



---

# OBSAH

1. Úvod a ciele kurzu
  2. **Časť 1: Základy digitálnej bezpečnosti pre bežného používateľa**
    - Pochopenie hrozieb: Malvér, Ransomvér, Spyvér
    - Prvá línia obrany: Heslá, 2FA, Aktualizácie
    - Príprava na najhoršie: Zálohovanie dát
  3. **Časť 2: Základy správy bezpečnosti systémov**
    - Rozlíšenie pojmov: Hrozba, Zraniteľnosť, Riziko
    - Proaktívna obrana: Skenovanie vs. Penetračné testovanie
    - Bezpečnostné technológie: Firewally, IDS/IPS
  4. **Záver a kľúčové poznatky**
-

---

# CIEĽ PREDNÁŠKY

- **Časť 1: Bežný používateľ (Úroveň 1)**
    - Poskytnúť netechnickému používateľovi základné vedomosti na ochranu jeho digitálneho života.
    - Zameranie na praktické a vysoko účinné kroky bez odborného žargónu.
  - **Časť 2: Správca systémov / Odborný zamestnanec**
    - Poskytnúť hlbší pohľad na terminológiu, procesy a technológie v kybernetickej bezpečnosti.
  - **Spoločný cieľ:** Budovať odolnú a bezpečnú digitálnu spoločnosť prostredníctvom vzdelaných používateľov a kompetentných správcov.
-

---

# **ČASŤ I**

## **ZÁKLADY PRE BEŽNÉHO POUŽÍVATEĽA**

---

---

# **POROZUMENIE HROZBÁM**

## **POROZUMENIE VÁŠMU DIGITÁLNEMU SVETU: HROZBY A OBRANA**

- V digitálnom svete existuje množstvo hrozieb, ktoré môžu ohroziť vaše osobné údaje a zariadenia.
  - Pochopenie ich základných typov je prvým krokom k účinnej ochrane.
-

---

## Prečo riešime zraniteľnosti?

- Útočníci dokážu začať zneužívať kritické zraniteľnosti často už **do 24–48 hodín** od ich zverejnenia.
  - Významná časť útokov začína zneužitím **známej, ale neopravenej zraniteľnosti** (cca 30–40 % podľa rôznych štúdií).
  - Najjednoduchší spôsob obrany? **Aktualizácie a záplaty.**
-

---

# Typy zraniteľností

- **Softvérové a hardvérové zraniteľnosti:** Chyby v kóde aplikácií, operačných systémov alebo firmvéru zariadení. Často majú pridelené označenie (CVE) a vyžadujú záplatu od výrobcu.
  - **Konfiguračné zraniteľnosti:** Slabiny spôsobené nesprávnym nastavením systémov administrátorom alebo používateľom. Nejde o chybu softvéru, ale o chybné nastavenie.
  - **Procesné zraniteľnosti:** Nedostatky v interných postupoch a procesoch organizácie. Vyplývajú z ľudských faktorov alebo chýbajúcich kontrol.
  - **Ľudské (sociálne) zraniteľnosti:** Slabiny prameniace z omylov používateľov alebo ich oklamania. Útočníci využívajú sociálne inžinierstvo.
- 
- Príklady: buffer overflow v aplikácii, SQL injection na webe, zraniteľnosť procesora (Meltdown/Spectre).
  - Príklady: ponechané predvolené heslá, otvorené porty/firewall nastavený „allow all“, vypnuté bezpečnostné funkcie.
  - Príklady: neexistuje proces na odoberanie prístupov po odchode zamestnanca, neformálne nasadzovanie zmien bez testovania, chýbajúce školenia o bezpečnosti.
  - napr. phishing – aby obišli technické zabezpečenia. (Tieto nezalátate patchom, vyžadujú tréning a povedomie.)

---

# Vzťah zraniteľností a bezpečnostných aktualizácií

- **Zraniteľnosť** → **Záplata**: Väčšina softvérových zraniteľností sa rieši vydaním bezpečnostnej aktualizácie (patchu). Záplata je oprava kódu, ktorá danú chybu odstraňuje.
  - **Patch management = core**: Riadenie záplat je kľúčovou súčasťou manažmentu zraniteľností – cieľom je aplikovať patch čo najskôr po jeho vydaní, aby sa okno na zneužitie zmenšilo.
  - **Nie všetko sa dá “zaplátať”**: Pre niektoré zraniteľnosti patch neexistuje (0-day) alebo nejde aplikovať (legacy systém). Vtedy musíme riziko znižovať inak (konfigurácia, kompenzačné opatrenia,...).
  - **Neaplikovaná záplata = pretrvávajúca zraniteľnosť**: Ak vendor vydá opravu, no my ju nenasadíme, zostávame zraniteľní.
- 

Príklad zo života: Po odchode administrátora z firmy nik nezrušil jeho VPN prístup a účty. Toto nie je „bug“ v IT systéme, ale vážna procesná chyba. O pol roka neskôr ten človek (alebo niekto, kto získal jeho staré poverenia) mohol stále prísť do siete – to je zraniteľnosť! A stala sa kvôli chýbajúcemu procesu na odobratie prístupov. Podobne často vidíme, že firmy nemajú proces na testovanie záloh – roky sa nerobia obnovy nanečisto. Keď potom príde incident (napr. ransomware), zistia, že zálohy sú neúplné alebo nefunkčné – to bola latentná zraniteľnosť procesu zálohovania.

- Ďalší príklad: Chýba politika update managementu – každý admin si záplatuje servery po svojom alebo vôbec. Výsledkom je nejednotný stav, niektoré servery sú roky bez patchov. To je procesné zlyhanie (chýba riadenie). Technicky je možno každý server v poriadku, ale proces “udržiavať všetko aktuálne” neexistuje alebo zlyháva.
- Procesné zraniteľnosti sú ľahko prehliadnuteľné, lebo neblíkajú ako kritické CVE v reporte. Vyžadujú analýzu pracovných postupov a interných pravidiel. Bezpečnostné audity a certifikácie (napr. ISO 27001) sa práve zameriavajú aj na tieto organizačné aspekty – pýtajú sa, či máte proces riadenia zraniteľností, proces zálohovania, reakcie na incidenty atď. Ak nie, auditor vytkne medzeru v procese, lebo to je rovnako dôležité ako technické opatrenia.
- Ako tieto zraniteľnosti riešiť? Podobne ako softvérové – najprv ich musíme identifikovať (napr. formou auditov, kontrolou súladu s normami), potom vyhodnotiť riziko (čo by sa stalo, ak proces zlyhá) a prijať opatrenia. Niekedy stačí zaviesť jednoduchú kontrolu (napr. štvrťročne prejsť zoznam účtov a zrušiť nepotrebné), inokedy väčšiu vec (napísať a zaviesť novú smernicu).

- Z praxe: Medzi najčastejšie prehliadané procesné slabiny patrí neexistujúci pravidelný audit prístupov, absencia bezpečnostných školení pre zamestnancov, chýbajúci plán obnovy po incidente, obchádzanie formálneho procesu zmien (admini niečo menia bez posúdenia dopadu) a podobne. Odstránenie týchto slabín často nevyžaduje drahé technológie, ale manažérsky dôraz a disciplínu. Preto je dôležité komunikovať vedeniu, že investície do procesov (čas, školenia, kontroly) sú rovnako potrebné ako investície do firewallov a antivírusov.

---

# Zero-day vs N-day

- **Zero-day zraniteľnosť**

- Neznáma chyba → neexistuje záplata.
- Objavená útočníkom alebo výskumníkom v deň nula.
- Vysoké riziko, ale **zriedkavý typ útoku**.
- Obrana: segmentácia, hardening, IDS/IPS, behaviorálna detekcia.

- **N-day (známa) zraniteľnosť**

- Chyba je **už verejne známa**.
  - Záplata existuje – problém je neaplikovanie.
  - Najčastejšie zneužívaný typ zraniteľnosti.
  - Obrana: patch management, prioritizácia, RBVM.
-

---

## Zero-click útoky

- Najpokročilejší typ útoku – **obete nemusia nič spraviť**.
  - Aktivuje sa automaticky pri prijatí správy alebo dát.
  - Využíva špecifické **zero-day chyby** v komunikačných aplikáciách (iMessage, WhatsApp, MMS, e-mail, VoIP).
  - Obeť nemá šancu útok rozpoznať ani zastaviť.
  - Nepomáha opatrnosť, nekliknutie ani ignorácia správy.
-

---

## ČO JE MALVÉR?

### Definícia: Malvér (Malware)

- **Malvér** je zastrešujúci pojem pre akýkoľvek „škodlivý softvér“ (z anglického *malicious software*).
  - **Cieľ:** Poškodiť, narušiť alebo kontaminovať počítačové systémy, často s cieľom prevziať čiastočnú kontrolu nad zariadením.
  - **Motívy:** Finančný zisk, sabotáž, politické vyhlásenia.
  - **Dôsledky:** Malvér môže kraťnúť, šifrovať alebo mazať vaše údaje, meniť funkcie počítača a špehovať vašu aktivitu.
- 

Podme teraz k pojmu **malvér**. Už sme ho párkrát spomenuli, tak si ho presne definujme. **Malvér** (z anglického *malicious software*) je súhrnný názov pre každý **škodlivý softvér** – čiže program, ktorý je zámerne vytvorený na to, aby **poškodil alebo zneužil počítačové systémy**. Pod malvér patria rôzne kategórie: vírusy, červy, trójsky kôň, spyware, ransomware, adware a ďalšie. **Cieľom malvéru** býva napríklad **prevziať kontrolu nad vašim zariadením**, kraťnúť údaje, špehovať vás, alebo spôsobiť nejakú škodu. Motivácie autorov malvéru sa líšia – často ide o **finančný zisk** (ukraťnúť peniaze alebo vydierať vás), inokedy **sabotáž** (napr. narušiť chod firmy či inštitúcie) alebo dokonca **politické dôvody** (kybernetické útoky medzi štátmi, hacktivizmus). Dôležité je vedieť, že hoci malvér spravidla nepoškodí fyzicky váš počítač (neodpáli vám procesor), **dokáže narobiť obrovské škody na dátach a súkromí** – môže vaše údaje **ukraťnúť, zašifrovať, vymazať**, alebo **odpočúvať vašu činnosť** na počítači bez vášho vedomia. Preto malvér nechceme ani náhodou.

---

# POROVNANIE BEŽNÝCH TYPOV MALVÉRU

Typ hrozby	Primárny cieľ	Ako sa šíri	Príklad
Vírus	Poškodiť súbory a šíriť sa	Pripojením k existujúcim programom a súborom	Makro vírusy v dokumentoch Office
Červ	Rýchle šírenie po sieti	Samostatne cez sieťové zraniteľnosti	Využíva chyby v operačnom systéme na prenos
Ransomvér	Vydieranie peňazí	E-mailové prílohy, škodlivé odkazy	Zašifruje súbory a žiada výkupné
Spyvér	Krádež informácií	Skrytý v legitímnom softvéri, zneužitie zraniteľností	Monitoruje stlačené klávesy a kradne heslá
Adware	Zobrazovanie reklám	Pridaný k bezplatnému softvéru	Neustále vyskakujúce okná v prehliadači

Tabuľka 1: Porovnanie bežných typov malvéru

Vidíme, že **malvér** nie je jednotná vec – má rôzne podoby a každá funguje trochu inak. **Vírus** potrebuje hostiteľa a šíri sa cez infikované súbory, **červ** sa šíri sám cez sieť. **Ransomvér** vám znepriístupní dáta a žiada výkupné, **spyvér** vás tajne sleduje a kradne informácie. Potom máme aj ďalšie typy: **trójsky kôň** (tvári sa ako užitočný program, ale obsahuje škodlivý kód), **adware** (otravný softvér s reklamami), **keyloggery** (programy odchyťávajúce stlačené klávesy) a podobne. Pre bežného používateľa nie je až také dôležité vedieť identifikovať presný typ malvéru, podstatné je **vedieť sa brániť všeobecne**: mať aktualizovaný systém, používať antivírus, neklikat' na podozrivé veci a pravidelne zálohovať dáta. Tým pokryjete väčšinu hrozieb, nech už ide o vírus či ransomvér.

---

# PRVÁ LÍNIA OBRANY

## BUDOVANIE VAŠEJ PRVEJ LÍNIE OBRANY: ZÁKLADNÉ BEZPEČNOSTNÉ POSTUPY

Tri kľúčové piliere osobnej digitálnej bezpečnosti:

1. Silné heslá a správcovia hesiel
2. Dvojfaktorová autentifikácia (2FA)
3. Pravidelné aktualizácie softvéru

---

Teraz keď poznáte základné hrozby, obráťme sa **na obranu**. Predstavte si bezpečnosť ako **cibuľu zloženú z viacerých vrstiev**. Vonkajšiu ochranu tvoria rôzne firewally či antivírusy – o tých sa bavíme neskôr – ale **úplne prvá línia obrany ste vy sami a vaše základné návyky**. V tejto časti sa zameriame na **tri kľúčové piliere osobnej digitálnej bezpečnosti: silné heslá** (a ich správa), **dvojfaktorová autentifikácia** a **pravidelné aktualizácie softvéru**. Tieto tri veci by mal praktizovať každý používateľ. Sú to **jednoduché, no mimoriadne účinné kroky**, ktoré dramaticky znižujú šancu, že sa stanete obeťou útoku. Ak ich budete dodržiavať, máte vybudovaný pevný základ bezpečnosti. Postupne si vysvetlíme prečo a ako na ne.

---

# SPRÁVCA HESIEL

## Najbezpečnejšie riešenie: Správca hesiel

- **Čo to je?** Aplikácia, ktorá funguje ako zabezpečený digitálny trezor pre všetky vaše heslá.
  - **Ako funguje?**
    - Generuje extrémne silné, náhodné heslá pre každú službu.
    - Bezpečne ich ukladá.
    - Vy si musíte pamätať iba jedno jediné, veľmi silné **hlavné heslo** (master password).
  - **Prečo ho používať?** Odstraňuje potrebu pamätať si alebo opakovane používať heslá, čím dramaticky zvyšuje vašu bezpečnosť.
- 

Napriek všetkým radám vyššie je jasné, že **pamätať si mnoho silných hesiel je pre bežného človeka prakticky nemožné**. Tu prichádza na pomoc **správca hesiel** (password manager). Toto je azda **najlepšie a najbezpečnejšie riešenie** správy hesiel dnes. **Čo je správca hesiel?** Predstavte si ho ako **zabezpečený digitálny trezor** na všetky vaše heslá. Je to aplikácia (môže byť v počítači, v mobile, alebo ako webová služba), do ktorej si uložíte všetky svoje heslá k rôznym účtom. Celý tento trezor je chránený jedným **hlavným heslom** (master password), ktoré **poznáte len vy**. Výhoda je, že **si musíte pamätať už len toto jedno jediné silné heslo** – a všetky ostatné za vás bezpečne uchová správca.

**Ako to funguje v praxi?** Keď potrebujete nové heslo, správca hesiel vám vie **vygenerovať extrémne silné, náhodné heslo** (napríklad 4Dx\$91Lt... atď.) pre daný účet. Vy si ho nemusíte pamätať ani opisovať – správca ho **zašifrovane uloží**. Keď sa chcete prihlásiť, správca hesiel sa vie integrovať s prehliadačom či telefónom, aby automaticky vyplnil príslušné heslo za vás. V praxi teda používanie správcu hesiel vyzerá tak, že si pamätáte svoje hlavné heslo do správcu (to musí byť naozaj silné a nepoužívate ho nikde inde!), a potom v každej službe použijete unikátne dlhé náhodné heslo, ktoré ani nepoznate – ale váš správca ho tam vloží, keď treba. **Prečo ho používať?** Lebo tým **odstránite potrebu pamätať si či zapisovať heslá** a hlavne **vyhnete sa pokušeniu opakovane používať jedno heslo**. Takto dramaticky zvýšite svoju bezpečnosť, lebo aj keby uniklo heslo z nejakej služby, nebude vám to vadiť – všade máte iné. Existuje mnoho správcov hesiel. Dobrá správa: **mnohé sú dostupné bezplatne** alebo už

ich možno aj používate, len o tom neviete. Napríklad **Google účet** ponúka vlastný správca hesiel (ak používate Chrome prehliadač, možno ste si všimli, že vám ponúka uloženie a generovanie hesiel). Podobne **Apple iCloud Keychain** spravuje heslá naprieč vašimi Apple zariadeniami. Okrem toho sú populárne samostatné aplikácie ako **LastPass**, **1Password**, **Bitwarden**, **KeePass** a ďalšie – niektoré zdarma, iné za malý ročný poplatok za extra funkcie. Dôležité je začať im dôverovať a používať ich. Správca hesiel **šifruje vaše heslá** tak, že ani jeho tvorcovia k nim nevidia – sú bezpečné, pokiaľ nevyzradíte svoje hlavné heslo. Samozrejme, aj tu platí opatrnosť: hlavné heslo si musíte dobre zapamätať (a nikde ho nepísať), prípadne si zapísať tzv. obnovovací kľúč na bezpečné miesto, keby ste hlavné heslo zabudli. Ale to je stále lepší prístup, než riskovať slabé či opakované heslá.

---

# DVOJFAKTOROVÁ AUTENTIFIKÁCIA (2FA)

## Implementácia dvojfaktorovej autentifikácie (2FA)

- **Čo je 2FA?** Bezpečnostný proces, ktorý na overenie identity vyžaduje dve rôzne formy potvrdenia, nielen heslo.
  - **Princíp:** Kombinácia dvoch z troch faktorov:
    1. **Niečo, čo viete:** Vaše heslo alebo PIN.
    2. **Niečo, čo máte:** Váš mobilný telefón alebo hardvérový kľúč.
    3. **Niečo, čo ste:** Odtlačok prsta alebo sken tváre.
  - **Prečo je kľúčová?** Aj keby útočník ukradol vaše heslo, bez fyzického prístupu k vášmu telefónu sa do účtu nedostane.
- 

## Dvojfaktorová autentifikácia (2FA)

Ďalší pilier je **dvojfaktorová autentifikácia**, často označovaná skratkou **2FA**. Tento pojem ste možno zachytili – po slovensky dvojfázové overenie alebo dvojstupňové overenie. **Čo to znamená?** Je to **bezpečnostný proces**, pri ktorom na prihlásenie **nestačí len heslo**, ale ešte **jeden ďalší faktor** na overenie identity. Klasicky používame kombináciu *meno + heslo*. Pri 2FA pridáte napríklad *jednorazový kód v SMS* alebo *potvrdenie v mobile*. **Princíp** vychádza z toho, že kombinujeme **dva z troch typov faktorov**:

**Niečo, čo viete** – čiže vaše heslo alebo PIN kód.

**Niečo, čo máte** – napríklad váš mobilný telefón (na ktorom vygenerujete alebo prijmete kód), alebo špeciálny **hardvérový bezpečnostný kľúč**.

**Niečo, čo ste** – tým sa myslí biometria, napríklad váš odtlačok prsta alebo **sken tváre**.

Najčastejšie sa využíva kombinácia prvých dvoch – **heslo + mobilný telefón**. Napríklad máte heslo do e-mailu, ale keď ho zadáte, služba ešte vyžiada kód, ktorý vám medzitým prišiel SMSkou alebo ktorý si vygenerujete v appke v mobile. **Prečo je 2FA také**

**dôležité?** Predstavte si, že útočník získa vaše heslo (či už ho niekde odpozoruje, ukradne z nejakej uniknutej databázy, alebo ste mu, nedajbože, naleteli na phishing). **Ak nemáte 2FA**, útočník sa vie **hneď prihlásiť** do vášho účtu – má všetko, čo potrebuje. **Ale ak máte 2FA zapnuté**, samotné heslo mu **nestačí**. Zrazu, keď skúsi login, systém pýta ešte kód z vášho telefónu – a ten, samozrejme, nemá. Čiže **aj keď heslo prezradíte**, dvojfaktor vás stále zachráni, lebo útočník by musel fyzicky získať aj váš telefón (alebo

iný druhý faktor), čo je o dosť nepravdepodobnejšie. Tým sa **bezpečnosť dramaticky zvyšuje**.

**Bežné metódy 2FA** zahŕňajú:

**SMS kód** – najrozšírenejšia forma. Po zadaní hesla vám príde SMS s jednorazovým 6-ciferným kódom, ktorý opíšete. Výhoda: funguje aj na starom telefóne bez aplikácií.

Nevýhoda: SMS môžu byť teoreticky odchytené (napr. cez tzv. *SIM-swapping* útok, keď vám útočník ukradne telefónne číslo). Stále je to však lepšie ako nič.

**Autentifikačné aplikácie** – napríklad **Google Authenticator**, **Microsoft Authenticator** alebo **Authy**. Tie generujú každých 30 sekúnd nový kód priamo vo vašom telefóne. Funguje to offline, netreba čakať na SMS. Je to považované za bezpečnejšie než SMS, lebo kód vidíte len vy v appke a nie je kam ho cestou odchytiť.

**Biometria** – niektoré služby umožňujú odtlačok prsta alebo rozpoznávanie tváre ako druhý faktor. Napríklad pri mobilnom bankovníctve zadáte PIN a potom vás aplikácia vyzve potvrdiť odtlačkom prsta.

**Hardvérové kľúče** – pre veľmi vysokú bezpečnosť existujú fyzické kľúče (napr. **YubiKey**), ktoré si pripojíte cez USB alebo Bluetooth a stlačením tlačidla overíte prihlásenie. Toto využívajú najmä firmy a ľudia, čo potrebujú špičkové zabezpečenie (novinári, správcovia, atď.), ale postupne sa to dostáva do povedomia aj bežným používateľom.

Dôležité je, že **dvojfaktor dnes ponúka väčšina veľkých služieb** – určite banky, väčšina e-mailov (Gmail, Outlook), sociálne siete (Facebook, Instagram) a podobne. Niekde je to dobrovoľné, inde povinné. **Odporúčanie znie: zapnite si 2FA všade, kde je to možné**, najmä na primárnom e-maile, cloude, sociálnych sieťach a iných dôležitých účtoch. Tá trocha nepohodlia (opísať kód z mobilu) je nič v porovnaní s ochranou, ktorú získate. Aplikácie ako Authenticator navyše vedú to overenie zjednodušiť (napr. priamo vám vyskočí v mobile výzva "Schváliť prihlásenie?" a len tapnete OK).

*(Príklad zo života: S 2FA je to ako s dvojítm zámkom. Ak aj niekto ukradne váš kľúč od brány, stále ho stopne druhý zámok na dverách. Pre útočníka často stačí, že vidí dodatočnú prekážku a vzdá to alebo si nájde ľahšiu obeť. Takže ak niečo také útočníkovi výrazne sťaží život a vám pritom nezaberie veľa času, určite to stojí za to.)*

---

# AKTUALIZÁCIE INFORMAČNÝCH SYSTÉMOV A SOFTVÉRU

- **Čo sú aktualizácie („záplaty“)?** Nové verzie softvéru, ktoré opravujú chyby a zatvárajú bezpečnostné „diery“ (zraniteľnosti).
  - **Riziko neaktualizovania:** Ak si aktualizáciu nenainštalujete, vaše zariadenie zostáva zraniteľné a stáva sa ľahkým cieľom pre útoky. Odkladanie aktualizácií vás vystavuje zbytočnému riziku.
  - **Ďalšie výhody:** Zlepšenie výkonu, nové funkcie a lepšia kompatibilita.
  - **Odporúčanie:** Vždy, keď je to možné, **zapnite automatické aktualizácie.**
- 

Treťou kľúčovou vecou v prvej línii obrany sú **aktualizácie**. Každý z nás pozná tie vyskakujúce okná: *“Je dostupná aktualizácia systému. Teraz reštartovať?”* – a my to často odkladáme s tým, že *neskôr*. Tu by som chcel zdôrazniť: **aktualizácie (tzv. záplaty)** sú mimoriadne dôležité pre bezpečnosť. Spomínali sme, že útočníci zneužívajú známe chyby. Aktualizácia je **oprava chyby**, ktorú vydá výrobca, keď sa o nej dozvie. Čiže keď vidíte, že váš telefón alebo počítač má k dispozícii aktualizáciu, znamená to, že **vývojári opravili nejaké zraniteľnosti alebo chyby** a vy si tú opravu musíte “nalepiť” na systém, aby ste neboli zraniteľní. **Riziko neaktualizovania** je jasné: vaše zariadenie zostáva deravé a **stáva sa ľahkým cieľom**. Útoky cez staré chyby môžu viesť ku krádeži dát, zavíreniu počítača a podobne. Keď odkladáte aktualizácie, **zbytočne riskujete**.

**Ako na to v praxi?** Ideálne je **zapnúť si automatické aktualizácie** všade, kde sa dá. Moderné operačné systémy (Windows, macOS, iOS, Android) to umožňujú – zariadenie si samo stiahne a nainštaluje záplaty (často v noci alebo keď ho nepoužívate). Skontrolujte si v nastaveniach, či to máte povolené. Ak si nie ste istí:  
Vo Windows choďte do *Nastavenia > Windows Update* a nastavte automatické sťahovanie a inštaláciu.  
V Androide zväčša *Nastavenia > Aktualizácia softvéru* (alebo *Systém > Rozšírené > Aktualizácie podľa výrobcu*).  
Na iPhone/iPad *Nastavenia > Všeobecné > Aktualizácia softvéru* a zapnúť automatické aktualizácie.

Taktiež nezabúdajte na aktualizácie aplikácií – majte **Google Play** a **App Store** nastavené na auto-update, a na počítači napríklad prehliadač Chrome sa už aktualizuje sám. Ak nejaký program hlási novú verziu, neváhajte ju nainštalovať.

Ešte pripomeniem to, čo zaznelo už skôr: Útočníci **aktívne skenujú internet** a hľadajú systémy so známymi chybami. Keď nájdu neaktualizovaný server či počítač, vedia doň automaticky preniknúť, ak poznajú zraniteľnosť. Presne tak sa šíril známy červ **WannaCry** v roku 2017 – využil diery vo Windows, na ktorú už síce existovala záplata, ale tisíce počítačov neboli aktualizované. Výsledok: masívna epidémia ransomvéru po celom svete. Poučenie? **Aktualizácia mohla zabrániť obrovským škodám**. Takže prosím, nenechajte svoje zariadenia zbytočne zastarané. Väčšina updatov prebehne rýchlo na pozadí.

*(Tip: Ak máte obavu, že aktualizácia rozbije kompatibilitu s nejakým starým programom, urobte si pred ňou pre istotu **zálohu** – ale tak či onak by ste mali zálohovať pravidelne, o tom hneď budeme hovoriť. Tým pádom ak by aj update spôsobil problém, viete sa vrátiť k starému stavu. Ale opakujem, prípady problematických updatov sú zriedkavé oproti riziku nechráneného systému.)*

---

# MODERNÝ PRÍSTUP K BEZPEČNOSTI

## Posun v myslení kybernetickej bezpečnosti

- **Starý prístup:** Vyžadoval od používateľa zapamätanie desiatok zložitých hesiel, čo viedlo k nebezpečnému správaniu (opätovné používanie hesiel).
  - **Moderný prístup:** Uvedomuje si, že používateľ je najslabší článok a potrebuje technologické pomôcky.
    - **Správcovia hesiel** odbremeňujú pamäť.
    - **Dvojfaktorová autentifikácia** poskytuje záchrannú sieť.
    - **Automatické aktualizácie** odstraňujú potrebu neustálej ostražitosťi.
  - Tento prístup zohľadňuje **ľudský faktor** a robí bezpečnosť dostupnejšou.
- 

Na záver prvej časti sa ešte zamyslime nad tým, **ako sa mení prístup k bezpečnosti** v posledných rokoch z pohľadu používateľa. Kedysi sa kládol dôraz na to, že *“používateľ nesmie robiť chyby”*. Od ľudí sa očakávalo, že si zapamätajú desiatky komplexných hesiel, budú stále v strehu pred každým e-mailom a budú odborníci na počítače. To bolo samozrejme **nereálne a neudržateľné**. Výsledkom týchto prehnaných očakávaní bolo predvídateľné správanie: ľudia si začali tie komplikované heslá recyklovať alebo písať na papieriky, prehliadali aktualizácie, lebo ich to otravovalo, a podobne. **Odborná komunita** si dnes uvedomuje, že **používateľ nie je najslabší článok preto, že by bol hlúpy alebo lenivý, ale preto, že od neho IT priemysel chcel nemožné. Moderný prístup** k kybernetickej bezpečnosti preto kladie dôraz na **pomôcky a technológie, ktoré urobia bezpečnú cestu tou najjednoduchšou**. Ide o to, aby **system pomáhal používateľovi**, nie aby všetka záťaž bola na ňom.

Konkrétne sa presadzuje presne to, čo sme si povedali:

**Správcovia hesiel** odbremeňujú našu pamäť tým, že si nemusíme pamätať 100 hesiel.

**Dvojfaktorová autentifikácia** poskytuje **záchrannú sieť**, keď prvá vrstva (heslo) zlyhá – teda aj keď urobíme chybu a prezradíme heslo, 2FA nás podrží.

**Automatické aktualizácie** odstraňujú potrebu, aby používateľ stále myslel na záplaty – systém sa aktualizuje sám na pozadí.

Tento nový prístup viac **zohľadňuje ľudský faktor** – chápe, že človek je omylný a nechce tráviť hodiny študovaním IT bezpečnosti, tak mu dáme nástroje, ktoré ho **chránia pred vlastnými chybami**. Pre bežného používateľa je tak **oveľa jednoduchšie**

**dosiahnuť vysokú úroveň bezpečnosti**, ak si osvojí týchto pár kľúčových nástrojov a zásad. Takže ak si z prvej časti odnesiete aspoň toto: *používajte správcu hesiel, zapnite si 2FA, nechajte si aktualizovať zariadenia a robte zálohy*, budete na tom **lepšie než 90 % populácie** z hľadiska bezpečnosti. A pritom nemusíte poznať detaily fungovania šifrier alebo siete – stačí dodržiavať tieto osvedčené postupy.







---

## **ČASŤ 2: PRE SPRÁVCOV SYSTÉMOV ZÁKLADY SPRÁVY BEZPEČNOSTI SYSTÉMOV**

---

(V druhej časti sa budeme venovať poslucháčom, ktorí sú skôr technicky zameraní – správcami sietí, systémovým administrátorom alebo jednoducho záujemcom o hlbšie know-how. Prejdeme si kľúčové koncepty a metódy, ktoré používajú profesionáli na udržanie bezpečnosti systémov.)

---

## Zraniteľnosť vs CVE

- **CVE (Common Vulnerabilities and Exposures)** je identifikátor zraniteľnosti, nie samotná zraniteľnosť. Slúži ako jednotné označenie, aby sa o konkrétnej chybe mohlo hovoriť jednotným jazykom.
- CVE záznam obsahuje **stručný popis**, **ID** (napr. CVE-2025-12345) a **odkazy** na podrobnosti či záplaty. Nie je to opravný kód ani úplný popis chyby.
- **Nie každá zraniteľnosť má CVE:** Interné zraniteľnosti (napr. v našom vlastnom kóde alebo konfigurácii) nemusia byť v žiadnej verejnej databáze.

- 
- Príklady: buffer overflow v aplikácii, SQL injection na webe, zraniteľnosť procesora (Meltdown/Spectre).
  - Príklady: ponechané predvolené heslá, otvorené porty/firewall nastavený „allow all“, vypnuté bezpečnostné funkcie.
  - Príklady: neexistuje proces na odoberanie prístupov po odchode zamestnanca, neformálne nasadzovanie zmien bez testovania, chýbajúce školenia o bezpečnosti.
  - napr. phishing – aby obišli technické zabezpečenia. (Tieto neزالátate patchom, vyžadujú tréning a povedomie.)

---

## CVSS a prečo nestačí

- **CVSS (Common Vulnerability Scoring System)** dáva zraniteľnostiam skóre 0–10 podľa technickej závažnosti, ale nehovorí nič o pravdepodobnosti zneužitia v praxi.
  - **Chýba kontext:** CVSS neberie do úvahy konkrétne podmienky – či je systém vystavený na Internet, či už existuje exploit, aká je hodnota aktíva, atď.
  - **Dôsledky:** Môžeme premrhať zdroje na záplaty „teoreticky kritických“ chýb, ktoré však útočníci reálne nevyužijú, zatiaľ čo prehliadneme stredne závažnú zraniteľnosť, na ktorú už existuje exploit a aktívne sa zneužíva.
  - **Príklad:** CVE s CVSS 9.0 mala <1% pravdepodobnosť zneužitia, iná s CVSS 5.9 mala ~80% pravdepodobnosť a patrila medzi najčastejšie zneužívané. Ak by sme išli iba podľa skóre, opravili by sme nesprávnu prvú a druhú (nebezpečnejšiu) zanedbali.
- 
- Príklady: buffer overflow v aplikácii, SQL injection na webe, zraniteľnosť procesora (Meltdown/Spectre).
  - Príklady: ponechané predvolené heslá, otvorené porty/firewall nastavený „allow all“, vypnuté bezpečnostné funkcie.
  - Príklady: neexistuje proces na odoberanie prístupov po odchode zamestnanca, neformálne nasadzovanie zmien bez testovania, chýbajúce školenia o bezpečnosti.
  - napr. phishing – aby obišli technické zabezpečenia. (Tieto nezalátate patchom, vyžadujú tréning a povedomie.)

---

# Konfiguračné zraniteľnosti

- **Vznikajú z nesprávneho nastavenia:** nejde o chybu softvéru, ale o chybu v jeho nasadení/konfigurácii administrátorom.
  - Server ponechaný s **defaultnými heslami** alebo **defaultným účtom admin/admin** (útočníci to skúsia ako prvé).
  - **Nesprávne prístupové práva:** napr. všetci používatelia vidia zdieľaný disk so citlivými súbormi; verejný cloud storage bez obmedzení prístupu.
  - **Vypnuté bezpečnostné funkcie:** napr. administrátor kvôli pohodliu vypne UAC alebo firewall na staniciach, používa protokol FTP namiesto SFTP, nezapne dvojfaktorovú autentifikáciu.
  - **Iné misconfigurácie:** Otvorený MongoDB/Elasticsearch bez hesla, služby bežiace s prístupmi SYSTEM/root aj keď netreba, zle nastavené TLS (slabé šifry).
  - **Dopad:** Konfiguračné chyby sú veľmi časté a útočníci ich aktívne vyhľadávajú. Takmer všetky zlyhania bezpečnosti v cloude sú spôsobené chybou zákazníka – najmä misconfiguráciou
- 

Príklad zo života: Po odchode administrátora z firmy nik nezrušil jeho VPN prístup a účty. Toto nie je „bug“ v IT systéme, ale vážna procesná chyba. O pol roka neskôr ten človek (alebo niekto, kto získal jeho staré poverenia) mohol stále prísť do siete – to je zraniteľnosť! A stala sa kvôli chýbajúcemu procesu na odobratie prístupov. Podobne často vidíme, že firmy nemajú proces na testovanie záloh – roky sa nerobia obnovy nanečisto. Keď potom príde incident (napr. ransomware), zistia, že zálohy sú neúplné alebo nefunkčné – to bola latentná zraniteľnosť procesu zálohovania.

- Ďalší príklad: Chýba politika update managementu – každý admin si záplatuje servery po svojom alebo vôbec. Výsledkom je nejednotný stav, niektoré servery sú roky bez patchov. To je procesné zlyhanie (chýba riadenie). Technicky je možno každý server v poriadku, ale proces „udržiavať všetko aktuálne“ neexistuje alebo zlyháva.
- Procesné zraniteľnosti sú ľahko prehliadnuteľné, lebo neblíkajú ako kritické CVE v reporte. Vyžadujú analýzu pracovných postupov a interných pravidiel. Bezpečnostné audity a certifikácie (napr. ISO 27001) sa práve zameriavajú aj na tieto organizačné aspekty – pýtajú sa, či máte proces riadenia zraniteľností, proces zálohovania, reakcie na incidenty atď. Ak nie, auditor vytkne medzeru v procese, lebo to je rovnako dôležité ako technické opatrenia.
- Ako tieto zraniteľnosti riešiť? Podobne ako softvérové – najprv ich musíme identifikovať (napr. formou auditov, kontrolou súladu s normami), potom vyhodnotiť riziko (čo by sa stalo, ak proces zlyhá) a prijať opatrenia. Niekedy stačí zaviesť jednoduchú kontrolu (napr. štvrťročne prejsť zoznam účtov a zrušiť nepotrebné), inokedy väčšiu vec (napísať a zaviesť novú smernicu).

- Z praxe: Medzi najčastejšie prehliadané procesné slabiny patrí neexistujúci pravidelný audit prístupov, absencia bezpečnostných školení pre zamestnancov, chýbajúci plán obnovy po incidente, obchádzanie formálneho procesu zmien (admini niečo menia bez posúdenia dopadu) a podobne. Odstránenie týchto slabín často nevyžaduje drahé technológie, ale manažérsky dôraz a disciplínu. Preto je dôležité komunikovať vedeniu, že investície do procesov (čas, školenia, kontroly) sú rovnako potrebné ako investície do firewallov a antivírusov.

---

# Procesné zraniteľnosti

- **Čo to je:** Zraniteľnosti vznikajúce z nedostatkov v procesoch a organizačných postupoch, nie z technických chýb.
  - **Neaktuálne alebo chýbajúce interné smernice a politiky** (napr. neexistuje politika patchovania alebo riadenia zmien).
  - **Slabé procedúry:** Napr. nevynucuje sa pravidelná zmena hesiel, neodoberajú sa prístupy po odchode zamestnancov, chyba kontrola štyroch očí pri citlivých operáciách.
  - **Nedostatok tréningu:** Zamestnanci nevedia rozpoznať phishing, IT tím nepozná nové hrozby a ľudský faktor potom zlyhá.
  - **Náprava:** Audit procesov a ich vylepšovanie je súčasťou bezpečnosti. Nestačí len záplaty na softvér ale musíme „zaplátať“ aj firemné procesy (dokumentáciou, školením, kontrolami).
- 

Príklad zo života: Po odchode administrátora z firmy nik nezrušil jeho VPN prístup a účty. Toto nie je „bug“ v IT systéme, ale vážna procesná chyba. O pol roka neskôr ten človek (alebo niekto, kto získal jeho staré poverenia) mohol stále prísť do siete – to je zraniteľnosť! A stala sa kvôli chýbajúcemu procesu na odobratie prístupov. Podobne často vidíme, že firmy nemajú proces na testovanie záloh – roky sa nerobia obnovy nanečisto. Keď potom príde incident (napr. ransomware), zistia, že zálohy sú neúplné alebo nefunkčné – to bola latentná zraniteľnosť procesu zálohovania.

- **Ďalší príklad:** Chýba politika update managementu – každý admin si záplatuje servery po svojom alebo vôbec. Výsledkom je nejednotný stav, niektoré servery sú roky bez patchov. To je procesné zlyhanie (chyba riadenie). Technicky je možno každý server v poriadku, ale proces „udržiavať všetko aktuálne“ neexistuje alebo zlyháva.
- Procesné zraniteľnosti sú ľahko prehliadnuteľné, lebo neblíkajú ako kritické CVE v reporte. Vyžadujú analýzu pracovných postupov a interných pravidiel. Bezpečnostné audity a certifikácie (napr. ISO 27001) sa práve zameriavajú aj na tieto organizačné aspekty – pýtajú sa, či máte proces riadenia zraniteľností, proces zálohovania, reakcie na incidenty atď. Ak nie, auditor vytkne medzeru v procese, lebo to je rovnako dôležité ako technické opatrenia.
- Ako tieto zraniteľnosti riešiť? Podobne ako softvérové – najprv ich musíme identifikovať (napr. formou auditov, kontrolou súladu s normami), potom vyhodnotiť riziko (čo by sa stalo, ak proces zlyhá) a prijať opatrenia. Niekedy stačí zaviesť jednoduchú kontrolu (napr. štvrťročne prejsť zoznam účtov a zrušiť nepotrebné), inokedy väčšiu vec (napísať a zaviesť novú smernicu).

- Z praxe: Medzi najčastejšie prehliadané procesné slabiny patrí neexistujúci pravidelný audit prístupov, absencia bezpečnostných školení pre zamestnancov, chýbajúci plán obnovy po incidente, obchádzanie formálneho procesu zmien (admini niečo menia bez posúdenia dopadu) a podobne. Odstránenie týchto slabín často nevyžaduje drahé technológie, ale manažérsky dôraz a disciplínu. Preto je dôležité komunikovať vedeniu, že investície do procesov (čas, školenia, kontroly) sú rovnako potrebné ako investície do firewallov a antivírusov.

---

# Kompenzačné opatrenia

- **Definícia:** Kompenzačné (náhradné) opatrenia sú dočasné alebo dodatočné bezpečnostné kontroly zavedené na zníženie rizika, keď primárne riešenie (patch) nie je hneď dostupné či aplikovateľné.
- **Účel:** Nekryjú zraniteľnosť priamo, ale zmierňujú šancu zneužitia alebo dopady – poskytujú nám “čas navyše” do finálnej opravy.

## Príklady:

- **Obmedzenie prístupu:** Segmentácia siete, dočasné vypnutie alebo izolácia zraniteľného systému, nastavenie firewall pravidiel zakazujúcich využiť danú chybu (napr. blokovať špecifické porty/protokoly).
  - **Dodatočná autentifikácia alebo šifrovanie:** Zavedenie 2FA a VPN. Šifrovať komunikáciu, aby prípadný útok nemohol odchytiť citlivé dáta.
  - **Monitoring a detekcia:** Nasadenie IDS/IPS signatúr na známu zraniteľnosť, zvýšený logging a alerty na podozrivé aktivity (aby sme včas odhalili pokus o zneužitie).
  - **„Virtuálne“ patchovanie:** V prípade aplikačných zraniteľností nasadiť WAF (Web Application Firewall) pravidlá, ktoré filtrujú známe útokové vstupy využívajúce tú chybu. Alebo skript na strane servera, ktorý validuje vstupy a znemožní exploit.
  - **Operačné obmedzenia:** Zníženie oprávnení služby, zvýšenie frekvencie zálohovania pre prípad incidentu, edukácia užívateľov.
- 

Príklad zo života: Po odchode administrátora z firmy nik nezrušil jeho VPN prístup a účty. Toto nie je „bug“ v IT systéme, ale vážna procesná chyba. O pol roka neskôr ten človek (alebo niekto, kto získal jeho staré poverenia) mohol stále prísť do siete – to je zraniteľnosť! A stala sa kvôli chýbajúcemu procesu na odobratie prístupov. Podobne často vidíme, že firmy nemajú proces na testovanie záloh – roky sa nerobia obnovy nanečisto. Keď potom príde incident (napr. ransomware), zistia, že zálohy sú neúplné alebo nefunkčné – to bola latentná zraniteľnosť procesu zálohovania.

- **Ďalší príklad:** Chýba politika update managementu – každý admin si záplatuje servery po svojom alebo vôbec. Výsledkom je nejednotný stav, niektoré servery sú roky bez patchov. To je procesné zlyhanie (chýba riadenie). Technicky je možno každý server v poriadku, ale proces “udržiavať všetko aktuálne” neexistuje alebo zlyháva.
- Procesné zraniteľnosti sú ľahko prehliadnuteľné, lebo neblíkajú ako kritické CVE v reporte. Vyžadujú analýzu pracovných postupov a interných pravidiel. Bezpečnostné audity a certifikácie (napr. ISO 27001) sa práve zameriavajú aj na tieto organizačné aspekty – pýtajú sa, či máte proces riadenia zraniteľností, proces zálohovania, reakcie na incidenty atď. Ak nie, auditor vytkne medzeru v procese, lebo to je rovnako dôležité ako technické opatrenia.
- Ako tieto zraniteľnosti riešiť? Podobne ako softvérové – najprv ich musíme identifikovať (napr. formou auditov, kontrolou súladu s normami), potom vyhodnotiť riziko (čo by sa stalo, ak proces zlyhá) a prijať opatrenia. Niekedy stačí zaviesť jednoduchú kontrolu (napr. štvrťročne prejsť zoznam účtov a zrušiť nepotrebné), inokedy väčšiu vec (napísať a zaviesť novú smernicu).

- Z praxe: Medzi najčastejšie prehliadané procesné slabiny patrí neexistujúci pravidelný audit prístupov, absencia bezpečnostných školení pre zamestnancov, chýbajúci plán obnovy po incidente, obchádzanie formálneho procesu zmien (admini niečo menia bez posúdenia dopadu) a podobne. Odstránenie týchto slabín často nevyžaduje drahé technológie, ale manažérsky dôraz a disciplínu. Preto je dôležité komunikovať vedeniu, že investície do procesov (čas, školenia, kontroly) sú rovnako potrebné ako investície do firewallov a antivírusov.

---

# Kedy NEpatchovať hneď

- **Nestabilná záplata:** Ak je patch novo vydaný a objavia sa správy, že spôsobuje pád systému či inú chybu, je rozumné počkať s jeho nasadením (aspoň kým sa otestuje alebo vydá opravená verzia).
  - **Kritické okno prevádzky:** Keď systém zabezpečuje kritickú službu (napr. nemocničný systém, výrobná linka 24/7), hneď patchovať môže spôsobiť výpadok. Tam plánujeme patch v údržbovom okne (radšej krátke odloženie ako neplánovaný pád systému).
  - **Nízke riziko v kontexte:** Ak zraniteľnosť neohrozuje náš systém (napr. chyba v module, ktorý nepoužívame, alebo služba nejde zvonka), nemusíme panikáriť. Patch nasadíme, ale nemusí to byť hneď.
  - **Kompenzačné opatrenia už nasadené:** Ak sme inými kontrolami pokryli riziko (napr. firewall blokuje vektory útoku, máme segmentáciu), vieme krátkodobo odložiť patch a spoliehať sa na tieto zábrany. (Stále platí, že patchnúť treba, len nie okamžite).
  - **Neprimeraná námaha/riziko:** Pri legacy systémoch môže patchovanie znamenať veľké riziko odstavky alebo nekompatibility.
- 

Príklad zo života: Po odchode administrátora z firmy nik nezrušil jeho VPN prístup a účty. Toto nie je „bug“ v IT systéme, ale vážna procesná chyba. O pol roka neskôr ten človek (alebo niekto, kto získal jeho staré poverenia) mohol stále prísť do siete – to je zraniteľnosť! A stala sa kvôli chýbajúcemu procesu na odobratie prístupov. Podobne často vidíme, že firmy nemajú proces na testovanie záloh – roky sa nerobia obnovy nanečisto. Keď potom príde incident (napr. ransomware), zistia, že zálohy sú neúplné alebo nefunkčné – to bola latentná zraniteľnosť procesu zálohovania.

- **Ďalší príklad:** Chýba politika update managementu – každý admin si záplatuje servery po svojom alebo vôbec. Výsledkom je nejednotný stav, niektoré servery sú roky bez patchov. To je procesné zlyhanie (chýba riadenie). Technicky je možno každý server v poriadku, ale proces „udržiavať všetko aktuálne“ neexistuje alebo zlyháva.
- **Procesné zraniteľnosti** sú ľahko prehliadnuteľné, lebo neblíkajú ako kritické CVE v reporte. Vyžadujú analýzu pracovných postupov a interných pravidiel. Bezpečnostné audity a certifikácie (napr. ISO 27001) sa práve zameriavajú aj na tieto organizačné aspekty – pýtajú sa, či máte proces riadenia zraniteľností, proces zálohovania, reakcie na incidenty atď. Ak nie, auditor vytkne medzeru v procese, lebo to je rovnako dôležité ako technické opatrenia.
- **Ako tieto zraniteľnosti riešiť?** Podobne ako softvérové – najprv ich musíme identifikovať (napr. formou auditov, kontrolou súladu s normami), potom vyhodnotiť riziko (čo by sa stalo, ak proces zlyhá) a prijať opatrenia. Niekedy stačí zaviesť jednoduchú kontrolu (napr. štvrťročne prejsť zoznam účtov a zrušiť nepotrebné), inokedy väčšiu vec (napísať a zaviesť novú smernicu).

- Z praxe: Medzi najčastejšie prehliadané procesné slabiny patrí neexistujúci pravidelný audit prístupov, absencia bezpečnostných školení pre zamestnancov, chýbajúci plán obnovy po incidente, obchádzanie formálneho procesu zmien (admini niečo menia bez posúdenia dopadu) a podobne. Odstránenie týchto slabín často nevyžaduje drahé technológie, ale manažérsky dôraz a disciplínu. Preto je dôležité komunikovať vedeniu, že investície do procesov (čas, školenia, kontroly) sú rovnako potrebné ako investície do firewallov a antivírusov.

---

# Životný cyklus zraniteľnosti

- **Vznik chyby:** Zraniteľnosť vznikne ako vedľajší produkt vývoja alebo konfigurácie – napr. programátorská chyba, ktorú si nik nevšimol, alebo zlé nastavenie systému.
  - **Objavenie:** Slabina je objavená buď bezpečnostným výskumníkom (eticky – oznámi ju) alebo útočníkom (zneužije ju potajme).
  - **Oznámenie (Disclosure):** Ak ju nájde výskumník, oznámi výrobcovi a po čase dôjde k verejnému zverejneniu detailov. Ak ju však prvý odhalí útočník, môže zostať utajená (zero-day zraniteľnosť).
  - **Záplata a publikácia:** Výrobca vyvinie opravu (patch) a vydá aktualizáciu; priradí sa CVE a zraniteľnosť sa popíše verejne. Od tohto momentu je známa ako N-day zraniteľnosť, teda existuje dostupná záplata, ale aj exploit k nej môže rýchlo vzniknúť.
  - **(Exploatácia):** Útočníci vyvíjajú exploit (skript alebo kód) pre zverejnenú chybu a snažia sa ju zneužiť skôr, než admini záplatu aplikujú. Často ide o preteky „patch vs. exploit“.
  - **Nasadenie záplaty:** Správcovia aplikujú aktualizácie na zraniteľné systémy, čím zraniteľnosť odstraňujú.
- 

Keď sme spomenuli tie najpokročilejšie útoky, obráťme list k tým **najbežnejším**. Väčšina útokov, s ktorými sa bežný používateľ stretne, je založená na takzvanom **sociálnom inžinierstve** – teda oklamaní človeka. A kráľom medzi nimi je **phishing**. Phishing je jednoducho povedané podvodná komunikácia (e-mail, SMS, chat), ktorá sa tvári napríklad ako správa z banky alebo od kuriéra, aby od vás **vylákala citlivé údaje** (heslá, čísla kariet a podobne). Phishingové správy často vyzerajú veľmi dôveryhodne – napríklad e-mail má logo vašej banky a vyzýva vás kliknúť na odkaz a prihlásiť sa, lebo *“treba potvrdiť platbu”*. **Ten odkaz vedie na podvrhnutú stránku**, ktorá vyzerá ako internetbanking, no v skutočnosti ak tam zadáte svoje meno a heslo, pošlete ich útočníkom. **Najčastejšie typy phishingu** sa vydávajú za **banku**, kuriérsku spoločnosť (napr. *“nezaplatené clo, kliknite sem”*), alebo za podporu k Apple/Google účtu. Tiež sú bežné falošné súťaže (*“vyhrali ste nový telefón”*) či varovania typu *“váš účet bude zablokovaný”*. Ako sa brániť? **Zlaté pravidlo: Nikdy nezadávejte heslo cez odkaz z e-mailu alebo SMS**. Ak vám príde správa z banky, radšej **ručne otvorte oficiálnu stránku banky** alebo im zavolajte na infolinku. Ďalej, **neotvárajte prílohy** ako ZIP, HTML či PDF, pokiaľ si nie ste 100 % istí ich pôvodom. Firmy vám bežne neposielajú .zip prílohu len tak – ak dostanete napríklad *“faktúru”* v zip súbore od neznámeho dodávateľa, je to veľmi podozrivé. **Neodpovedajte na podozrivé správy** a nič v nich neklikajte. Ak vám píše *“vnuk z Nigérie”*, že potrebuje peniaze, radšej to ignorujte. Phishing má aj sofistikovanejšiu verziu zvanú **spear phishing** – vtedy je útok **cielený priamo na vás alebo vašu firmu**. Útočník si o vás niečo zistí a e-mail môže obsahovať napríklad vaše

celé meno či informáciu, ktorá pôsobí dôveryhodne, aby ste sa chytili na udicu. Preto buďte vždy obozretní, keď od vás niekto online pýta heslo, peniaze alebo údaje – radšej dvakrát overte, kým raz kliknete.

---

## Risk based vulnerability management

- **RBVM** je riadenie zraniteľností na základe rizika, nie len na základe číselného skóre. Odlišuje sa od tradičného prístupu, ktorý často mechanicky riešil všetky „kritické“ podľa CVSS.
  - **Focus na to, čo hrozí najviac:** RBVM prioritizuje zraniteľnosti podľa reálneho rizika pre firmu – kombinuje údaje o aktuálnych hrozbách, kontexte aktíva a dopade na biznis.
  - **Kľúčové faktory:** Pri hodnotení sa zohľadňuje napr. aktívne zneužívanie (threat intel: či útoky prebiehajú), kritickosť systému (asset value, čo na ňom beží a či je vystavený), obtiažnosť exploitácie v našom prostredí a potenciálny dopad na dostupnosť, dáta, reputáciu.
  - Cieľom je opraviť najprv to, čo predstavuje najväčšie riziko, nie iba technicky najzávažnejšie chyby, ale tie, ktoré by útočníci najskôr mohli a chceli zneužiť s najhoršími následkami
- 
- **RBVM v praxi:** Zaviesť risk-based prístup znamená spojiť tím správy zraniteľností s tímom pre riadenie rizík a hrozieb. Vyžaduje to dáta – o aktívach (CMDB), o hrozbách (threat intel feedy, napr. aj správy od CERT, vlastné logy útokov), o zneužívaných zraniteľnostiach (CVE trending). Moderné nástroje, napr. platformy pre RBVM, vedia využívať aj strojové učenie na priradenie skóringov, ktoré uprednostnia napr. zraniteľnosti, u ktorých sa očakáva útok v blízkej dobe.

- Prechod na RBVM pomáha organizáciám byť o krok vpred pred útočníkmi a lepšie využívať zdroje. Namiesto snažiť sa utesniť každú diery (čo je nereálne), sústredíme sa na tie, cez ktoré by naozaj mohlo pretiecť najviac škody. Samozrejme, nezanedbávame ostatné – ale tie buď priebežne riešime neskôr, alebo ak riziko je minimálne, vedome ho na istý čas akceptujeme. RBVM je teda o efektívite cez chytrú prioritu. Firmy, ktoré ho aplikujú, často zistia, že z ~1000 nájdených zraniteľností reálne stačí urgentne riešiť povedzme 5–10%, ktoré predstavujú 95% rizika.

---

## Asset-based pohľad na zraniteľnosti

- **Inventár aktív je základ:** Musíme vedieť čo všetko máme, teda zariadenia, servery, aplikácie a akú majú hodnotu. Zraniteľnosť na neznámom aktíve sa totiž určite prehliadne.
- **Kritickosť aktíva:** Rovnaká zraniteľnosť má iný dopad na rôznych systémoch.
- **Prioritizácia podľa aktív:** Opravy riadime aj podľa dôležitosti systému.
- **Kontext pre riziko:** Pri vyhodnocovaní rizika zraniteľnosti berieme do úvahy, kde sa nachádza.

- 
- (Príklad: kritická chyba na verejnom serveri s klientskými dátami vs. tá istá chyba na izolovanom testovacom servery.)
  - (napr. infraštruktúra, databázy osobných údajov) opravujeme prednostne, menej dôležité alebo izolované systémy môžu krátko počkať.
  - Otvorený port je väčší problém na serveri v DMZ (prístupný z internetu) než na internom PC za firewallom.

---

# HROZBA vs. ZRANITEĽNOSŤ vs. RIZIKO

- **Zraniteľnosť (Vulnerability):**
    - Slabina, chyba alebo medzera v systéme, ktorá môže byť zneužitá. Je to pasívna „bezpečnostná diera“.
    - *Príklad:* Neaktualizovaný softvér, slabé heslo.
  - **Hrozba (Threat):**
    - Potenciálny zdroj nebezpečenstva alebo aktér, ktorý môže zneužiť zraniteľnosť. Je to aktívny prvok.
    - *Príklad:* Kyberzločinec, malvér, prírodná katastrofa.
  - **Riziko (Risk):**
    - Potenciálna škoda alebo strata, ktorá nastane, keď hrozba zneužije zraniteľnosť.
    - Hodnotí sa na základe **pravdepodobnosti** a **dopadu**.
- 

Na úvod tejto pokročilejšej časti si musíme **uvojasniť terminológiu**. Tri pojmy, ktoré často počúvame – **hrozba, zraniteľnosť a riziko** – bývajú niekedy laicky zamieňané. Pre správnu bezpečnostnú správu je však kľúčové presne chápať, čo znamenajú a ako spolu súvisia.

**Zraniteľnosť (Vulnerability)** je v podstate **slabina alebo chyba v systéme**, ktorá môže byť zneužitá na kompromitáciu bezpečnosti. Je to **pasívna “diera”** – sama o sebe ešte nespôsobila škodu, ale poskytuje priestor pre hrozbu. Môže to byť technická chyba (napr. neaktualizovaný softvér so známou bezpečnostnou chybou, zle nakonfigurovaný server, slabé heslo) alebo procesná chyba (napr. zamestnanec, ktorý nemá školenie a ľahko naletí phishingu). Podstatné: ak existuje zraniteľnosť, znamená to “máme problém, ktorý **môže byť využitý**”.

**Hrozba (Threat)** je **akýkoľvek potenciálny zdroj útoku alebo nebezpečná udalosť**, ktorá by mohla zneužiť zraniteľnosť. Hrozba môže byť **aktér** (konkrétny hacker, malvér, interný zamestnanec, ale aj prírodný živý) alebo **udalosť** (napr. požiar v dátovom centre, výpadok prúdu, kybernetický útok). Hrozba je teda niečo **aktívne**, čo číha a čaká na príležitosť udrieť. Príklady: kyberzločinec, ktorý skenuje internet a hľadá zraniteľné servery; ransomvérový útok šíriaci sa e-mailami; povodeň, ktorá môže vytopiť serverovňu.

**Riziko (Risk)** je **potenciálna škoda alebo strata**, ktorá nastane, keď sa **hrozba zneužije zraniteľnosť**. Riziko je teda **priesečník zraniteľnosti a hrozby** – kde sa tieto dva stretnú, tam vzniká riziko dopadu. Riziko sa hodnotí podľa **pravdepodobnosti**, že k

tomu dôjde, a **dopadu**, aký by to malo. Napríklad: zraniteľnosť = otvorený port so slabým heslom na serveri, hrozba = hacker to objaví a nabúra sa, riziko = odcudzenie zákazníckych dát a finančná strata + pokuty.

Čiže aby sme to zhrnuli: **Zraniteľnosť je príčina (slabé miesto), hrozba je spúšťač (útočník alebo udalosť), a riziko je následok (možná škoda).**

---

# KAUZÁLNY VZŤAH

## Ako sú tieto pojmy prepojené?

Tieto tri pojmy sú prepojené v jasnom kauzálnom reťazci:

**Zraniteľnosť** (príčina) → umožňuje, aby sa **Hrozba** prejavila → čo vytvára **Riziko** (následok).

### Príklad:

1. **Zraniteľnosť**: Neaktualizovaný webový server.
2. **Hrozba**: Hacker.
3. **Riziko**: Hacker nainštaluje malvér a ukradne dáta, čo predstavuje vysoké finančné a reputačné riziko.

Úlohou správcu je identifikovať a odstraňovať zraniteľnosti, čím priamo znižuje riziko.

---

Tieto tri pojmy sú prepojené v **kauzálnom reťazci**: Zraniteľnosť umožní hrozbe realizovať sa, čo vedie k riziku. Ak by sme to dali do vety: *“Zraniteľnosť X môže umožniť hrozbe Y spôsobiť riziko Z.”* **Príklad**: Máme **zraniteľnosť** – napríklad **neaktualizovaný webový server** s bezpečnostnou dierou. Existuje **hrozba** – **hacker**, ktorý aktívne hľadá takéto servery a vie tú chybu využiť. Keď sa tieto stretnú (hacker nájde ten server a spustí exploit), dôjde k napadnutiu – hacker napríklad **nainštaluje malvér a ukradne dáta** z toho servera. Výsledné **riziko** je **vysoká finančná a reputačná škoda pre organizáciu** – únik dát, pokuty, strata dôvery zákazníkov. Tu presne vidno ten trojuholník: ak by server nemal zraniteľnosť, hacker by nemal ako preniknúť a riziko (škoda) by nevzniklo. Naopak, ak by nebolo hackera (hrozby), tak aj keď server nebol aktualizovaný, nič sa nestane – bez aktéra, ktorý by dieru zneužil, je riziko minimálne. **Riziko vždy potrebuje oboje: slabinu aj používateľa slabiny.**

Preto úlohou bezpečnostného správcu je **manažovať riziko** tým, že **odstraňuje zraniteľnosti** alebo **zmiernuje hrozby**. V praxi je efektívnejšie odstraňovať zraniteľnosti, lebo hrozby (útočníkov alebo prírodu) nevieme vždy kontrolovať. Ak **neexistuje zraniteľnosť**, hrozba jednoducho **nemá čo zneužiť** a riziko nevznikne. Práca admina je teda často o tom **hľadať a lepiť diery skôr, než ich nájde útočník**. To je presne náplň procesov, o ktorých budeme hovoriť – **skenovanie zraniteľností, aktualizácie** atď., aby sme znížili riziko. Samozrejme, popri tom treba rátať aj s hrozbami a mať pripravené plány (incident response, zálohy, DR plány) – to je tá druhá stránka, keď riziko predsa len nastane.

---

# PROAKTÍVNA OBRANA

**Systematický a kontrolovaný proces**

**Skenovanie zraniteľností vs. Penetračné testovanie**

Obe metódy sú nevyhnutné pre komplexnú bezpečnostnú stratégiu, ale slúžia na rôzne účely.

Základný rozdiel je v prístupe **šírka vs. hĺbka** a **identifikácia vs. zneužitie**.

---

## **Proaktívna obrana: Skenovanie vs. penetračné testovanie**

Prejdime teraz k **metódam proaktívnej obrany**. Ako admini nechceme čakať, kým nás niekto hackne, aby sme zistili, že máme dieru. Chceme **predvídať a predchádzať** incidentom. Na to slúžia **procesy hodnotenia zraniteľností**, hlavne **skenovanie zraniteľností** a **penetračné testovanie**. Tieto dve metódy sa často pletú, pretože ich cieľ je podobný – nájsť slabé miesta – no ich prístup a hĺbka sú odlišné. Obe sú dôležité v komplexnej bezpečnostnej stratégii, ale **slúžia na rôzne účely**. Jednoducho povedané: **Skenovanie zraniteľností** robí **širokú inventúru** slabín – je to viac povrchové, ale zato zaberie veľkú šírku (mnoho systémov naraz).

**Penetračné testovanie** ide **do hĺbky**, simuluje skutočný útok a skúša naozaj preraziť – je to užšia zameraná akcia, ale zato dôkladná.

Niekedy sa to popisuje ako **šírka vs. hĺbka** a **identifikácia vs. zneužitie**. Poďme si ich rozobrať samostatne.

---

# SKENOVANIE ZRANITEĽNOSTÍ

## Skenovanie zraniteľností (Vulnerability Scanning)

- **Čo to je?** Prevažne **automatizovaný** proces, ktorý prehľadáva systémy s cieľom identifikovať **známe** zraniteľnosti.
  - **Cieľ:** Identifikovať a katalogizovať potenciálne slabiny. Je to preventívne opatrenie, ktoré poskytuje **široký prehľad** o bezpečnostnom stave („inventúra“ slabín).
  - **Výstup:** Podrobný report so zoznamom nájdených zraniteľností, ohodnotených podľa závažnosti.
  - **Frekvencia:** Často (týždenne, mesačne), je relatívne lacné a rýchle.
- 

## Skenovanie zraniteľností (Vulnerability Scanning)

**Čo to je?** Skenovanie zraniteľností je **prevažne automatizovaný proces**, kde špeciálny softvér (skenovací nástroj) systematicky prehľadáva vaše systémy, servery, sieťové zariadenia či aplikácie a snaží sa **identifikovať známe zraniteľnosti**. Takýto skener má databázu známych chýb (CVE), chýbajúcich záplat, konfigurácií, ktoré sú považované za nebezpečné, slabých hesiel atď.. Porovná váš systém s touto databázou a vypľuje zoznam nájdených problémov.

**Cieľ:** Skenovanie má za cieľ **identifikovať a katalogizovať potenciálne slabiny**. Inými slovami, je to **preventívne opatrenie** na získanie **širokého prehľadu** o bezpečnostnom stave – taká **inventúra slabých miest** vo vašej infraštruktúre. Skener vám povie napríklad: *“Tento server beží Windows s neaktuálnym patchom KB123, táto webová aplikácia má nezaplátanú chybu XSS, táto databáza má defaultné heslo”*, a tak ďalej.

**Výstup:** Typicky je to **podrobný report** so zoznamom nájdených zraniteľností, pričom každá je **ohodnotená podľa závažnosti** (napr. CVSS skóre) a sú tam odporúčania na nápravu. Dostanete akoby **to-do list**, čo treba opraviť – napr. aktualizovať server, vypnúť slabý protokol, nastaviť lepšie heslo atď.

**Frekvencia:** Skenovanie je pomerne **lacné a rýchle**, takže sa dá robiť **často – napríklad týždenne alebo mesačne**. V mnohých firmách beží skener nonstop a pravidelne skenuje IP rozsahy. Nie je problém spustiť ho každý večer, ak máte veľkú sieť (len pozor na záťaž). Dôležité je, že skener vie bežať automaticky bez ľudskej práce, takže **náklady a potrebné zručnosti sú relatívne nízke**. Samozrejme, treba niekoho,

kto tie reporty spracuje a zadá opravy, ale to môže byť aj junior analytik.

**Limity:** Skenovanie však má aj svoje medze. Keďže ide poväčšine o automat, dokáže odhaliť len **známe zraniteľnosti**. Nevšimne si nejakú úplne novú chybu, ktorú nemá v databáze. Tiež väčšinou nejde do nejakej kreatívnej kombinatoriky – ak by slabinu bolo treba zneužiť komplikovanejším spôsobom, skener to nevykoná. A hlavne, skener sa **nepokúša zraniteľnosť zneužiť** do hĺbky (maximálne pošle nejaký benign exploit na overenie). Čiže povie vám *“na dverách je zámok typu XY ktorý je známe že ide vypáčiť”*, ale **nevypáči ich reálne** – to by už bol pentest.

Zhrnutie: **Skenovanie zraniteľností je ako rýchla bezpečnostná prehliadka** – identifikuje všetko podozrivé, ale nepotvrduje to útokom. Je nevyhnutné pre **základnú hygienu** – viete rýchlo, kde máte aké diery, a môžete ich začať plátať.

*(Príklad nástrojov: Populárne skenery sú napr. **Nessus, OpenVAS, QualysGuard, Rapid7 InsightVM** a pod. Mnohé organizácie používajú aj open-source skripty nmap + vulners, či komunitný OpenVAS. Tie vypíšu stovky položiek, takže dôležitá zručnosť je potom **prioritizovať** – opravovať najprv kritické a vysoké riziká.)*

---

# PENETRAČNÉ TESTOVANIE

## Penetračné testovanie (Penetration Testing, Pentesting)

- **Čo to je?** Zväčša **manuálny** proces, pri ktorom etickí hackeri aktívne simulujú útok s cieľom **zneužiť** nájdené zraniteľnosti.
  - **Cieľ:** Overiť účinnosť bezpečnostných opatrení a zistiť **reálny dopad** útoku. Testuje odolnosť systému do **hĺbky**.
  - **Výstup:** Komplexná správa, ktorá obsahuje aj **dôkaz o zneužití (Proof of Concept)**, popisuje cesty útoku a hodnotí obchodný dopad.
  - **Frekvencia:** Menej často (ročne), je časovo náročné a podstatne drahšie.
- 

## Penetračné testovanie (Pentesting)

**Čo to je?** Penetračné testovanie je zväčša **manuálny proces**, pri ktorom **etickí hackeri (pentesteri)** aktívne simulujú **reálny útok** na vaše systémy s cieľom **preniknúť dnu**.

Kým skener je stroj, pentest robia ľudia (hoci používajú aj nástroje). Pentester sa správa ako skutočný útočník – najprv preskúma systém (informačný zber), potom skúša rôzne útoky, hľadá slabiny a tie sa snaží **skutočne zneužiť** (exploituje ich), aby dokázal, že sa cez ne vie dostať.

**Cieľ:** Overiť **účinnosť bezpečnostných opatrení** a zistiť **reálny dopad útoku**. Pentest nejde len o to niečo nájsť, ale **otestovať odolnosť systému v hĺbke** – či sa dá prelomiť a čo z toho plyní. Pentester sa často snaží dostať čo najďalej – napríklad získať administrátorský prístup, ukradnúť citlivé dáta, pivotnúť do vnútornej siete. Ide o taký **záťažový test** bezpečnosti v praxi.

**Výstup:** Je to typicky **komplexná správa**, ktorá obsahuje nielen zoznam nájdených zraniteľností, ale aj **dôkaz o zneužití (Proof of Concept)**, popis priebehu útoku a vyhodnotenie obchodného dopadu. Napríklad správa povie: *“Na serveri X sme našli SQL Injection, použili sme ho na získanie databázy zákazníkov, tu je výpis 10 záznamov ako dôkaz, a keby to bol ostrý útok, unikli by všetky zákaznícke údaje – dopad: vysoký.”* Čiže menežment dostane **konkrétny obraz**, čo by reálny hacker mohol spôsobiť a aké následky by to malo.

**Frekvencia a náklady:** Pentesty sú **časovo náročné a drahšie**. Zväčša sa robia **menej často** – napríklad raz za rok, alebo po veľkých zmenách v infraštruktúre. Vyžadujú

**vysoko kvalifikovaných ľudí**, ktorí vedia myslieť ako útočník. Preto ich kapacita je drahá. Napríklad externý pentest pre strednú firmu môže trvať 2-6 týždňov a stáť tisíce eur. Pentesty teda nerobíte denne – skôr periodicky na kritické systémy, alebo keď potrebujete audit (napr. kvôli norme PCI DSS v bankovníctve).

**Rozdiel oproti skenu:** Ako už asi jasné, **pentesting ide užšie a hlbšie**. Namiesto toho, aby testoval 1000 serverov povrchno, vezme si 10 najdôležitejších a skúša všetko možné do detailu. Tam, kde skener zahlási “port 443 open, možno zraniteľný na CVE-XYZ”, tam pentester reálne vyšle exploit a skúsi ten server ovládnuť. Pentester tiež vie robiť **kreatívne veci**: kombinovať viac zdanlivo nízko závažných chýb dokopy na preniknutie, využívať logické chyby, sociálne inžinierstvo, atď. Skener by vám ich neodhalil, lebo také kombinácie sa do skriptu nedajú ľahko dať.

Zhrnuté: **Pentest je simulovaný útok na mieru**. Je nevyhnutný, ak chcete vedieť, či vaša bezpečnosť obstojí proti schopnému hackerovi. Ale pre bežnú dennú prevádzku by sa pentesteri “*neuživili*”, tam nastupuje skenovanie.

*(Príklad: Firma môže mať permanentne nasadený skener na internú sieť, ktorý generuje mesačne reporty a admini priebežne opravujú chyby. A raz ročne si zavolá externú firmu na pentest internet-banking aplikácie a firemnej siete – tí strávia 3 týždne intenzívnym testovaním, nájdu hlbšie veci a firma ich potom opraví. Taký model je veľmi častý.)*

---

# POROVNANIE: SKENOVANIE vs. PENTESTING

Tabuľka 2: Porovnanie skenovania zraniteľností a penetračného testovania

Atribút	Skenovanie zraniteľností	Penetračné testovanie
Cieľ	Identifikovať známe zraniteľnosti (šírka).	Zneužiť zraniteľnosti a posúdiť reálny dopad (hĺbka).
Metóda	Prevažne automatizovaná, pasívna.	Prevažne manuálna, aktívna, simulácia útoku.
Frekvencia	Vysoká (denne, týždenne).	Nízka (štvrtročne, ročne).
Náklady	Stredné.	Vysoké.
Výstup	Zoznam potenciálnych zraniteľností.	Dôkaz o zneužití (PoC), cesty útoku.
Najlepšie pre	Pravidelnú hygienu, compliance.	Hĺbkové overenie bezpečnosti.

---

## Porovnanie: Skenovanie vs. Pentesting

Pre lepší prehľad môžeme zhrnúť kľúčové rozdiely medzi skenovaním a pentestom:

**Šírka vs. hĺbka:** Skenovanie pokryje široko veľa systémov, pentest ide do hĺbky na vybrané systémy.

**Automatizované vs. manuálne:** Sken je z 90 % automat, pentest z veľkej časti ručná expertná činnosť (hoci používajú skripty a exploity).

**Identifikácia vs. zneužitie:** Skener identifikuje potenciálne problémy, pentester skúša reálne zneužiť a potvrdiť problémy.

**Výstup:** Skener dá zoznam možných zraniteľností (aj false positives niekedy), pentest dá potvrdené zneužitia a cesty útoku.

**Frekvencia:** Skenovanie často (aj denne či týždenne pri kontinuálnom monitoringu), pentest zriedka (ročné, polročné intervaly).

**Cena a zdroje:** Skener lacný (licencia + 1 admin), pentest drahý (platení experti hodiny práce).

**Použitie:** Sken sa hodí na **priebežnú hygienu a compliance** (napr. aby ste plnili základné bezpečnostné štandardy), pentest na **hĺbkové overenie bezpečnosti a prípravu na reálne útoky**.

Obe metódy sa navzájom **dopĺňajú**. Skenovanie môže bežať celý rok a udržiavať vám akú-takú hygienu; pentest raz za čas preverí, či vám niečo neuniklo alebo či nejaká kombinácia slabín nevedie ku kritickému prieniku. Pentesting často využíva výsledky skenu ako východisko (pentesteri si nechajú dať posledný VA scan report, aby vedeli

základné info, a potom idú ďalej kreatívne).

Pre správcu systémov je dobré vedieť argumentovať manažmentu, prečo potrebujete oboje. Napríklad môžete povedať: **“Lacné a pravidelné skenovanie je nutné na splnenie compliance požiadaviek a udržanie základnej ochrany. Ale iba drahší ročný pentest vie skutočne overiť, či sme odolní proti špičkovému útočníkovi.”** Tým pádom viete zdôvodniť rozpočet na bezpečnosť – lebo niekedy sa CFO spýta, na čo platíme aj skener, aj hackerov. Odpoveď: je to ako rozdiel medzi pravidelnou servisnou prehliadkou auta a crash testom. Servis (sken) spraví základnú kontrolu, ale občas treba spraviť crash test (pentest), aby sme vedeli, čo sa stane pri náraze.

---

# OBRANA PERIMETRA: FIREWALLY

## Obrana perimetra: Tradičné firewally, UTM a NGFW

- **Tradičný (stavový) firewall:**
    - Filtruje prevádzku na základe IP adresy, portov a protokolov (vrstva 3 a 4 OSI modelu).
  - **UTM (Unified Threat Management):**
    - Zariadenie „všetko v jednom“ pre malé a stredné podniky (SMB).
    - Spája firewall, antivírus, VPN atď. do jedného zariadenia.
    - Výhodou je jednoduchosť, nevýhodou môže byť nižší výkon.
  - **NGFW (Next-Generation Firewall):**
    - Pokročilý firewall, ktorý pridáva kľúčové schopnosti na úrovni aplikácií (vrstva 7 OSI modelu).
- 

## Obrana perimetra: Firewally (tradičné, UTM, NGFW)

**Firewall** je asi najznámejší bezpečnostný prvok siete. Je to v podstate **bariéra medzi internou (dôveryhodnou) sieťou a externou (nedôveryhodnou) sieťou**. Predstavte si ho ako **vrátnika**, ktorý stojí na okraji vašej siete a **filtruje prichádzajúcu a odchádzajúcu sieťovú prevádzku** podľa nastavených pravidiel. Firewally prešli dlhým vývojom. Máme:

**Tradičný stavový firewall** – toto je staršia generácia firewallov, ktoré pracujú na 3. a 4. vrstve OSI modelu (sieťová a transportná vrstva). Znamená to, že **filtrujú podľa IP adries, portov a protokolov**, a sledujú stav spojení (napr. že ide o odpoveď na požiadavku zvnútra). Napríklad pravidlo: povoliť prichádzajúce TCP spojenia na port 80 na webový server z internetu, inak všetko zamietnuť. Tieto firewally nerozumejú tomu, aký obsah nesú pakety, len vidia hlavičky (adresy, porty). Boli revolučné v 90. rokoch, ale dnes sú základom, na ktorom sa stavia ďalej.

**UTM – Unified Threat Management** – tzv. **“všetko v jednom” zariadenie** pre malé a stredné podniky. UTM kombinuje firewall s ďalšími bezpečnostnými funkciami: často má v sebe okrem firewallu aj antivírus pre kontrolu prechádzajúceho obsahu, antispam, VPN bránu, web filter atď., všetko v jednom boxe s jednotnou správou. Výhoda:

**jednoduchosť** – menšia firma si kúpi jedno zariadenie, dostane komplexnú ochranu.

Nevýhoda: **výkon** – keď jedno zariadenie robí všetko, pri vyššej záťaži nestíha alebo musíte investovať do drahšieho modelu. UTM sa hodí tam, kde nemáte veľký IT tím ani komplexnú sieť a chcete plug-and-play ochranu.

**NGFW – Next-Generation Firewall** – moderný firewall, ktorý predstavuje **evolúciu tradičného firewallu**. NGFW robí všetko, čo tradičný (stavový) firewall, ale pridáva **klúčové schopnosti na aplikačnej vrstve (7. vrstva OSI)** a integruje pokročilé bezpečnostné funkcie. Prakticky NGFW často zahrňuje aj UTM funkcie, ale posúva sa ďalej vo výkone a granularite. Je cielený pre stredné a väčšie podniky, kde chcete detailnú kontrolu.

---

## KLÚČOVÉ VLASTNOSTI NGFW

### Čo dokáže Next-Generation Firewall?

- **Deep Packet Inspection (DPI):** Analyzuje nielen hlavičky paketov, ale aj ich obsah.
  - **Povedomie o aplikáciách (App-ID):** Dokáže identifikovať a riadiť konkrétne aplikácie (napr. Facebook, Dropbox) bez ohľadu na použitý port. Umožňuje granulórne pravidlá.
  - **Integrovaný Intrusion Prevention System (IPS):** Aktívne deteguje a blokuje známe sieťové útoky.
  - **Povedomie o používateľoch (User-ID):** Umožňuje vytvárať pravidlá založené na identite používateľa alebo skupiny, nielen na IP adrese.
- 

Pozrime sa bližšie na **klúčové vlastnosti NGFW:**

**Deep Packet Inspection (DPI)** – Kým tradičný firewall pozeral len na hlavičky paketov, **NGFW analyzuje aj obsah paketov** v reálnom čase. Teda vie napríklad zistiť, že hoci komunikácia ide na port 80 (HTTP), vo vnútri je podozrivý kód alebo malware. DPI umožňuje odhaliť útoky skryté v bežnej prevádzke (napr. exploit v HTTP požiadavke).

**Application awareness (App-ID)** – NGFW **rozpoznáva konkrétne aplikácie a protokoly**, nielen podľa portu. Napríklad tradičný FW vidí port 443 a myslí si “aha, HTTPS”. NGFW sa pozrie do šifrovaného toku (ak má dešifrovanie) alebo podľa vzorcov a zistí: “toto nie je web, to je vlastne VPN alebo BitTorrent traffic”. Vie tak identifikovať stovky aplikácií (Facebook, YouTube, Skype, atď.) podľa signatúr. **Umožňuje to písať pravidlá na úrovni aplikácií:** napr. “*povoliť Facebook, ale blokovať v ňom chat*” alebo “*zakázať Tor sieť*” atď. Pre firmy je to užitočné na kontrolu, čo ľudia robia na sieti.

**Integrovaný IPS (Intrusion Prevention System)** – NGFW má často v sebe plnohodnotný **IPS modul**, čiže vie **aktívne detegovať a blokovať známe útoky a exploity** v sieti. Tradične ste mali separé IDS/IPS box, ale NGFW ho integruje, takže na rovnakom zariadení beží aj kontrola signatúr útokov, anomálií atď. Čiže ak prichádza exploit na web server, NGFW ho rozpozná a zahodí (aj keď by prešiel firewall pravidlom).

**User-ID (povedomie o používateľoch)** – NGFW sa dokáže integrovať s adresárovými službami ako **Active Directory** a **mapovať IP adresy na konkrétnych používateľov**. Potom viete písať politiky typu “*povoliť prístup na databázový server iba užívateľovi Jozef.Majko alebo členom skupiny DB-Admin*” namiesto IP adries. To výrazne

zjednodušuje politiku v prostredí, kde IP nie sú fixné alebo ich je veľa – pravidlá viete naviazať na identity a skupiny.

(Ďalšie: NGFW často ponúka aj SSL dešifrovanie a kontrolu šifrovaného toku, sandboxing neznámeho malware, a rôzne fancy featury, ale to už závisí od konkrétneho výrobcu.)

**NGFW vs. UTM:** Niekedy sa NGFW a UTM zamieňajú, lebo obe spájajú viac funkcií. Hlavný rozdiel je však **v cieľovej skupine a architektúre**. UTM je pre SMB – kladie dôraz na **široké spektrum funkcií v jednom jednoduchom balíku**, ale nie nutne na vysoký výkon. NGFW je pre enterprise – kladie dôraz na **výkon, škálovateľnosť a detailnú kontrolu**. NGFW býva robustnejší, zvládne viac throughputu, má modulárny softvér, lepšiu integráciu do veľkých sietí. UTM je skôr “plug and play with wizard”, NGFW má tisíc nastavovaní pre experta. Preto vo veľkej korporácii nasadíte NGFW od Palo Alto alebo Fortinet a v malej firme napr. Zyxel UTM zariadenie.

*(Na trhu dnes vlastne všetci veľkí hráči nazývajú svoje produkty NGFW: Check Point, Palo Alto, Fortinet, Cisco Firepower atď. Ide o to, že v dnešnej dobe obyčajný firewall nestačí, keď veľká časť útokov sa maskuje ako legitímna prevádzka na povolených portoch. NGFW je odpoveď – dáva nám “RTG snímok” do paketov.)*

---

# DETEKCIA A PREVENCIA PRIENIKOV

## Systémy na detekciu a prevenciu prienikov (IDS/IPS)

- **IDS (Intrusion Detection System):**
    - Je **pasívny** monitorovací systém.
    - Analyzuje prevádzku a v prípade podozrenia vygeneruje **upozornenie** (alert).
    - Hrozbu samotnú neblokuje.
  - **IPS (Intrusion Prevention System):**
    - Je **aktívny** systém, nasadený priamo v ceste prevádzky (*inline*).
    - Nielenže hrozby deteguje, ale dokáže ich v reálnom čase aj **blokovat'**.
- 

## Detekcia a prevencia prienikov (IDS/IPS)

Ďalším dôležitým prvkom obrany sú **IDS a IPS systémy** – čiže **Intrusion Detection System** a **Intrusion Prevention System**. Už sme ich trochu načali pri NGFW, ale povedzme si všeobecne.

**IDS (Systém detekcie prienikov):** Je to **pasívny monitorovací systém**. IDS sa umiestni do siete tak, že **sleduje sieťovú prevádzku (alebo logy)**, ale **nezasahuje do nej**. Funguje často tak, že má sniffer port (napr. cez mirror port na prepínači) a analyzuje premávku. Keď IDS **deteguje podozrivú aktivitu**, vygeneruje **upozornenie (alert)** pre administrátorov. Napríklad: zistí signatúru známeho útoku na SMB protokol, tak pošle alert, že "tento počítač možno napadnutý exploitom EternalBlue". **Nič však automaticky neblokuje** – to už musí človek alebo iný systém zareagovať.

**IPS (Systém prevencie prienikov):** IPS je vlastne **IDS, ktorý je zapojený inline a vie aktívne zasiahnuť**. Čiže IPS sedí priamo v ceste sieťovej komunikácie (napr. ako brána) a keď vidí niečo, čo vyhodnotí ako útok, **zasiahne v reálnom čase** – napríklad zahodí tie škodlivé pakety alebo zresetuje spojenie. Čiže IPS nielen deteguje, ale aj **prevenciu vykoná**.

Dnes sa často stretnete s kombinovaným pojmom IDS/IPS, lebo moderné systémy môžu pracovať v oboch módoch (len monitor alebo aktívny mód). Ak nasadíte v monitorovacom móde a potom prepnete do inline, stane sa z IDS-u IPS.

---

# METÓDY DETEKČIE IDS/IPS

## Ako IDS/IPS systémy detegujú hrozby?

- **Detekcia založená na signatúrach (Signature-Based):**
    - Porovnáva prevádzku so známymi vzormi (signatúrami) útokov.
    - Veľmi efektívna pri detekcii **známych hrozieb**, ale nedokáže odhaliť nové útoky (*zero-day*).
  - **Detekcia založená na anomáliách (Anomaly-Based):**
    - Vytvorí si model „normálneho“ správania siete a upozorňuje na akékoľvek odchýlky.
    - Dokáže detegovať aj **nové typy útokov**, ale je náchylná na generovanie falošných poplachov (*false positives*).
- 

**Metódy detekcie:** Ako IDS/IPS rozpoznáva, že niečo je útok? Má typicky dve hlavné metódy:

**Detekcia na základe signatúr (signature-based)** – Systém má databázu **signatúr známych útokov** (podobne ako antivírus) a porovnáva sieťovú prevádzku s týmito vzormi. Napríklad signatúra môže byť reťazec bajtov, ktorý sa vyskytuje v exploite pre CVE-1234, alebo sekvencia volaní, ktorá indikuje portscan. Výhoda: je to **veľmi efektívne a presné pre známe hrozby** – málo falošných poplachov a rýchla detekcia. Nevýhoda: **neodhalí niečo úplne nové** – ak príde zero-day útok, na ktorý ešte nie je signatúra, prešmykne sa.

**Detekcia na základe anomálií (anomaly-based)** – Systém si vytvorí **model “normálneho” správania siete** (baseline) a potom **hľadá odchýlky od tohto normálu**. Napríklad: normálne z tohto PC odchádza max 1 Mbps traffic, zrazu odtiaľ ide 50 Mbps – to je anomália, možno exfiltrácia dát. Alebo normálne nikto neposiela 1000 ICMP paketov za sekundu – ak sa tak deje, asi prebieha ping flood útok. Výhoda: **môže odhaliť aj úplne nové, neznáme typy útokov**, lebo sa nespolieha na signatúry, ale na “niečo tu nesedí”. Nevýhoda: **náchylnosť na falošné poplachy** (false positives) – niekedy legitímna aktivita vyzerá ako odchýlka (napr. zálohovanie veľkého objemu dát v noci by mohol IDS vyhodnotiť ako anomáliu). Administrátori tak môžu byť zaplavení alertami, ktorých vyhodnocovanie ich unaví.

Preto v praxi IDS/IPS systémy kombinujú obe metódy. Najskôr sa aplikuje signatúrna detekcia (rýchla a presná) a popritom beží anomálny modul na advanced threats. Admini

môžu ladiť citlivosť, vypínať signatúry, ktoré generujú plané popluchy, atď.  
(Príklad IDS/IPS systémov: **Snort** (open-source IDS), *Suricata*, proprietárne od Cisco (Sourcefire), Palo Alto má v NGFW integr. IPS, atď. Často sa stretnete s tým, že IDS/IPS je vlastne súčasť NGFW alebo UTM. Ale veľké siete môžu mať špecializované IPS senzory s vysokým výkonom, najmä na kritických segmentoch.)

---

## HIDS vs. NIDS

### Typy nasadenia: HIDS vs. NIDS

- **HIDS (Host-based IDS):**
  - Nainštalovaný na **jednotlivých zariadeniach** (serveroch, PC).
  - Monitoruje interné aktivity systému: logy, integritu súborov, procesy.
  - Poskytuje pohľad na to, čo sa deje **VNÚTRI** systému.
- **NIDS (Network-based IDS):**
  - Nasadený na strategických bodoch **v sieti**.
  - Monitoruje všetku prevádzku, ktorá prechádza **CEZ** sieť.
  - Poskytuje pohľad na to, čo sa deje **MEDZI** systémami.

Tieto dva systémy sa dopĺňajú v rámci stratégie obrany do hĺbky (*defense in depth*).

---

### HIDS vs. NIDS – nasadenie IDS na hoste a v sieti

Ešte spomeniem rozdiel medzi **HIDS (Host-based IDS)** a **NIDS (Network-based IDS)**, pretože je dôležité nasadiť detekciu na viacerých úrovniach:

**HIDS (Host-based IDS):** Je to IDS, ktorý beží **priamo na koncovom zariadení** (hoste) – napr. na serveri alebo PC. Monitoruje **vnútorné aktivity toho systému**: systémové logy, integritu súborov, bežiacie procesy, registruje pokusy o neautorizované zmeny, atď. Poskytuje detailný pohľad **vnútri daného zariadenia**. Napríklad Tripwire je HIDS, ktorý vás upozorní, ak sa zmenil obsah kritického súboru, čo by mohlo indikovať zásah malvéru.

**NIDS (Network-based IDS):** Toto je klasický IDS, o akom sme hovorili – nasadený **na strategických bodoch v sieti**, sleduje **sieťovú komunikáciu medzi zariadeniami**. Čiže napríklad senzor na hranici siete za firewallom, alebo v DMZ sieti sledujúci prevádzku do a z databázového servera. Poskytuje prehľad o tom, **čo sa deje medzi systémami po sieti**.

Tieto dve prístupy sa **nevylučujú, ale dopĺňajú** v rámci filozofie “**defense in depth**” (**obrana do hĺbky**). NIDS vidí veci typu “*niekto skenuje naše porty, niekto skúša poslať exploit*”, HIDS zas vidí “*tento súbor sa zmenil, v logu pribudlo 100 pokusov o prihlásenie*”. Ak útočník obíde sieťovú detekciu (napr. šifrovaná komunikácia), HIDS ho môže odhaliť na hoste (napr. zrazu nový proces beží). Preto robustné bezpečnostné programy implementujú oboje.

Správca systémov môže využiť tento fakt aj pri zdôvodnení investícií: Napríklad **navrhne**

**nasadiť NIDS senzor na perimetri siete pre blokovanie všeobecných útokov** (vonkajších), a **HIDS agentov na kritické servery** (databázy, web servery) pre ochranu pred cieľenými útokmi a monitorovanie, čo sa deje na nich. NIDS totiž nevidí dovnútra šifrovaného spojenia do webservera (ak nerobí dešifrovanie, čo je niekedy právny problém), ale HIDS na tom webserveri vidí, že zrazu príkazový riadok beží pod webovým procesom – bingo, to je indikácia útoku.

*(Zhrnutie: Udržujte **viac vrstiev detekcie** – perímetrovo aj host-based. Je to ako mať stráž na hradbách aj v strážnej veži vnútri hradu.)*



---

## KLÚČOVÉ ZÁVERY A TRENDY

- **Riadenie zraniteľností je disciplínou riadenia rizík, nie len IT operácií.** Vyžaduje strategický dohľad a pochopenie obchodného kontextu.
  - **Prechod od kvantity ku kvalite je nevyhnutný.** Snaha "opraviť všetko" je neudržateľná. Strategický posun k prioritizácii na základe reálneho rizika (Risk-Based Vulnerability Management) je jediným udržateľným prístupom.
  - **Bezpečnosť sa posúva "doľava" (Shift-Left).** S nástupom DevSecOps sa ťažisko presúva na analýzu kódu a konfigurácií ešte pred nasadením.
  - **Definícia "nápravy" sa rozširuje.** Okrem tradičnej záplaty existuje aj virtuálne záplatovanie a preventívne opatrenia.
- 

Dostali sme sa na koniec nášho rozsiahleho výletu kybernetickou bezpečnosťou pre obe skupiny poslucháčov. **Aké sú kľúčové závery?** V prvom rade, či už ste bežný používateľ alebo správca, uvedomte si, že **riadenie zraniteľností a aktualizácií je nekončiaci cyklus** – stále hodnotíme nové hrozby, posilňujeme obranu a pripravujeme sa na prípadné incidenty. Nie je to jednorazový projekt, ale **nepretržitý proces**. Pre **bežných používateľov** znova zdôrazním tri piliere: **heslá, 2FA, aktualizácie** (a plus zálohy ako záchrana). Vaša rola v bezpečnosti je nezastupiteľná – vzdelaný používateľ vie predísť množstvu útokov tým, že nespraví triviálnu chybu. Ako sme povedali, úspech v kyberbezpečnosti si vyžaduje **vzdelaných používateľov, kompetentných správcov a strategicky uvažujúcich špecialistov – všetkých dohromady**.

Pre **správcov** a organizácie tu máme niekoľko trendov:

**Riadenie zraniteľností je vlastne riadenie rizík** – už to nie je len IT úloha "aplikuj update". Stáva sa to súčasťou celkového risk managementu firmy. Rámce ako NIST CSF 2.0 dokonca pridávajú funkciu "Govern", ktorá formalizuje, že vedenie má dozeráť na kybernetické riziká. Treba brať do úvahy obchodný kontext, dodávateľské reťazce atď., nielen techniku.

**Od kvantity ku kvalite:** S tým, ako počet zraniteľností neustále rastie (tzv. *vulnerability fatigue*), už sa nedá všetko zaplátať hneď. Treba **prioritizovať na základe reálneho rizika** – tzv. **Risk-Based Vulnerability Management (RBVM)**. Teda pozeráť nielen CVSS skóre, ale aj kritickosť aktíva a reálne hrozby. Opraviť radšej 10 najrizikovejších

dier než 100 menej podstatných, ak nemáme kapacity na všetko. Len tak to bude udržateľné.

**Shift-left v bezpečnosti:** Bezpečnosť sa posúva “doľava” – t.j. **bližšie k fáze vývoja (build) a ďalej od runtime**. S príchodom DevSecOps, kontajnerov, infra as code sa stále viac bezpečnostných aktivít deje ešte pred nasadením do produkcie. Napríklad integrácia skenerov do CI/CD pipeline, kontrola IaC skriptov na chyby, automatizované code security testy. Cieľom je **predchádzať zraniteľnostiam už pri vzniku**, nie až hasiť v bežiacich systémoch. Tým sa dramaticky znižuje náklad na opravu (chybu je lacnejšie opraviť v kóde pred nasadením ako patchovať výrobu).

**Rozšírenie pojmu “náprava” (remediation):** Klasicky sme brali nápravu zraniteľnosti ako nainštalovanie patchu. Dnes to už nie je jediná možnosť. Máme **virtuálne záplatovanie** (napr. WAF alebo IPS pravidlo, ktoré zablokuje exploit skôr než nasadíme patch) a **preventívne opatrenia v SDLC** (ako spomenuté shift-left). Čiže ak je zero-day, možno nasadíme dočasne IPS filter – to je remediation na úrovni prevencie. Alebo ak starý systém nejde updatovať (legacy), nasadíme segmentáciu okolo neho. Budúcnosť sľubuje aj využitie AI na predikciu zraniteľností a automatizáciu záplatovania. Každopádne, pojem opravy zraniteľností sa rozširuje za hranice len “aplikuj oficiálny patch”.

Celkovo teda vidíme, že **kybernetická bezpečnosť dospieva** – spája technické, organizačné aj strategické prístupy. Už to nie je doména pár adminov v rohu serverovne; týka sa to manažmentu, vývojárov, každého zamestnanca.

---

# FINÁLNE POSOLSTVO

## Spoločne k bezpečnejšej digitálnej spoločnosti

Úspech v kybernetickej bezpečnosti si vyžaduje:

- **Vzdelaných používateľov**, ktorí rozumejú základným hrozbám a ovládajú základné obranné postupy.
  - **Kompetentných správcov**, ktorí rozumejú technológiám a procesom riadenia bezpečnosti.
  - **Strategicky uvažujúcich špecialistov**, ktorí integrujú bezpečnosť do celopodnikového riadenia rizík.
- 

**Bezpečnejšiu digitálnu spoločnosť vieme vybudovať len spoločne.** Kybernetická bezpečnosť nie je len o firewalle alebo antivírose – je to hlavne o ľuďoch. Potrebujeme **vzdelaných používateľov**, ktorí rozumejú základným hrozbám a vedia sa brániť základnými postupmi (to bola celá prvá časť). Ďalej potrebujeme **kompetentných správcov**, ktorí vedia tie technológie nastaviť, udržiavať, reagovať na incidenty a stále zlepšovať bezpečnosť (o tom bola druhá časť). A v neposlednom rade **strategicky zmýšľajúcich špecialistov a lídrov**, ktorí začlenia bezpečnosť do celkového riadenia, budú myslieť dopredu a podporia kultúru bezpečnosti odhora.

Každý z nás má v tom rolu: či už si doma nastavíte lepšie heslo, alebo vo firme nasadíte nový IDS, alebo na úrovni štátu prijmete zákon na zvýšenie kyber ochrany – **všetko sa počíta**. Kybernetické útoky tu s nami budú neustále a budú sa vyvíjať. Ale ak budeme **spolupracovať, vzdelávať sa a používať rozum aj technológie**, máme šancu ten pomyselný boj udržať pod kontrolou.