NCC-SK
SLOVAKIA CYBERSECURITY COORDINATION CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Systémová, sieťová a komunikačná bezpečnosť

Marián Franko

16. september 2025

ZÁKON 69/2018 Z. Z. O KYBERNETICKEJ BEZPEČNOSTI

§ 19 Povinnosti prevádzkovateľa základnej služby

(1) Prevádzkovateľ základnej služby je povinný ... v závislosti od vykonanej analýzy rizík prijať, dodržiavať a vykonávať všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa § 20 a vykonávať ich s cieľom zabezpečovania kybernetickej bezpečnosti a odolnosti. ...

§ 20 Bezpečnostné opatrenia

(1) Bezpečnostnými opatreniami na účely tohto zákona sú úlohy, procesy, role a technológie v organizačnej, personálnej, fyzickej a technologickej oblasti, ktorých cieľom je dosiahnutie, zaručenie a udržanie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov a operačných technológií. ...

ČO HOVORÍ „KRÁSNA VEĽKÁ“ NOVÁ VYHLÁŠKA 227/2025

https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2025/227/

VYHLÁŠKA Č. 227/2025 Z. Z.

Vyhláška č. 227/2025 Z. z. Národného bezpečnostného úradu (NBÚ) **nadobudla účinnosť 1. septembra 2025** a nahradila predchádzajúcu vyhlášku č. 362/2018 Z. z.

Jej cieľom je upraviť :

- obsah a štruktúru bezpečnostnej dokumentácie
  - zahŕňa stratégiu, analýzu rizík, klasifikáciu informácií, topológiu infraštruktúry atď.
- obsah bezpečnostných opatrení
  - Konkrétne prvky/postupy/konfigurácie, ktoré opatrenia implementujú
    - Napríklad požiadavky na školenia, audity, klasifikáciu informácií, konkrétne technológie alebo procesy
- rozsah všeobecných bezpečnostných opatrení pre siete, informačné systémy a operačné technológie
  - Určuje do akej miery sa opatrenia musia zaviesť
    - veľkosti a významu organizácie, kategórie kybernetického priestoru (napr. základná služba, kritická infraštruktúra),
    - počtu a typu aktív, výsledkov analýzy rizík

ORGANIZAČNÉ BEZPEČNOSTNÉ OPATRENIA

Zamerané na riadenie, procesy, ľudí a dokumentáciu:

- **Bezpečnostná politika a stratégia** – dokumenty, ktoré určujú smerovanie a pravidlá.
- **Bezpečnostná dokumentácia** – všetky dokumenty, ktoré popisujú opatrenia a procesy.
- **Určenie manažéra kybernetickej bezpečnosti** – zodpovedná osoba za koordináciu.
- **Klasifikácia informácií** – určenie citlivosti a spôsobu spracovania údajov.
- **Riadenie kybernetických rizík a hrozieb** – procesy na identifikáciu, hodnotenie a riadenie rizík.
- **Organizačná štruktúra a rozdelenie rolí** – určenie zodpovedností a právomocí.
- **Vzdelávanie a budovanie povedomia** – školenia, kampane, testovanie zamestnancov.
- **Riadenie dodávateľských vzťahov** – zmluvné zabezpečenie kybernetickej bezpečnosti.
- **Audit a kontrolné činnosti** – interné a externé preverovanie dodržiavania opatrení.

TECHNICKÉ BEZPEČNOSTNÉ OPATRENIA

Zamerané na technológie, systémy a infraštruktúru:

- **Bezpečnosť siete a komunikačných systémov** - Ochrana pred neoprávneným prístupom, útokmi a narušením komunikácie.
- **Ochrana proti škodlivému kódu a nežiaducemu obsahu** - Detekcia a blokovanie vírusov, malvéru, ransomvéru a škodlivých webov.
- **Systémová bezpečnosť a konfigurácia** - Bezpečné nastavenie operačných systémov, aplikácií a služieb.
- **Zálohovanie a obnova po havárii** - Pravidelné zálohovanie dát a plán obnovy systémov po výpadku alebo incidente.
- **Monitorovanie, zaznamenávanie a hlásenie udalostí** - Zber logov, sledovanie aktivít a automatické hlásenie podozrivých udalostí.
- **Kryptografické opatrenia** - Šifrovanie dát, komunikácie a autentifikácie.
- **Bezpečnosť koncových zariadení** - Ochrana počítačov, mobilov a IoT zariadení pred kompromitáciou.
- **Bezpečnosť pri vývoji, údržbe a prevádzke IKT systémov** - Bezpečnostné princípy pri vývoji softvéru, testovanie a správa zraniteľností.
- **Detekcia a riešenie kybernetických incidentov** - Identifikácia, analýza a reakcia na bezpečnostné incidenty.
- **Používanie certifikovaných produktov IKT** - Využívanie technológií, ktoré spĺňajú bezpečnostné normy a certifikácie.

KOMBINOVANÉ (TECHNICKO-ORGANIZAČNÉ) OPATRENIA

Kombinované opatrenia zahŕňajú technické aj organizačné prvky. Inými slovami, ich účinné zavedenie si vyžaduje technologické riešenia a procesné a riadiace pravidlá

- **Riadenie prístupov**
  - Technické: autentifikačné systémy, správa hesiel, viacfaktorová autentifikácia.
  - Organizačné: pravidlá prideľovania oprávnení, revízia prístupov, školenia.
- **Incident management** – technické detekčné nástroje + organizačné postupy riešenia.
  - Technické: detekčné nástroje, SIEM systémy, logovanie.
  - Organizačné: postupy hlásenia, tímová koordinácia, dokumentácia incidentov.
- **Kontinuita činností a obnova po havárii** – technické zálohovanie + organizačné plány obnovy.
  - Technické: zálohovacie systémy, redundancia, obnova dát.
  - Organizačné: plán obnovy, testovanie scenárov, zodpovednosti.
- **Správa identít** – technické systémy + pravidlá prideľovania oprávnení.
  - Technické: identity management systémy, LDAP, SSO.
  - Organizačné: pravidlá prideľovania identít, kontrola životného cyklu používateľa.

BEZPEČNOSŤ SIETE A KOMUNIKAČNÝCH SYSTÉMOV

Bezpečnosť siete a komunikačných systémov je jedným z kľúčových technických opatrení podľa vyhlášky č. 227/2025 Z. z. o kybernetickej bezpečnosti. Jej cieľom je zabezpečiť, aby sieťová infraštruktúra a komunikačné kanály boli chránené pred neoprávneným prístupom, manipuláciou, odpočúvaním a narušením dostupnosti.

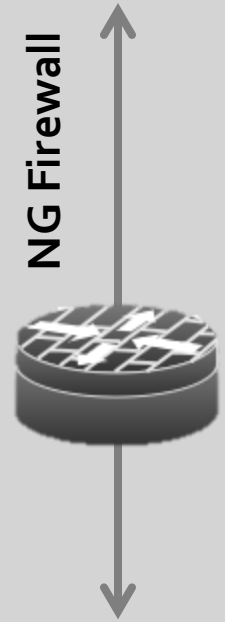
Hlavné oblasti bezpečnosti siete a komunikácie

1. **Ochrana perimetra**
   - Použitie firewallov, proxy serverov, IDS/IPS systémov na kontrolu a filtrovanie sieťovej prevádzky.
   - Oddelenie interných sietí od externých (napr. DMZ zóna).
2. **Segmentácia siete**
   - Rozdelenie siete na logické časti (napr. VLAN), aby sa obmedzil pohyb útočníka v prípade kompromitácie.
3. **Bezpečná komunikácia**
   - Šifrovanie dát pri prenose (napr. TLS, VPN, IPsec).
   - Ochrana proti Man-in-the-Middle útokom.
4. **Riadenie prístupu do siete**
   - Autentifikácia používateľov a zariadení (napr. 802.1X, MAC filtering).
   - Monitoring pripojených zariadení.
5. **Monitoring a detekcia**
   - Sledovanie sieťovej prevádzky na identifikáciu anomálií.
   - Využitie SIEM systémov na koreláciu udalostí.
6. **Kontinuita - Ochrana dostupnosti služby**
   - Zabezpečenie systémov, aplikácií a služieb aby boli nepretržite dostupné pre oprávnených používateľov – aj v prípade technických porúch, kybernetických útokov alebo iných incidentov.

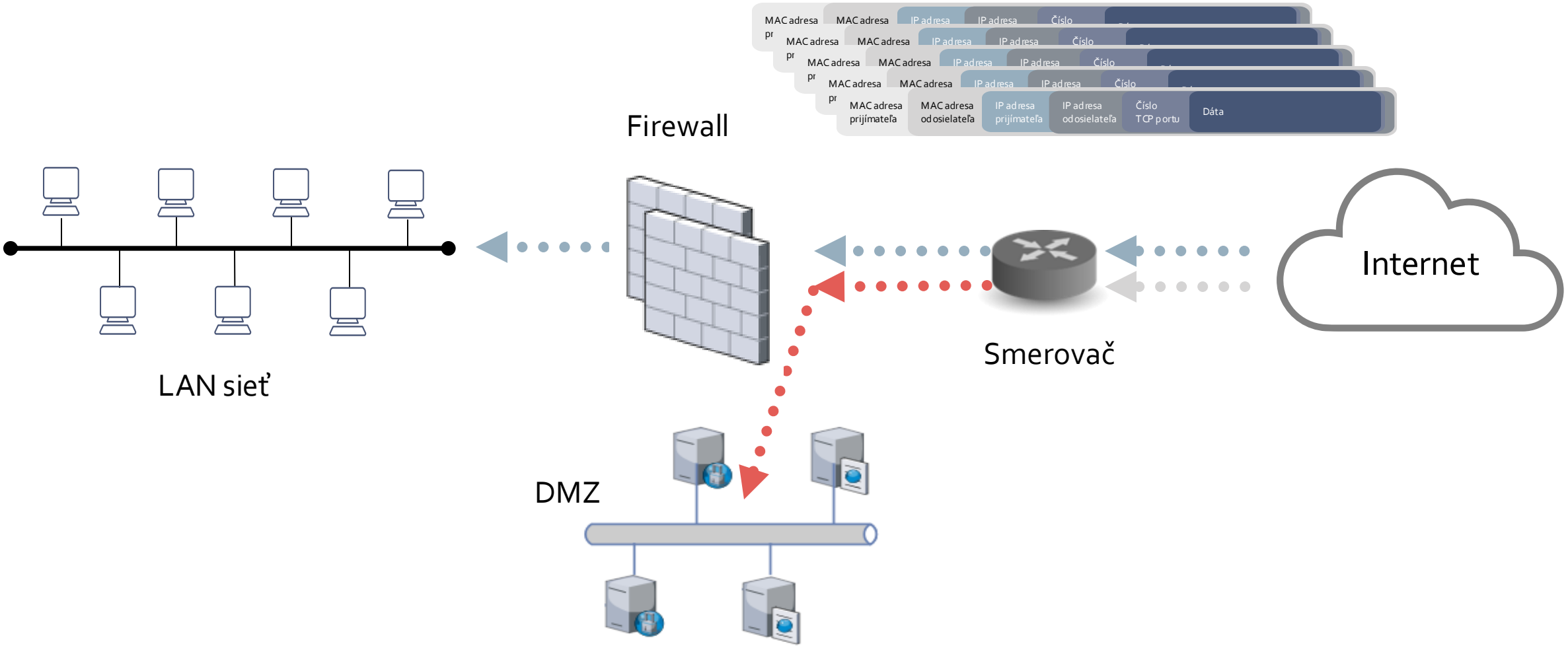
MODEL ISO/OSI

	TCP /IP		ISO OSI	Popis vrstvy	
Vrchné vrstvy	4	Aplikačná	7	**Aplikačná vrstva** formát správ, rozhranie človek - stroj	
			6	**Prezentačná vrstva** kódovanie, šifrovanie, kompresia	
			5	**Relačná vrstva** Autentizácia, prideľovanie práv, registrácia relácie	
Spodné vrstvy	3	Transportná	4	**Transportná vrstva** Ošetrovanie chýb	Segmenty
	2	Internetová	3	**Sieťová vrstva** Adresovanie v sieti: smerovanie alebo prepínanie paketov	Pakety
	1	Sieťová	2	**Dátová vrstva** Detegovanie chýb, riadenie toku vo fyzickom spojení	Rámce
			1	**Fyzická vrstva** Prúd bitov, fyzické médium, metódy reprezentácie bitov	Bity

SIEŤOVÉ ZARIADENIA

4	**Aplikačná vrstva (L7)** Rozhranie pre používateľa a aplikácie (HTTP, FTP, SMTP, DNS)	▪ Funkciou je sprostredkovávať a poskytovať služby aplikáciám a rozhranie pre používateľov		
3	**Sieťová vrstva (L3)** Adresovanie v sieti: smerovanie alebo prepínanie paketov	Pakety ▪ Sieťový smerovač (router) ▪ Prepája viaceré segmenty alebo viaceré siete ▪ Riadi prenos medzi segmentami siete podľa IP adries		
2	**Dátová vrstva (L2)** Detegovanie chýb, riadenie toku vo fyzickom spojení, prepínanie rámcov	Rámce ▪ Sieťový prepínač L2 (switch) ▪ Multiportový most (multiport bridge) ▪ Zvyšuje výkon siete znížením počtu prenášaných rámcov (mikrosegmentácia) ▪ Filtruje prenos medzi segmentami siete podľa cieľovej MAC adresy		
1	**Fyzická vrstva (L1)** Prúd bitov, fyzické médium, metódy reprezentácie bitov	Bity ▪ Metalické vedenie ▪ Optické vedenie ▪ Prenos vzduchom (WiFi)		

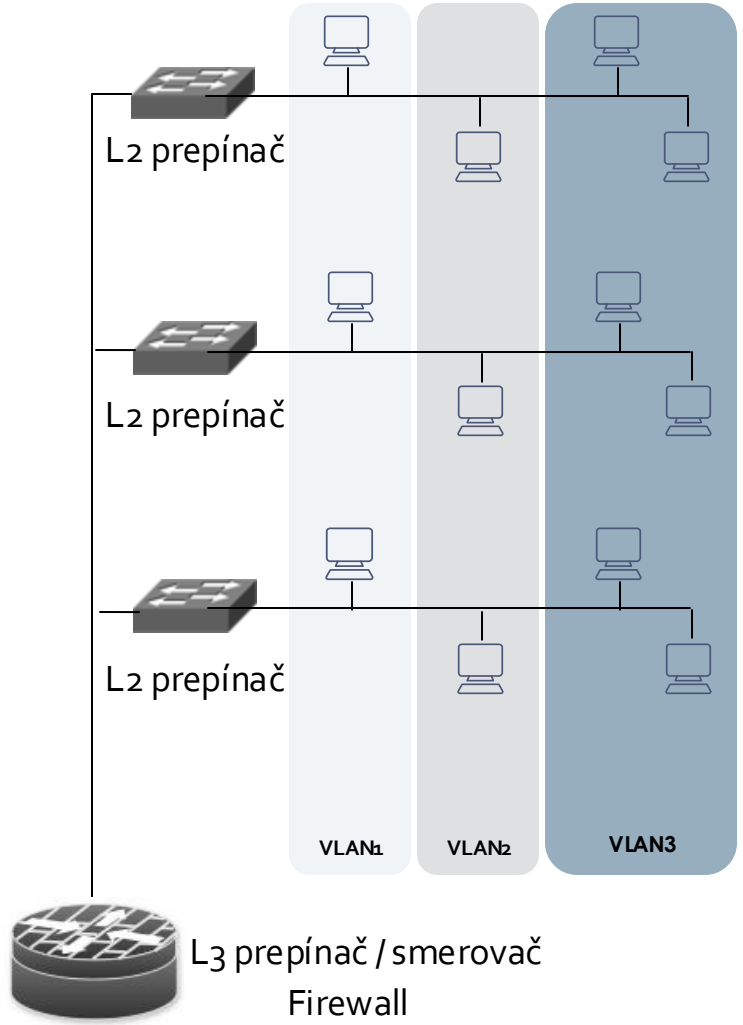
OCHRANA PERIMETRA



SEGMENTÁCIA SIETÍ

Rozdelenie počítačovej siete na menšie, izolované časti (segmenty) s cieľom zvýšiť bezpečnosť a efektivitu prevádzky.

- Hlavné prínosy segmentácie:
  - Obmedzenie šírenia útokov: Útočník sa po kompromitovaní jednej časti siete nedostane jednoducho do ďalších segmentov.
  - Lepšia kontrola prístupov: Prístup medzi segmentmi je riadený firewallmi, ACL alebo inými bezpečnostnými politikami.
  - Zvýšená prehľadnosť a správa: Jednoduchšie monitorovanie a správa prevádzky v menších častiach siete.
  - Zvýšená odolnosť voči ransomvéru a laterálnemu pohybu útočníka.
- Typy segmentácie:
  - Fyzická segmentácia: Oddelené káblovanie, samostatné prepínače a smerovače.
  - Logická segmentácia: VLAN (Virtual LAN), subnety, mikrosegmentácia (napr. pomocou SDN).



BEZPEČNÁ KOMUNIKÁCIA

Bezpečná komunikácia v kybernetickej bezpečnosti sa týka ochrany dát počas ich prenosu medzi systémami, zariadeniami alebo používateľmi. Jej cieľom je zabezpečiť dôvernosť, integritu a dostupnosť prenášaných informácií.

1. **Dôvernosť (Confidentiality)**
   - Zabezpečuje, že prenášané dáta sú prístupné len oprávneným stranám.
   - Používa sa šifrovanie (napr. TLS, VPN, IPsec).
2. **Integrita (Integrity)**
   - Zaručuje, že dáta neboli počas prenosu zmenené alebo poškodené.
   - Používajú sa digitálne podpisy, hashovacie algoritmy (napr. SHA-256).
3. **Autentifikácia (Authentication)**
   - Overuje identitu komunikujúcich strán.
   - Príklady: certifikáty, heslá, viacfaktorová autentifikácia.
4. **Nepopierateľnosť (Non-repudiation)**
   - Zaisťuje, že odosielateľ nemôže poprieť, že správu poslal.
   - Používajú sa digitálne podpisy a časové pečiatky.

Technológia	Účel
TLS/SSL	Šifrovanie webovej komunikácie (napr. HTTPS)
VPN	Zabezpečený tunel medzi vzdialenými systémami
IPsec	Šifrovanie na úrovni IP protokolu (L3/L4)
S/MIME PGP/GPG	Šifrovanie a podpisovanie e-mailov
802.1AE (MACsec)	Šifrovanie na úrovni Ethernetu (L2)

RIADENIE PRÍSTUPU DO SIETE

preventívne

Cieľ opatrenia

- Zabrániť neoprávnenému prístupu, zneužitiu systémov a dát, a obmedziť pohyb útočníka v prípade kompromitácie.

Hlavné prvky riadenia prístupu:

1. **Autentifikácia**
   - Overenie identity používateľa alebo zariadenia.
   - Príklady: heslá, biometria, MFA (multi-faktorová autentifikácia).
2. **Autorizácia**
   - Určenie, k čomu má používateľ prístup (napr. súbory, aplikácie, servery).
   - Pravidlá založené na rolách (RBAC), atribútoch (ABAC) alebo politikách.
3. **Správa prístupových práv**
   - Prideľovanie, zmena a odoberanie oprávnení.
   - Pravidelná revízia prístupov (napr. pri zmene pozície alebo odchode zamestnanca).
4. **Sieťová kontrola prístupu**
   - Technológie ako 802.1X, NAC (Network Access Control).
   - Povolenie prístupu len pre dôveryhodné zariadenia.
5. **Záznamy a monitoring**
   - Logovanie prístupov, pokusov o prístup, zmeny oprávnení.
   - Detekcia podozrivých aktivít.

MONITOROVANIE A DETEKCIA

Cieľ opatrenia je zabezpečiť nepretržité sledovanie systémov a infraštruktúry, identifikovať podozrivé správanie, zaznamenať udalosti, reagovať na incidenty, podporiť forenznú analýzu.

Hlavné komponenty monitorovania a detekcie

1. **Zber logov a udalostí**
   - Zaznamenávanie aktivít používateľov, systémov, aplikácií a sietí.
   - Príklady: prihlasovanie, zmeny konfigurácie, prístup k citlivým dátam.
2. **Centralizované logovanie**
   - Zbieranie logov z rôznych zdrojov do jedného systému (napr. Syslog, ELK stack, Graylog).
3. **SIEM systémy (Security Information and Event Management)**
   - Kombinujú zber, koreláciu a analýzu bezpečnostných udalostí.
   - Príklady: Splunk, IBM QRadar, Microsoft Sentinel, ArcSight.
4. **Detekčné mechanizmy**
   - IDS/IPS (Intrusion Detection/Prevention Systems) – detekcia a blokovanie útokov.
   - Behaviorálna analýza – identifikácia anomálií oproti bežnému správaniu.
5. **Alertovanie a reakcia**
   - Automatické upozornenia pri výskyte podozrivých udalostí.
   - Integrácia s incident management systémami.
6. **Forenzná analýza**
   - Uchovávanie logov pre spätné vyšetrenie incidentov.
   - Podpora právnych a auditných procesov.

KONTINUITA - OCHRANA DOSTUPNOSTI SLUŽBY

Cieľ opatrenia je zabezpečiť, že služby fungujú spoľahlivo a stabilne, sú dostupné v požadovanom čase a dajú sa po výpadku rýchlo obnoviť.

Kľúčové prvky ochrany dostupnosti

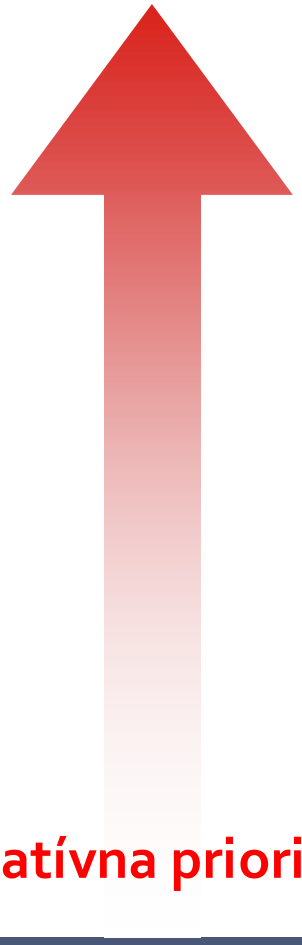
1. **Redundancia**
   - Duplikácia kritických komponentov (napr. servery, sieťové prvky).
   - Použitie HA (High Availability) architektúr.
2. **Zálohovanie a obnova**
   - Pravidelné zálohovanie dát a konfigurácií.
   - Plán obnovy po havárii (Disaster Recovery Plan).
3. **Monitoring dostupnosti**
   - Sledovanie stavu služieb v reálnom čase.
   - Automatické upozornenia pri výpadku.
4. **Ochrana proti DoS/DDoS útokom**
   - Filtrovanie škodlivej prevádzky.
   - Využitie cloudových DDoS ochranných služieb.
5. **Rozdelenie záťaže - Load balancing**
   - Rozdelenie záťaže medzi viaceré servery.
   - Zvyšuje výkon a odolnosť voči výpadkom.
6. **Plán kontinuity činností (BCP)**
   - Postupy na zachovanie prevádzky počas krízových situácií.
   - Zahŕňa aj náhradné pracoviská, komunikáciu a koordináciu tímov.

ROZDIELNY PRÍSTUP IT A OT SVETA

Kategória	IT	OT / IACS
Účel	Uskutočnenie transakcií, poskytovanie informácií	Riadenie alebo monitoring fyzických procesov a zariadení
Architektúra	Široká korporátna infraštruktúra a aplikácie	Udalosťami riadený, bežiaci v reálnom čase, proprietárny HW a SW
Rozhrania	GUI, Web browser, terminál a klávesnica	Elektromechanické komponenty, senzory, ovládacie prvky, displeje, ručné prenosné ovládacie terminály
Vlastníctvo	CIO a IT	Priemyselní pracovníci, technici, operátori a manažéri výroby
Konektivita	Korporátna sieť, IP-based	Priemyselné siete, priemyselné krútené káble, koaxiálne káble a IP-based
Rola	Podpora ľudských činností	Ovládanie a riadenie strojov
Odozva	Čo najskôr	V reálnom čase
Dostupnosť/stabilita systémov	Akceptovateľné či žiadúce reštarty	Neakceptovateľné
Dôležité parametre pre risk manažment	• Ochrana dát / informácií • Priorita je dôvernosť a integrita	• Riadenie fyzických procesov • Ochrana života a zdravia
Zmenové konanie	Časté a pravidelné aplikovanie nových vydaní SW	Aplikovanie nových SW vydaní iba po robustnom testovaní
Komunikácia	Štandardné komunikačné protokoly	Proprietárne protokoly ICS systémov a niektoré štandardné
Životnosť komponentov	3 až 5 rokov	10 až 15 rokov

ODLIŠNÉ PRIORITY BEZPEČNOSTI V OT A IT

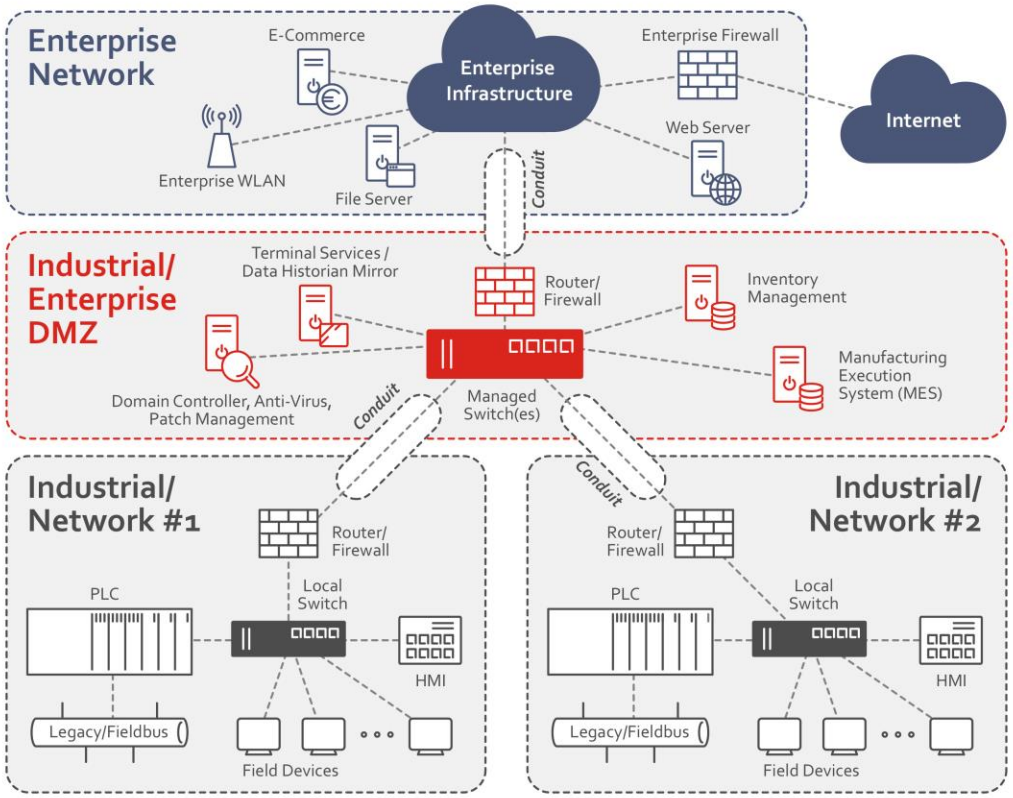
Priemyselné systémy OT/IACS	Informačné technológie IT
Availability	**C**onfidentiality
Integrity	**I**ntegrity
Confidentiality	**A**vailability



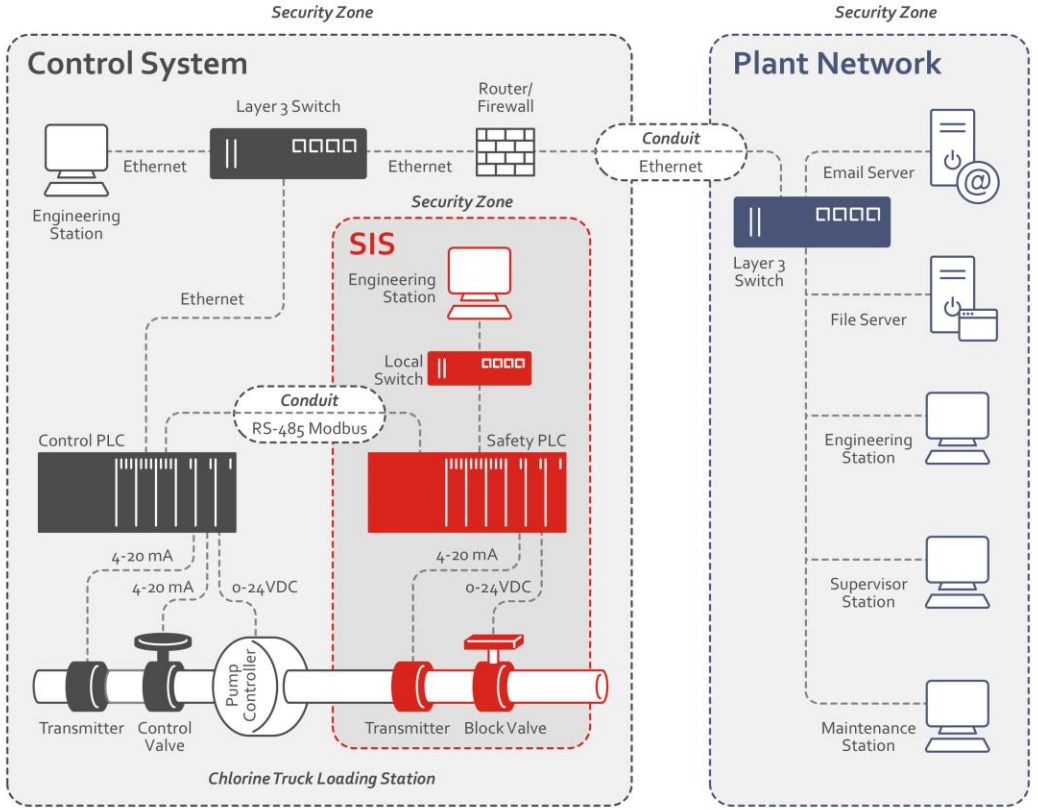
Relatívna priorita

SEGMENTÁCIA OT PROSTREDIA

preventívne
detekčné



© 2009 National Institute of Standards & Technology (NIST)

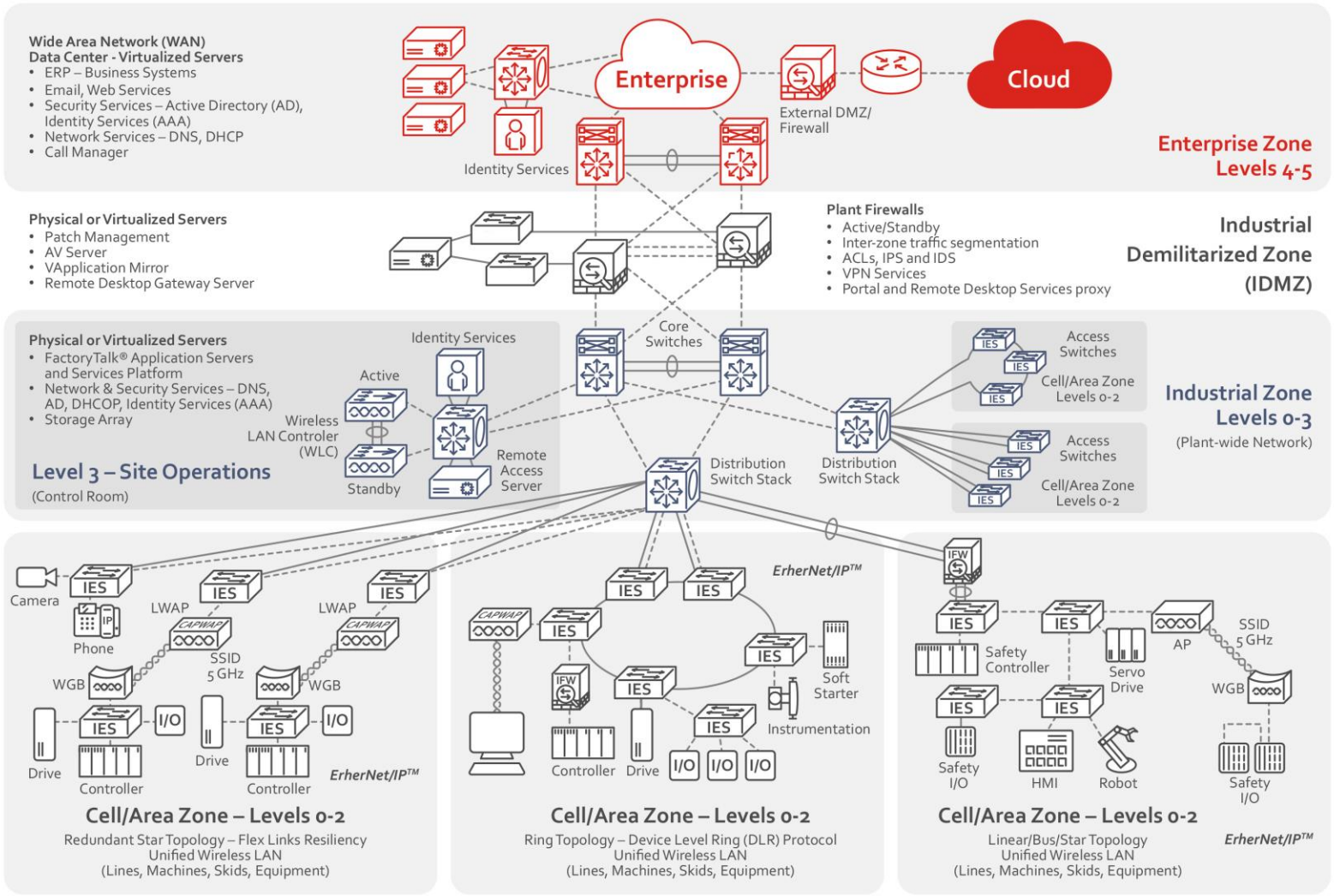


- Rovnako kritické, ako pre IT tak aj pre OT, je oddelenie segmentov siete s podobnou povahou a teda úrovňou zabezpečenia
- Pre OT prostredie sa už pri úvodnej analýze zraniteľností identifikujú tzv. „Zones" a prepojenia medzi nimi tzv. „Conduits"
- Pre všetky takéto prvky sú stanovené cieľové úrovne zabezpečenia tzv. Security Levels (SL-T)

SIEŤOVÝ REFERENČNÝ MODEL OT

- **Level 4** – Enterprise Systems (business plánovanie, logistika)
- **Level 3** – Operations Management (riadenie procesov výroby)
- **Level 2** – Supervisory Control (procesy monitorovania a ovládania fyzických procesov)
- **Level 1** – Local or Basic Control (riadenia a ovládanie lokálnych fyzických procesov)
- **Level 0** – Process (fyzický proces, snímače, ovládače)

V prílohe 1 vyhlášky 227/2025 je „Level" Označený výrazom „Vrstva".



Obr.: Cisco Systems

ZÁVER

- Ďakujeme za Váš čas
- Nasledujúci webinár na tému „ Obstarávanie, vývoj a údržba sietí, informačných systémov a aplikácií.“ 21.10.2025



NCC-SK

SLOVAKIA CYBERSECURITY COORDINATION CENTRE



Financované Európskou úniou

Vyjadrené názory a postoje sú názormi a vyhláseniami autorov a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za nich nepreberajú žiadnu zodpovednosť.

Ochrana vlastníckych práv

Všetky autorské práva k tomuto dokumentu sú vyhradené pre Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (ďalej len „KCCKB“). Autorské práva k tomuto dokumentu má a autorské práva k tomuto dokumentu vykonáva KCCKB.

Vlastnícke práva tretích strán

Všetky ochranné známky a iné obdobné právne chránené označenia spomenuté v tomto dokumente sú výhradným vlastníctvom ich vlastníkov, ktorí sú, pokiaľ sa nejedná o KCCKB, v dokumente označení vo forme príslušnej citácie.

Akékoľvek kopírovanie či iné neoprávnené použitie celého dokumentu alebo jeho časti, v elektronickej alebo listinnej podobe, bez predchádzajúceho písomného súhlasu jeho autorov, napr. KCCKB, je zakázané. Porušenie vlastníckych a iných súvisiacich práv bude riešené v zmysle právnych predpisov Slovenskej republiky.

Limity informácií

Informácie obsiahnuté v tomto dokumente sú poskytované iba na informačné účely a bez akejkoľvek záruky, výslovnej či implicitnej. Názov KCCKB, logo KCCKB a ďalšie produkty a služby KCCKB sú ochrannými známkami KCCKB. Ostatné názvy spoločností, produktov alebo služieb môžu byť ochrannými známkami, alebo značkami služieb iných organizácií.