

Bezpečnosť prevádzky informačných systémov a sietí

21. novembra 2025



PLÁN [OBNOVY]



- 1 Úvod: Prečo je kybernetická bezpečnosť dôležitá?
- 2 Bezpečnosť prevádzky informačných systémov
- 3 Bezpečnosť DNS - Doménového systému mien
- 4 Bezpečnosť priemyselných (OT/SCADA) systémov
- 5 Praktické odporúčania pre každého
- 6 Záver a kľúčové posolstvá

Prečo je kybernetická bezpečnosť dôležitá?

Realita dnešného sveta

Každých **39 sekúnd** dochádza k kybernetickému útoku niekde na svete.

Čo je v ohrození:

- Osobné údaje a súkromie
- Finančné prostriedky
- Obchodné tajomstvá
- Kritická infraštruktúra
- Zdravie a bezpečnosť ľudí

Príklady reálnych útokov:

- Ransomvér - zašifrovanie dát
- Krádež identít a hesiel
- Finančné podvody
- Výpadky elektriny
- Priemyselné havárie

Kľúčové posolstvo

Každý zamestnanec je súčasťou obrany organizácie

Prečo dodržiavať pravidlá?

Nie je to len o technikách - je to aj o zákonoch a zodpovednosti

Medzinárodné štandardy:

- **ISO 27001** - Systém riadenia informačnej bezpečnosti
- **NIST CSF** - Framework kybernetickej bezpečnosti
- **CIS Benchmarks** - Odporúčania pre konfiguráciu

Slovenská legislatíva:

- Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti
- Vyhláška č. 362/2018 Z.z.
- **NIS2** - nové povinnosti od 2025

GDPR a pokuty

Porušenie GDPR môže znamenať pokutu až **20 mil. €** alebo **4% globálneho obratu!**

Zero Trust Architecture (ZTA)

Nová bezpečnostná filozofia

„Nikdy nedôveruj, vždy overuj”

Tradičný prístup (zastaraný):

- Dôvera všetkému vo vnútornej sieti
- Pevný perimeter (hradby)
- Ak ste „dnu”, máte prístup

Problém: Útočník vo vnútri má voľnú ruku

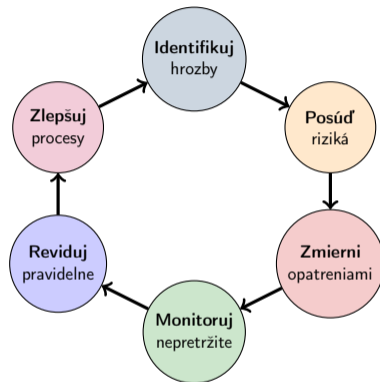
Zero Trust (moderný):

- Nikdy automaticky nedôverovať
- Overovať každý prístup
- Minimálne oprávnenia
- Predpokladať narušenie

Výhoda: Aj keď útočník vstúpi, nemá voľný pohyb

Analógia

Ako v hoteli - aj keď ste hosť, potrebujete kartu ku každým dverám, nie len na recepciu.



Základný princíp

Riadenie rizík je **nepretržitý cyklus**, nie jednorazová aktivita

Definícia

Proces minimalizácie útočnej plochy systému odstránením nepotrebných funkcií a posilnením bezpečnostnej konfigurácie.

Základné kroky:

- 1 Silné heslá a MFA
- 2 Odstránenie nepotrebných programov
- 3 Vypnutie nepotrebných služieb
- 4 Aktualizácie a záplatovanie
- 5 Obmedzenie sieťových portov
- 6 Minimálne oprávnenia

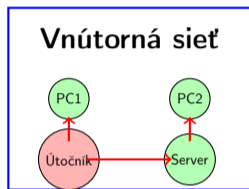
Štandardy pre hardening:

- **CIS Benchmarks** - konkrétne pokyny pre OS, databázy, cloud
- **NIST SP 800-53** - katalóg kontrol
- **ISO 27001** - požiadavky ISMS

Príklad

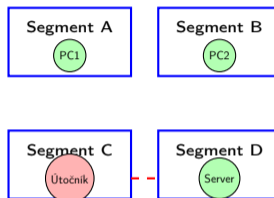
Windows Server s vypnutým Telnet, RDP len cez VPN, firewall zapnutý

Tradičná sieť (problém):



Útočník má prístup všade

Mikrosegmentácia (riešenie):



Blokované!

Princíp

Každý systém/aplikácia je v oddelenom segmente s presnými pravidlami komunikácie.

Reálny príklad

Databáza smie komunikovať len s webovým serverom, nie s PC zamestnancov.

Čo je DNS a prečo je dôležitý?

DNS - Domain Name System

„Telefonný zoznam internetu” - prekladá ľudsky čitateľné názvy (www.google.com) na IP adresy (142.250.185.78)

Ako funguje DNS:

- 1 Napíšete www.banka.sk do prehliadača
- 2 Počítač sa opýta DNS servera
- 3 DNS server odpovie IP adresou
- 4 Prehliadač sa pripojí na IP adresu
- 5 Vidíte webstránku banky

Prečo je DNS cieľom útokov:

- Nemá natívne šifrovanie
- Nemá natívnu autentifikáciu
- Implicitne dôveryhodný
- Prechádza firewall
- Ak je narušený, útočník môže:
 - Presmerovať na falošné stránky
 - Kradnúť heslá
 - Šíriť malvér

1 DNS Cache Poisoning/Spoofing

- Útočník vloží falošné dáta do DNS cache
- Obete sú presmerované na škodlivé stránky
- Trvá až do vymazania cache (hodiny/dni)

2 DNS Hijacking (Únos DNS)

- Zmena DNS nastavení na routeri/PC
- Malvér mení lokálne DNS
- Všetka prevádzka cez útočníkov server

3 DNS Tunneling

- Skrytie komunikácie v DNS požiadavkách
- Obchádzanie firewallov
- Krádež dát (exfiltrácia)

4 DNS Amplifikácia (DDoS)

- Zahľtenie cieľa obrovským objemom dát
- Zneužitie otvorených DNS serverov
- Amplifikačný faktor až 50:1

DNSSEC:

- **Čo rieši:** Autenticitu a integritu
- **Ako:** Digitálne podpisy
- **Chráni pred:** Cache poisoning, spoofing
- **Nechráni:** Súkromie (stále nešifrované)

DNS záznam + Podpis

Šifrované DNS (DoT/DoH):

- **Čo rieši:** Súkromie a dôvernosť
- **Ako:** Šifrovanie TLS/HTTPS
- **Chráni pred:** Odpočúvaním, sledovaním
- **Problém:** Strata viditeľnosti pre bezpečnostné nástroje

DNS dotaz Šifrované

Odporúčanie

Ideálne použiť **obe technológie** - DNSSEC (autenticita) + DoT/DoH (súkromie)

V firemnom prostredí

DoH môže byť problém - obchádza firemnú DNS politiku Zvážte DoT.

Čo sú OT/SCADA systémy?

Definícia

OT (Operational Technology) - Hardvér a softvér, ktorý monitoruje a riadi fyzické procesy a zariadenia v priemysle.

Príklady OT systémov:

- Elektrárne a rozvodne
- Vodárne a čistiarne odpadových vôd
- Výrobné linky v továrňach
- Chemické závody
- Plynárne a ropovody
- Dopravné systémy (semafóry, metro)
- Inteligentné budovy (HVAC)

Prečo sú kritické:

- Ovplyvňujú fyzický svet
- Zlyhanie = ohrozenie životov
- Zlyhanie = ekonomické škody
- Dlhý životný cyklus (20-30 rokov)
- Často zastaralé systémy
- Nemožnosť vypnutia na údržbu

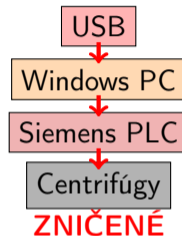
Prvá digitálna zbraň

Cieľ:

- Sabotáž iránskych centrifúg na obohacovanie uránu
- Fyzické zničenie zariadení

Ako fungoval:

- 1 Šíril sa cez USB kľúče (air-gap bypass)
- 2 Využil 4 zero-day zraniteľnosti
- 3 Infikoval Windows PC
- 4 Našiel Siemens PLC riadiace centrifúgy
- 5 Zmenil rýchlosť otáčania
- 6 Centrifúgy sa zničili



Poučenie

Aj „izolovaný“ systém môže byť napadnutý!

Ako chrániť OT systémy?

1. Segmentácia:

- Oddelenie IT od OT
- DMZ zóna medzi nimi
- Purdue Model - vrstvomá architektúra
- Firewall medzi úrovňami

2. Správa aktív:

- Vedieť, čo všetko máte
- Inventár zariadení
- Verzie firmvéru
- Kritickosť pre proces

3. Monitoring:

- Pasívne monitorovanie siete

4. Prístup:

- Zero Trust aj v OT
- MFA pre vzdialený prístup
- Jump servery v DMZ
- Auditovanie prístupov

5. Záplatovanie (keď možné):

- Testovanie mimo produkcie
- Schvaľovací proces
- Okná údržby
- Záložné systémy

6. Kompenzačné kontroly:

- Ak nemôžete záplatovať

Silné heslá a viacfaktorová autentifikácia (MFA)

Slabé heslá (NIKDY):

123456, password, qwerty,
meno + rok narodenia, firma2024

Čas na prelomenie: sekundy

Silné heslá:

- Min. 14 znakov
- Kombinácia: A-z, 0-9, #,%
- Unikátne pre každý účet
- Správca hesiel

Čas na prelomenie: roky

Typy MFA:

- SMS kód (najslabší)
- Autentifikačná appka (Google Authenticator)
- Hardvérový token (YubiKey)
- Biometria (Face ID, odtlačok)

Štatistika

MFA blokuje 99.9% automatizovaných útokov

Pravidlo

Nikdy nepoužívajte rovnaké heslo na rôznych miestach

Čo je phishing?

Podvodné e-maily alebo SMS správy, ktoré sa tvária ako legitímne a snažia sa vás oklamať.

Príznaky phishingu:

- 1 Neočakávaný e-mail
- 2 Naliehavosť: „Konajte TERAZ“
- 3 Hrozby: „Účet bude zablokovaný!“
- 4 Podozrivý odosielateľ
 - support@banko.sk namiesto @banka.sk
- 5 Pravopisné chyby
- 6 Prílohy (.exe, .zip)
- 7 Odkazy na podozrivé stránky

Príklad phishing e-mailu:

Od: support@paypal.com

Predmet: **NALIEHAVÉ: Váš účet bude zablokovaný!**

Dobrý deň,

Zistili sme podozrivú aktivitu na vašom účte. **Musíte okamžite overiť svoju identitu, inak bude účet do 24 hodín trvalo zablokovaný!**

Kliknite tu: <http://paypal-verify.com/urgent>

S pozdravom,
Tím PayPal

ČO JE PODOZRIVÉ?

- Nesprávna doména (paypal1 namiesto l)
- Naliehavosť a hrozba
- Podozrivý odkaz

Hrozba: Baiting (Návnada)

- 1 Útočník zanechá USB na parkovisku
- 2 Lákavé označenie: „Výplaty 2025“, „Dôverné“
- 3 Zvedavý zamestnanec ho nájde
- 4 Pripojí do firemného PC
- 5 Automatická inštalácia malvéru
- 6 Celá sieť kompromitovaná

Štatistika

45% ľudí pripojí nájdený USB do PC

NIKDY:

- Nepripájajte nájdené USB
- Nepoužívajte neznáme nabíjačky
- Nenechávajte PC/notebook odomknutý
- Nenechávajte zariadenia bez dozoru

VŽDY:

- Zamknite obrazovku (Win+L)
- Používajte káblové zámky na notebooky
- Nájdené USB odovzdajte IT
- Oznamte stratu prístupovej karty

Príklad

Stuxnet sa šíril práve cez USB klúče

Zálohovanie - Poistka na dáta

Pravidlo 3-2-1:

- 3 kópie dát
- Na 2 rôznych médiách
- 1 kópia off-site (mimo)

Prečo zálohovať:

- Ransomvér - zašifruje dáta
- Hardvérové zlyhanie
- Omylom vymazané súbory
- Požiar, povodeň, krádež

Príklad

Ransomvér útok - výkupné 50 000 €. Ale máte

Aktualizácie - Záplatovanie dier

Čo aktualizovať:

- Operačný systém (Windows, Mac, Linux)
- Prehliadače (Chrome, Firefox, Edge)
- Aplikácie (Adobe, Office, Java)
- Antivírus
- Firmware na routeri

Prečo aktualizovať:

- Opravujú bezpečnostné zraniteľnosti
- Útočníci zneužívajú staré verzie
- Jeden neopravený systém = vstupná brána

Kľúčová myšlienka

Zamestnanec, ktorý nahlási incident, je **HRDINA**, nie problém

Čo nahlásiť:

- Podozrivý e-mail (phishing)
- Kliknutie na škodlivý odkaz
- Stratená prístupová karta
- Stratený/ukradnutý notebook/telefón
- Neobvyklé správanie PC
- Podozrivá osoba v priestoroch
- Nájdený USB kľúč
- Únik dát (aj náhodný)

Ako nahlásiť:

- 1 **OKAMŽITE** - každá minúta sa ráta
- 2 IT helpdesk / bezpečnostný manažér
- 3 E-mail: security@firma.sk
- 4 Telefón: +421...
- 5 Osobne

Prečo nahlásiť:

- Útok sa môže zastaviť
- Škody sa minimalizujú
- Ostatní sú varovaní

- 1 **Každý je zodpovedný**
 - Nie len IT - všetci zamestnanci sú súčasťou obrany
- 2 **Zero Trust prístup**
 - Nikdy automaticky nedôverujte - vždy overujte
- 3 **Základy sú najdôležitejšie**
 - Silné heslá + MFA
 - Aktualizácie
 - Zálohovanie
- 4 **DNS a OT sú kritické**
 - DNS je „telefónny zoznam“ - ak je narušený, ste stratení
 - OT útoky môžu ohroziť životy
- 5 **Hlásenie je povinnosť**
 - Okamžite nahlásiť podozrivé aktivity
 - No-Blame Culture - chyby sa môžu stať

Útok cez telefónne predvoľby (Caller ID Spoofing)

Čo je to?

Útočník dokáže zmeniť číslo, ktoré sa vám zobrazí pri hovore - môže sa tváriť ako banka, polícia, alebo váš kolega.

Ako to funguje:



Scenár útoku:

- 1 Zavolá vám „banka“ (0800...)
- 2 „Detegovali sme podozrivú transakciu“
- 3 „Potrebujeme overiť vašu identitu“
- 4 Žiadajú PIN, CVV, heslo
- 5 Prípadne vás presmerujú na falošnú stránku

Ochrana

Banka/polícia NIKDY nežiada heslá, PIN alebo CVV. Ak voláte späť, použite číslo z oficiálnej stránky, nie z displeja telefónu!

Dakujem za pozornosť