Páskové jednotky**
   - více než 60 let
   - vysoká trvanlivost záznamu
   - nevýhodou sekvenční přístup
   - kapacity řádově TB až desítky TB
2) **Magnetické disky** – rychlý náhodný přístup k datům
   - náchylnější na poškození, vysoká hustota dat
   - kapacita až cca 10TB, sdružování do polí
3) **NAS úložiště** – síťová datová úložiště
   - umožňují zapojení více disků do RAID polí
   - vhodná pro menší až střední pole
   - hot-swap disky, integrace s majoritními systémy
4) **Flash paměti** – NAND paměti, omezený počet opakovaných přepisů
   - rychlý náhodný přístup
   - omezená kapacita (2TB/32tisíc)
   - problematická trvanlivost záznamu
   - v případě poškození problematická obnova
5) **SAN pole** – disková pole
   - dle typu, Block-level přístup, propojení fibre channel
6) **Optická média** – CD, DVD, blu-ray
   - kapacita až 100 GB, vypalování/lisovaná média
   - data uložena ve spirále

## *Zálohovací techniky*

→ fyzický způsob provedení zálohy
→ dle způsobu rozložení záloh

1) **Úplná záloha** – zálohuje celý obraz aktuálních dat
   - je nejnáročnější na objem zálohovaných dat a datový přenos
   - nejjednodušší obnova, bitová kopie disku
2) **Inkrementální záloha**
   - obsahuje poslední plnou zálohu a změny za jednotlivé časové úseky mezi zálohami
   - pro obnovu je potřeba plná záloha a všechny inkrementální/přírůstkové zálohy
3) **Rozdílová záloha** – rozdíl mezi poslední plnou zálohou a aktuální zálohou
   - k obnově stačí plná záloha a poslední rozdílová
4) **RAID pole**
   - Redundant Array of Independent Discs

***RAID 0*** – bez ochrany proti selhání (*pro zrychlení*)

- rozdělení dat mezi jednotlivé disky
- zvýšená efektivita při čtení i zápisu
- selhání části pole zničí celé pole

***RAID 1*** – mirroring

- zrcadlení dat
- nejvyšší ztráty na kapacitě (dvojnásobná velikost oproti zálohované kapacitě)

***RAID 10/1+0*** – zrcadlené stripování disků

- kombinace předchozích metod

***RAID 3,4*** – pole s paritním diskem

- v případě výpadku disku lze chybějící data dopočítat (*parita – kontrolní součet*)
- rozdíl 3 a 4 ve výpočtu parity

***RAID 5*** – parita je rozpočítána, rozložena mezi jednotlivé disky

- vysoká rychlost zápisu
- v současnosti nejpoužívanější typ

7) **Vzdálené zálohování**
   - ukládání do vzdáleného úložiště pro případ lokální ztráty dat
8) **Rotace záloh** – slouží k archivaci
   - odolnost proti náhodné modifikaci/smazání dat
   - schéma závisí na potřebách a politikách organizace
9) **Zálohování v cloudu** – odesílání dat do distribuovaného úložiště na internetu
   - omezený dohled nad přístupem k datům
   - pravidelné platby za úložiště dat

***Cloudová úložiště souborů*** – Google Drive, Microsoft OneDrive; zachování předchozích verzí souborů (částečná ochrana před ransomware); přístup k souborům odkudkoliv
***Specializovaná úložiště záloh*** – iDrive, Acronis True Image, Veeam Backup

## *Ochrana záloh*

**Fyzické zabezpečení** médií

- proti krádeži
- proti náhodnému zničení/katastrofě
- před zneužitím pracovníkem s přístupem k médiím – šifrovací záloha
- vhodné podmínky pro uchování záloh (vlhkost a teplota, sluneční světlo)

**Zabezpečení vzdáleného přístupu** k médiím (cloud, SAN, síťová úložiště)

- důvěryhodnost poskytovatele vzdáleného systému
- individuální účty záloh pro jednotlivé systémy
- šifrování uložených dat

# 6. přednáška – Ochrana dat v OS

**Přístupová oprávnění:**

- zajišťuje operační systém
- ochrana je pouze logická
- při vložení do jiného počítače je ochrana neúčinná

**Šifrovaný souborový systém**

- šifrování symetrickou kryptografií

## *OS Linux*

→ nastavení práv na úrovni **uživatele** a **skupiny** uživatele
→ ACL nadstavba
→ šifrovaný souborový systém

1) **Systém uživatelů**
   - uživatel root (*správce celého systému, neomezený přístup*); běžný uživatel
   - uživatel má přiřazenou (*právě jednu*) primární skupinu a další skupiny
   - hesla uložena ve formě hashe salt+heslo (více uživatelů se shodným heslem – různý hash)
2) **Přístupová práva**
   - **Práva na úrovni souborového systému**
     - nepoužívá dědění oprávnění
     - soubory a adresáře mají nastavené oprávnění pro: vlastníka, skupinu, ostatní
     - možná oprávnění: **r** (read), **w** (write), **x** (execute/vstup do adresáře)
     - změnu oprávnění může provést root nebo vlastník (*pomocí bitové masky*)
     - ***sticky bit*** – při nastavení u adresáře mohou uživatelé v adresáři modifikovat/mazat pouze soubory, jejichž jsou vlastníci
     - ***setgid*** (*set group id*) – skupina, která se nastaví pro nově vytvořené soubory (standardně se jako skupina nastavuje primární skupiny uživatele)
   - **ACL** – použitelné pro majoritní souborové systémy
     - ***setfacl*** – modifikace oprávnění pro další uživatele
     - ***getfacl*** – výpis oprávnění pro zvolený soubor
     - umožňuje výchozí práva pro dědění oprávnění z rodičovského adresáře
3) **Šifrovaný souborový systém**
   - šifrování symetrickou kryptografií (AES)
   - možnost šifrovat oddíl
   - při připojování oddílu (mount) je nutné zadat heslo
   - nejsou šifrována data pro bootování systému

## *OS Windows*

→ nastavení oprávnění k souborům a složkám
→ nastavení oprávnění ke sdílenému prostředku
→ transparentní šifrování souborů; historie souborů

1) **Oprávnění v souborovém systému**
   - využívá dědičnosti
   - dědičnost lze přerušit, nebo lze naopak přepsat podřízených objektů při změně nadřazeného oprávnění
   - vlastník má neomezený přístup (může si nastavit libovolná oprávnění)

- oprávnění pro uživatele a skupiny uživatelů
- vlastnictví souboru může převzít administrátor
- oprávnění lze přidělit nebo naopak odepřít
- systém oprávnění; nastavitelná oprávnění; auditování; oprávnění sdílení

2) **Šifrovaný systém EFS**
   - šifruje data symetrickou šifrou AES (*šifrovací klíč = symetrický*)
   - asymetricky je šifrován šifrovací klíč (*veřejným klíčem uživatele*)
   - heslo uživatele je součástí privátního klíče uživatele, bez znalosti hesla tedy není možné dešifrování šifrovacího klíče

## *Šifrované disky*

→ pevné disky s hardwarovým šifrováním (vestavěný kryptoprocesor)
→ většinou se vyskytuje u USB disků
→ podporuje některá NAS zařízení, AES šifrování

# 7. přednáška – Počítačové viry

→ **malware** je obecný název pro škodlivý kód
→ **počítačový virus** je specifický typ malware
→ hlavní důvody pro vznik virů: výdělek, mazání dat, krádež dat, krádež identity

---

**1) Dle uložení v paměti**

- rezidentní – zůstávají v paměti; vytváří více instancí, které se kontrolují navzájem
- nerezidentní – spuštěné s konkrétním programem

**2) Podle místa nákazy:**

- bootovací viry – jsou přítomny v paměti před spuštěním OS; omezený přístup do OS
- souborové viry – závislé na konkrétním OS
- multiparitní viry – kombinují výhody obou předchozích
- makroviry – využívají schopnosti vybraných softwarů spouštět kód – MS Office

**3) Podle chování:**

- stealth viry – rezidentní část viru schovává výskyty virů v souborovém systému
- polymorfní viry – mění svůj otisk – každá instance je unikátní

---

**Trojské koně** – nedokážou se samy šířit; spustitelný soubor, který si uživatel dobrovolně stáhne a spustí

- Pro kradení hesel – keyloggery, mouseloggery, zachytávání obrazovky, vyhledávání uložených hesel
- Destruktivní – mažou nebo šifrují data v počítači
- Backdoor/zadní vrátka – umožňují vzdálené ovládání počítače
  - agenti pro hacking team
  - počítač může být vzdáleně ovládán, vymazán

**Červi** – používají sítě a internet pro svoje automatické šíření

- využívají bezpečnostních děr v operačních systémech a routerech
- extrémně rychlé šíření, 6 stupňů volnosti

**Rootkity** – maskují se jako služby systému

- často ve formě ovladačů
- obtížné na detekci, přístup k periferiím, SONY BMG XPC

**Crimeware** – krádež identity, pomocí webových stránek

- exploity – využívají bezpečnostních děr

**Phishing** – snaží se přimět uživatele k zaslání citlivých údajů

- často ve formě e-mailů; případně ve formě telefonátů

**Spyware** – sledování činnosti uživatelů

- trojské koně, adware, tracking cookies

**Adware** – kanál k šíření reklamy

- pro zvýšení příjmů zadavatelů reklam
- ve formě pluginů s běžnými programy
- ve standardních distribucích výrobců hardware

**Spam** – nevyžádaná pošta ve formě e-mailu, ve formě příspěvků v diskuzních fórech

- nízké náklady, předmětem právního omezení v mnoha zemích

**Ransomware** – způsob zpeněžování počítačových virů
- šifruje důležité soubory – dokumenty, fotky, databáze
- obsahuje informace, jak zaplatit a dostat se ke klíči k rozšifrování
- ochrana – zálohování, Windows OS stínové kopie, historie souborů

**Hoax** – klamná/falešná informace
- některé mohou být destruktivní
- šíření, sociální sítě, e-maily, dopisy

## *Ochrana proti malware*

**1) Na úrovni OS**
- instalované záplaty, spuštění ověřených souborů
- používání nejnižších možných oprávnění
- nepoužívání crackových aplikací

**2) Antivirový software** – základní počítačová ochrana
- aktualizované definice virů
- rychlost šíření viru, sandboxing

**3) Firewall** – ochrana před SPAM a antivirová ochrana
- povolení pouze ověřeným programům, otevření pouze žádoucích reportů
- ochrana proti DDoS
- SPI – stateful packet inspection

**4) Analýza webových stránek**
- DNS sec, IP blacklisting, content analysing

**5) Ochrana proti spamu** – host v hlavičce HELO
- DNS-MAX, DKIM podpis
- používání SPE, greylisting, IP black/white listing

# 8. přednáška – Bezpečnost síťové komunikace

**HTTP/HTTPS**

- Hypertext Transfer Protocol, bezestavový protokol
- **HTTP** neposkytuje možnost šifrování
- **HTTPS** je rozšířen o SSL/TLS vrstvu
- Předávání parametrů – GET – přenášené v URL požadavku, POST – přenášené v těle

**HTTPS**

- vzájemné ověření protistrany
- asymetrická kryptografie použita pro výměnu klíčů
- ověření protistrany certifikátem CA; původně SSL, dnes TLS
- zajištění integrity přenášených stránek
- důvěrnost přenášených dat
- zranitelnost při vynuceném downgradingu
- nutnost certifikátů, výkonnostní vliv
- nutnost pro některé služby (poloha, přihlašovací údaje)

– **SSL** – Secure Socket Layer
  - mezivrstva mezi transportní a aplikační vrstvou
  - šifrování a autentizace

– **TLS** – následník protokolu SSL
  - TLS 1.0 jako SSL 3.0, další TLS výrazně zvyšují bezpečnost

**SSH** – Secure shell

- zabezpečený komunikační protokol
- přístup ke vzdálenému terminálu
- tunelování přes SSH – reverzní tunelování, tunelování přes gateway

**SMTP** = *Simple Mail Transfer Protocol*
**+ TLS** – protokol SMTP přes zabezpečený přenos dat

– šifrovaný přenos hesla
– podobně jako u HTTPS problém s dowgradingem
– přenos samotného e-mailu ze serveru

**Telnet** – pro připojení ke vzdáleným terminálům

– na principu příkaz – odpověď
– nastavování vzdálených služeb
– používání nedoporučeno (nahrazeno SSH)

**FTP** – slouží k přenosu souborů

– možnost zabezpečeného přenosu přes SSH
– FTP s podporou SSL
– ***příkazy*:** MKD – vytvoření adresáře; USER – uživatel, PASS – heslo;
  - PASV – pasivní mód, DELE – smazat, LIST – výpis adresáře;
  - RETR – stažení souboru, CWD – změna adresáře

– **Aktivní a pasivní režim:**
  - standardně v FTP navazuje spojení server s klientem
  - klient osloví server a následně se k němu server připojí
  - pokud není možné iniciovat spojení směrem ke klientovi, je nutné použít pasivní režim

**VPN** – umožňuje bezpečné tunelování dat v nezabezpečeném prostředí

- pakety jsou zabaleny do šifrovaných kanálů
- možnost bezpečného propojení sítí nebo spojení klient-síť

**IPSec** – oba konce tunelu jsou rovnocenné

- přesdílený klíč
- definice propojovaných sítí

**PPTP** – snadná konfigurace

- využíván u vytáčených připojení a DSL
- 2012 prolomení MS-CHAPv2 (DES šifrování

**L2TP** – tunelování na 2. vrstvě

- komunikace přes UDP
- nejčastější forma je L2TP/IPSec
- nezávislost na aplikačních protokolech

# 9. přednáška – Elektronický podpis

→ zajišťuje autenticitu, integritu, nepopiratelnost, časový rámec
→ podepisované údaje – e-mail, dokumenty, požadavky při volání služeb

## *Certifikáty*

- certifikují příslušnost otisku veřejného klíče ke konkrétní osobě – **osobní** certifikát
- **systémový** certifikát – elektronická pečeť
- kvalifikované certifikáty vydávané v souladu se zákonem
- komerční certifikáty pro širší využití

**Hierarchie** – kořenové/podřízené certifikační autority

**Osobní certifikát** – jednoznačně spojuje veřejný klíč s konkrétní osobou
– pro vystavení nutná osobní návštěva, ověření totožnosti
– lze prodloužit před koncem
– může obsahovat údaje o osobě a přiřazení společnosti

**Služby vytvářející důvěru** – (*EU definice*) elektronická služba, zpravidla za úplatu a spočívá:
– vytváření, ověřování shody a platnosti podpisů, razítek a služeb
– certifikace pro autentizaci internetových stránek nebo uchovávání podpisů

**Uložení privátního klíče** – úložiště s nemožností exportu klíče
– informace o uložení klíče v bezpečném úložišti je součástí certifikátu
– nelze tedy mít privátní klič v souboru nebo úložišti

**Certifikát pro elektronickou pečeť** – dříve systémový certifikát
– vystaven pro organizaci, pro automatizované zpracování
– není spojený s konkrétní osobou
– není kvalifikovaným certifikátem podle eIDAS

**Platnost a odvolání certifikátu**
– omezená doba (1-3 roky)
– při podezření odcizení lze odvolat

## *Certifikační autority*

→ vystavují certifikáty k otiskům veřejných klíčů
→ důvěryhodnost certifikačních autorit je klíčem pro důvěryhodnost podpisu

- **České** (*3*)
  - První certifikační autorita (*ica.cz*), Česká pošta s.p., eIdentity a.s.
- **Certifikační autority EU**
  - v rámci EU musí být uznávány všechny certifikáty vydávané certifikačními autoritami registrovanými v členských státech jako důvěryhodné
- **Celosvětové certifikační autority:**
  - GeoTrust, Comodo, RapidSSL
  - Thawte, Symantec
- **Nedůvěryhodné CA** – DigiNotar
  - součást nizozemského e-governmentu
  - pomalá reakce na incident (měsíc snaha o utajení)
  - ztratil akreditaci, certifikáty považovány za nedůvěryhodné

## *Časová razítka*

- datum a čas podepsání dokumentu
- ověřují, že zpráva v okamžiku připojení razítka již existovala *v této podobě*
- nejedná se však o čas vzniku dokumentu
- údaj o časovém razítku je připojen k podpisu dokumentu

**Poskytovatelé** – PostSignum dle počtu razítek: 1-30 – 120 Kč, 1001-3500 – 6500 Kč

- Comodo CA Code Signing timestamp

# 10. přednáška – Bezpečnostní systémy

## *SIEM*

→ Security Information and Event Management; původně SIM a SEM
→ *Sbírají informace a na jejich základě rozhodují, co dál*

**Požadavky na SIEM**
- identifikace zdrojů: strukturované logy, SNMP systémy, nestrukturované textové soubory
- počet událostí za sekundu
- velikost logu, archivace a retence
- dostupnost SIEM řešení

**Nasazení** – výběr vhodného řešení na základě požadavků ze vstupní analýzy
- identifikace předdefinovaných logovacích systémů
- parsování specifických logů
- výběr hardware pro monitoring

**Udržitelnost a rozvoj**
- dokumentace stávajícího systému
- identifikace a kategorizace rizik
- vytvoření pravidel pro události; automatické akce při změně stavu
- průběžná aktualizace při změnách v systémech; pravidelné testování funkčnosti
- ulehčení „rutinní práce“ – **automatizace procesů**

**Forenzní sklady** – uchování dat z logů pro prokazování událostí v systémech
- zabezpečení forenzních skladů (read only)
- součást SIEM systémů
- podklady pro CESNET, CSIRT, Policii
- prokazování incidentů zaměstnanců, útočníků

## *DLP*

→ Data Loss Prevention; síťová DLP, DLP koncových zdrojů

**Síťová DLP** – DLP na rozhraní sítě
- analýza procházející komunikace – e-mail, FTP, HTTP/HTTPs
- snazší implementace v jednom nebo několika málo bodech
- integrace s firewallem
- problém šifrované komunikace
- ve formě HW nebo SW

**DLP koncových bodů** – obdoba antivirového programu na stanici
- kontrola portů – tiskárny, USB; kontrola přístupu na CD/DVD; kontrola vnitřní komunikace; kontrola messengerů
- náročnější implementace a údržba

**Analýza požadavků na DLP**
- identifikace citlivých dat (smlouvy, tabulky, klíčová slova, množství dat v tabulkách)
- řešení incidentů – verifikace operace u samotného uživatele (prevence lidské chyby)
- politiky zacházení s externími disky (požadavky na šifrování dat)

**Implementace DLP**

- výběr řešení (network/endpoint)
- minimalizace false-positive incidentů (s rostoucím počtem falešných upozornění roste pravděpodobnost opomenutí)
- kontrola tisku dokumentů
- kontrola přístupu k datům v cloudových systémech

## *IPS/IDS*

→ původně Intrusion Detection Systems; nyní spíše Intrusion Prevention Systems

**Síťové IPS** – kontrola provozu v počítačové síti

- analýza provozních anomálií
- kontrola zranitelnosti aplikací
- kontrola chyb v protokolech (obrana před DDoS útoky)
- kontrola signatur – předdefinovaných vzorků známých útoků

**IPS koncových stanic** – individuální ochrana jednotlivých stanic

- analýza chování systému a detekce anomálií – lze odhalit již aktivní útok
- bývá součástí antivirových řešení jako HIPS (Host-based Intrusion Prevention)

**Spolupráce s ostatními systémy**

- integrace do firewallů na routerech
- nastavení pravidla firewallu reagující na probíhající útok
- zapojení IPS systémů do cloudových systémů – informace ze senzorů ze sítě
- dynamická aktualizace signatur, zrychlení detekce průniku
- izolace (karanténa) nakažených částí

## *UTM*

→ Unified Threat Management

→ sjednocení bezpečnostních systémů pro menší společnosti

**Součásti UTM** – firewall, VPN, IPS, antivirus, antispam, content-filtering

**Možnosti nasazení**

- nasazení v menším provozu – není potřeba výkonný hardware pro zpracování a logů a testování v reálném čase
- pravidelné roční platby za aktualizace signatur (jako u antivirových řešení)