„NIS2 – BEZPEČNOSTNÍ NÁSTROJE“

Ing. Ondřej Salák

NGSS

Technická opatření

- Technické (spíše však technicko-organizační) požadavky z **návrhu** vyhlášky k novému **ZoKB** /NIS2 (Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu **vyšších povinností**).
- Požadavky na nástroje – vyjádřeny explicitně (**N**), nebo jsou odvozené
- Rozdělení dle oblastí dle vyhlášky

- Bezpečnost komunikačních sítí (§ 19) **N**
- Správa a ověřování identit (§ 20) **N**
- Řízení přístupových oprávnění (§ 21) **N**
- Detekce kybernetických bezpečnostních událostí (§ 22) **N**
- Zaznamenávání událostí (§ 23) **N**
- Vyhodnocování kybernetických bezpečnostních událostí (§ 24) **N**

- Aplikační bezpečnost (§ 25)
- Kryptografické algoritmy (§ 26)
- Zajištění dostupnosti regulované služby(§ 27)
- Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv (§ 28)

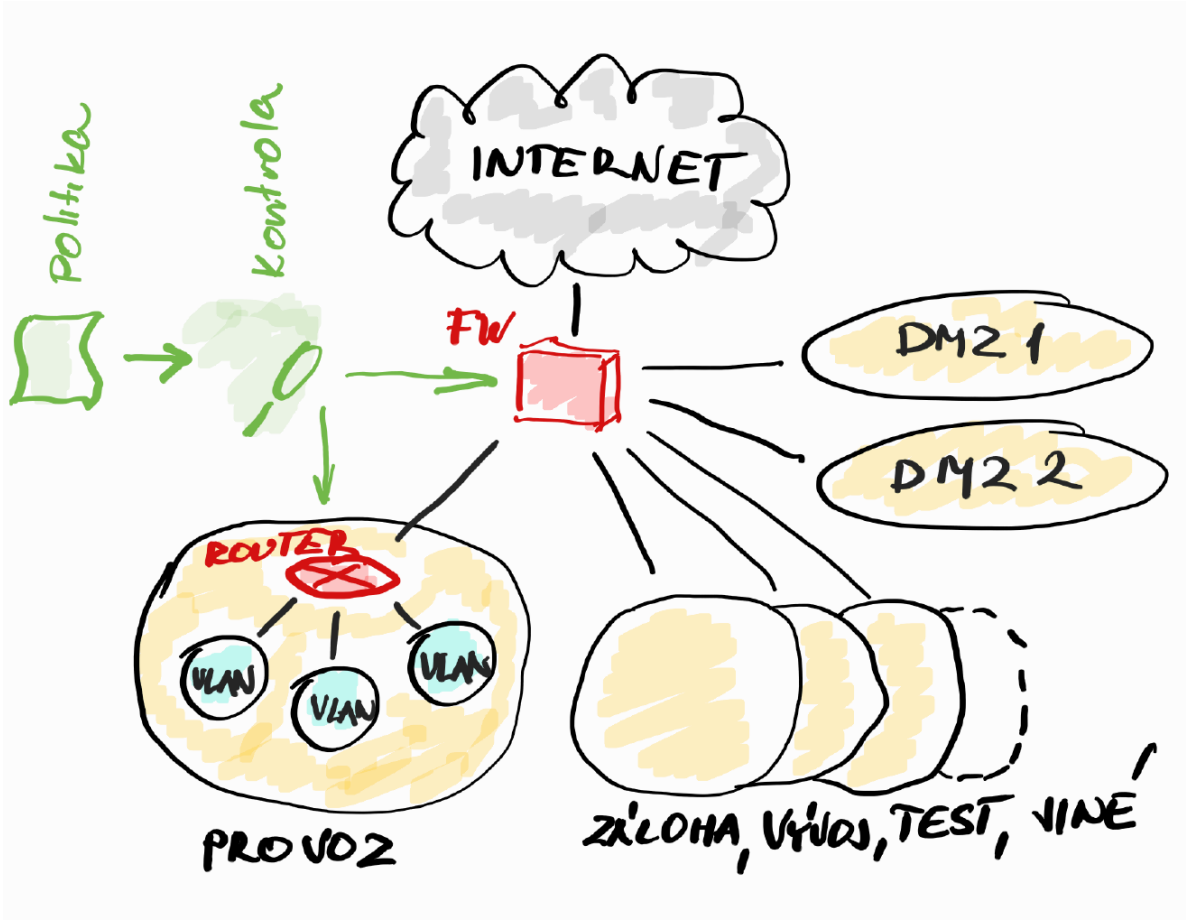
Bezpečnost komunikačních sítí (§ 19)

- **Segmentace** komunikační sítě
- **Řízení komunikace** (mezi sítěmi, VLAN, DMZ,…) a omezení na nezbytný provoz (filtry)
- **Oddělení prostředí** (podukce, vývoj, test, zálohy, další)

  Na síťové úrovni (např. VLAN) nebo vyšších vrstvách modelu OSI (např. middleware)
- **Řízení vzdáleného přístupu** a vzdálené správy
- **Nástroj** na zajištění integrity komunikační sítě – rozumíme topologie/architektura, switche, routery, FW

Bezpečnost komunikačních sítí (§ 19)

- **Segmentace sítí, řízení provozu a oddělení prostředí**

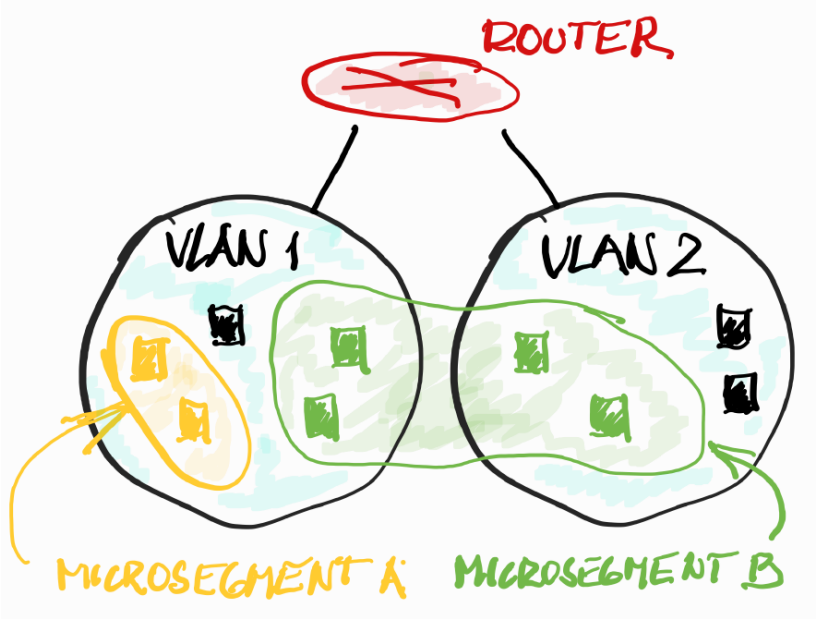


Bezpečnost komunikačních sítí (§ 19)

Mikrosegmentace

- Není to explicitní požadavek
- V souladu se **Zero Trust** principem
- SW based
- Odstranění rizika tzv. lateral movement
- Zvýšené nároky na správu (klasifikace, detailní znalosti,…)

- Př. OMG DDS (Data Distribution Standard) -> RTI Connext

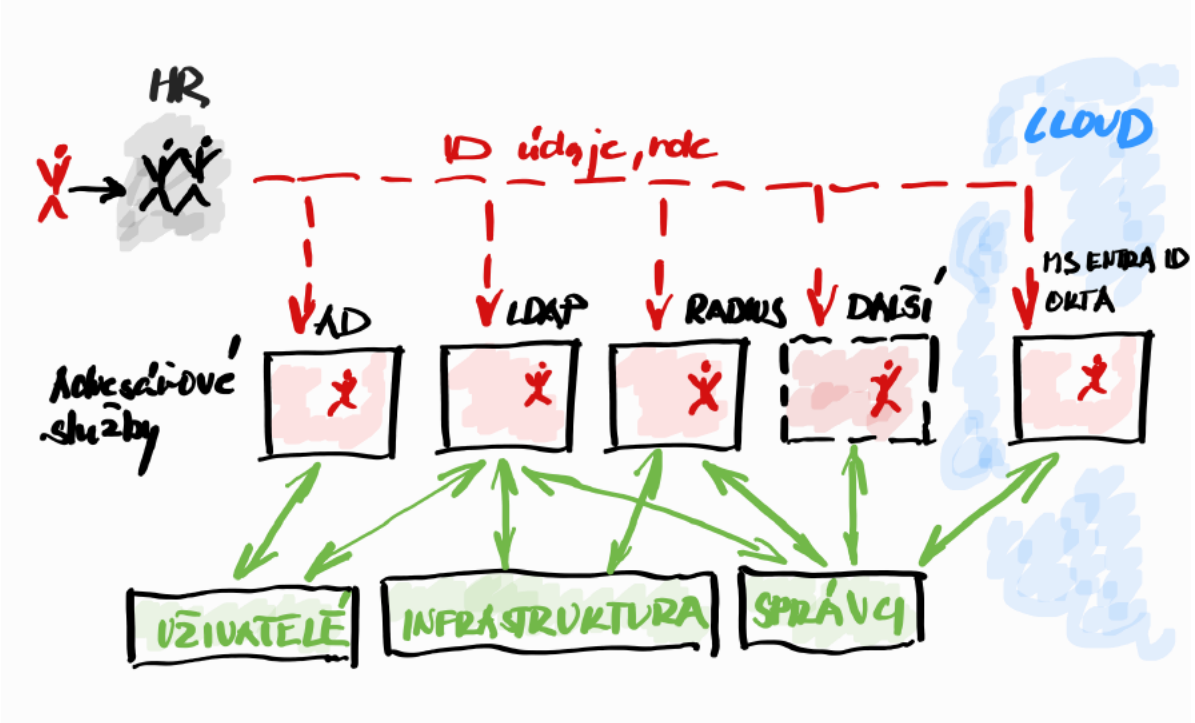


Správa a ověřování identit (§ 20)

- **Nástroj** pro správu a ověření identity (admina, uživatele technického aktiva) – adresářové služby, např. MS AD, RADIUS, OpenLDAP, apod.
  - Ověření identity
  - Řízení počtu neúspěšných pokusů o přihlášení
  - Zabezpečení údajů
  - Znovu ověření po nečinnosti
  - Bezpečné předání výchozích údajů (náhodné,hned změna, zneplatnění po 24 hod)
  - Centralizovaná správa
- **MFA** jako základ
  - Jinak evidence výjimky a **klíče/certifikáty**
    - Jinak v nástroji **ID a heslo**

Správa a ověřování identit (§ 20)

- Identity management a adresářové služby – příklad



Řízení přístupových oprávnění (§ 21)

- Centralizovaný **nástroj**

  často funkčně spojeno se Správou a ověřováním identit

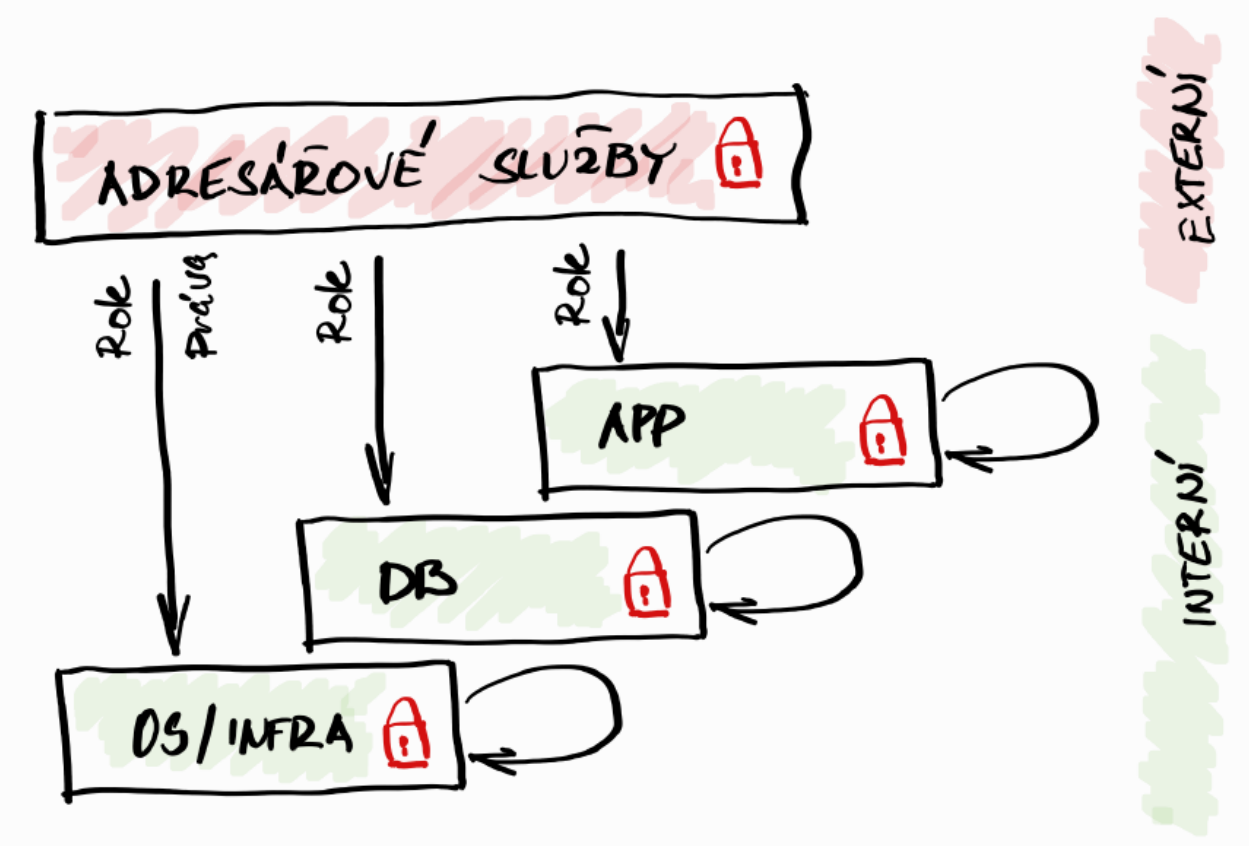
  např. adresářové služby
- Řízení oprávnění pro přístup

  pomocí **centrálního nástroje** nebo nastavením „interního nástroje“ v **aplikaci/DB/OS zařízení**
- Řízení typů přístupu (práva RO, RW, změna oprávnění)

  zajišťuje příslušný nástroj

Řízení přístupových oprávnění (§ 21)

- Lokalizace uložení přístupových oprávnění

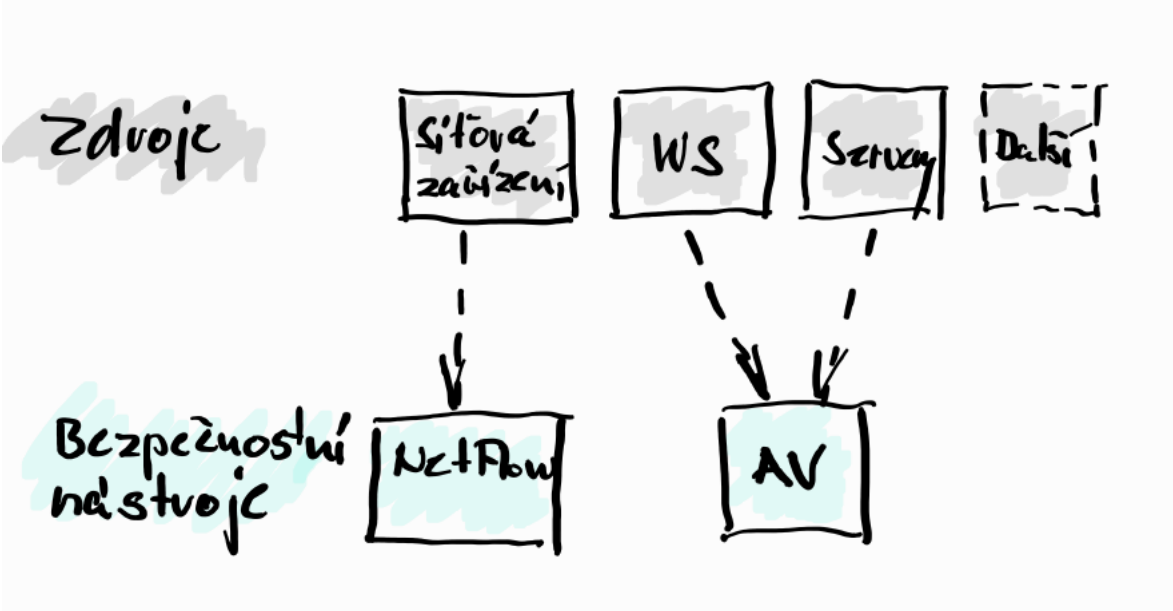


Detekce kybernetických bezpečnostních událostí (§ 22)

- **Nástroj(e)** pro detekci kybernetických bezpečnostních událostí
  - Ochrana před **škodlivým kódem** (Antimalware, Endpoint protection,…)
  - Řízení a sledování **výměnných zařízení**
  - Řízení automatického spouštění obsahu (např. politikou v AD)
  - Řízení oprávnění ke spouštění kódu (práva v adresářových službách,…)
  - Řízení a sledování **komunikace** (Netflow, DLP, IDS/IPS, FW, …)
  - Detekce **událostí nad technickými aktivy** (obecně specifikace rizikových událostí a logování)
  - Detekce na základě chování (nástroje typu behaviour analysis)

Detekce kybernetických bezpečnostních událostí (§ 22)

- **Nástroj(e)** pro detekci kybernetických bezpečnostních událostí



Zaznamenávání událostí (logování - § 23)

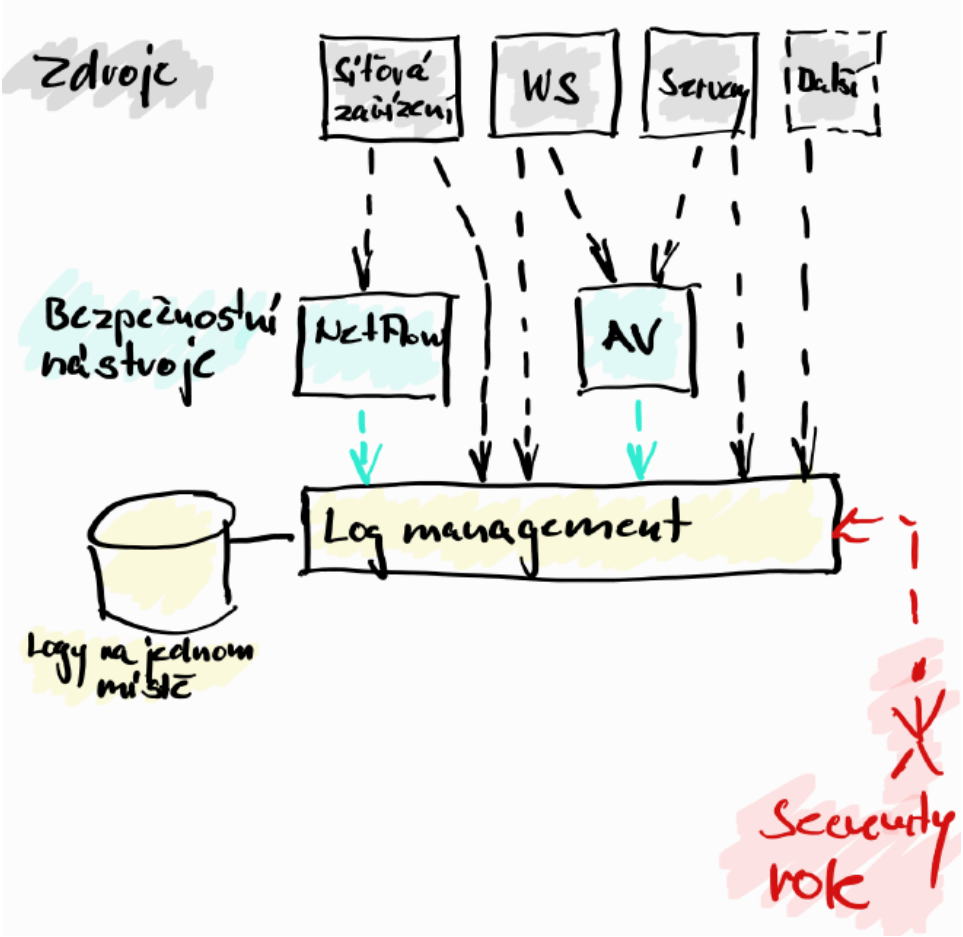
- **Nástroj** na zaznamenávání událostí (log management)
- Definovat **rozsah** logovaných aktiv
- **Obsah** logované informace
  - Datum a čas
  - Typ činnosti
  - Kdo zaznamenal
  - Účet spojený s aktivitou
  - ID zařízení (nutná jednoznačná identifikace)
  - Úspěch/neúspěch
- **Synchronizace** času

Zaznamenávání událostí (logování - § 23)

- Požadované **typy** logovaných informací (minimálně)
  - Přihlašování/odhlašování
  - Privilegované činnosti (i neúspěšný pokus)
  - Manipulace s oprávněními (i neúspěšný pokus)
  - Zahájení/ukončení činnosti technických aktiv
  - Kritická chybová hlášení technických aktiv
  - Přístup k záznamům událostí a pokus o změnu
  - Další činnosti – plyne např. z analýzy rizik
- Uchovat záznamy min. **18 měsíců**

Zaznamenávání událostí (logování - § 23)

- **Log management**

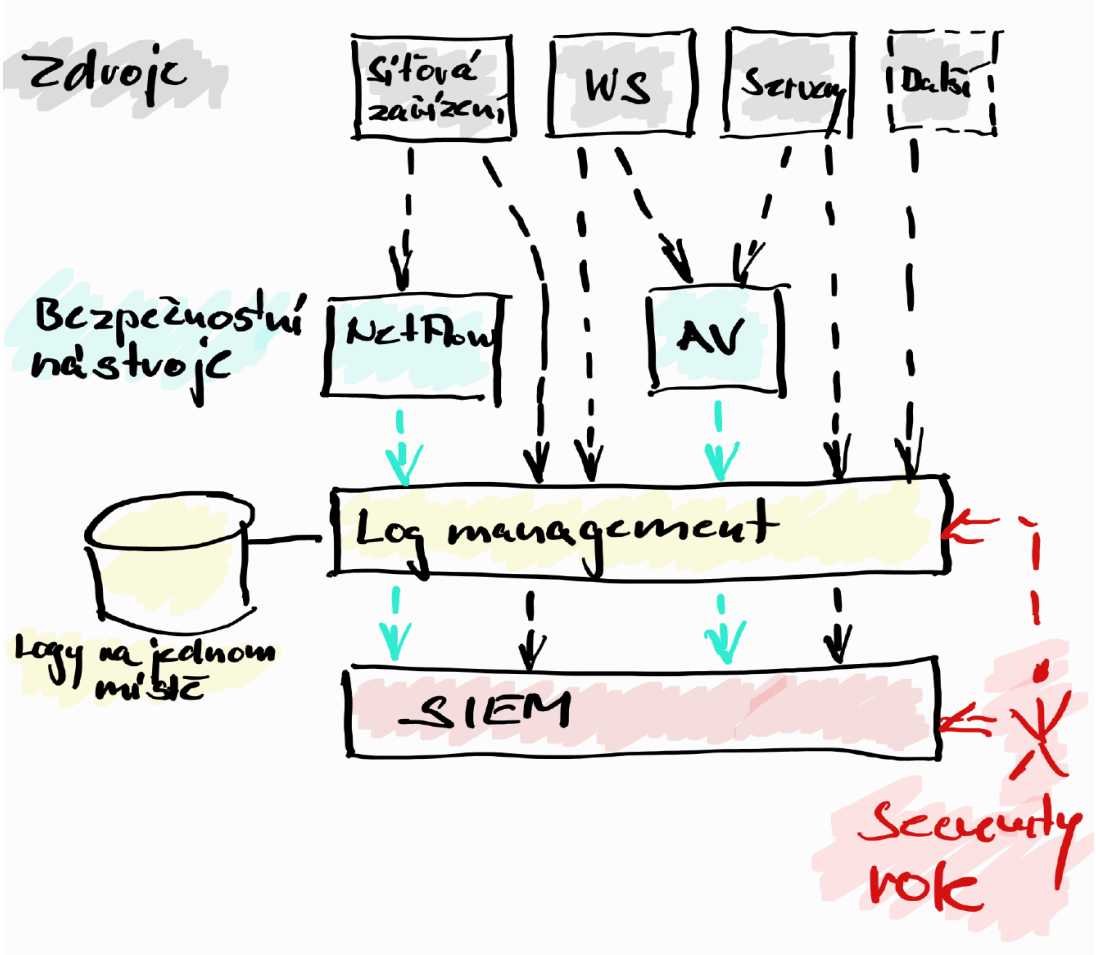


Vyhodnocování kybernetických bezpečnostních událostí (SIEM - § 24)

- **Nástroj** pro vyhodnocování kybernetických bezpečnostních událostí
  - SIEM (Security Information and Event Management)
  - Schopnost kombinovat informace z více zdrojů (např. uživatel neprošel vstupním turniketem, ale přihlásil se na počítači v objektu, apod.)
- **Aktualizovat** nastavení nástroje, užitých pravidel a alertingu
  - (**nekonečný proces**, nastavení musí odpovídat měnícím se potřebám)

Detekce, zaznamenávání a vyhodnocování událostí (§ 22, 23, 24)

- Log management, SIEM



Aplikační bezpečnost (§ 25)

- Používat pouze podporovaná technická aktiva a všechny aktualizace – jinak **Evidence** a **Bezpečnostní opatření**
- Pravidelné **skenování zranitelností** min. 1x/rok (z interní a externí sítě),

  Následně zhodnocení rizik a opatření
- **Penetrační testování** dle rizik min. 1x/2 roky
  - Před uvedením do provozu
  - Při významné změně

  Následně hodnocení rizik, opatření a **retest**

Kryptografické algoritmy, klíče a certifikáty (§ 26)

- **Aktuálně odolné** – viz např. doporučení NÚKIB
- Kryptografické klíče – **management klíčů a certifikátů** (bezpečnost)
  - Generování
  - Distribuce
  - Ukládání
  - Změny
  - Omezení platnosti
  - Zneplatnění
  - Likvidace

Zajištění dostupnosti regulované služby (§ 27)

- Dostupnost dle **stanovených cílů**
- Odolnost proti hrozbám, které mohou snížit dostupnost
- **Redundance** aktiv
  - Sítě (redundantní prvky a připojení, virtualizace)
  - Výpočetní výkon (virtualizace a HA/Standby, clustery)
  - Datová úložiště (disky, RAID, disková pole, virtualizace)
- **Zálohování**
  - **Testování** vč. dokumentování
  - Ochrana záloh (CIA)
  - Oddělení zálohovacího prostředí

Architekt kybernetické bezpečnosti

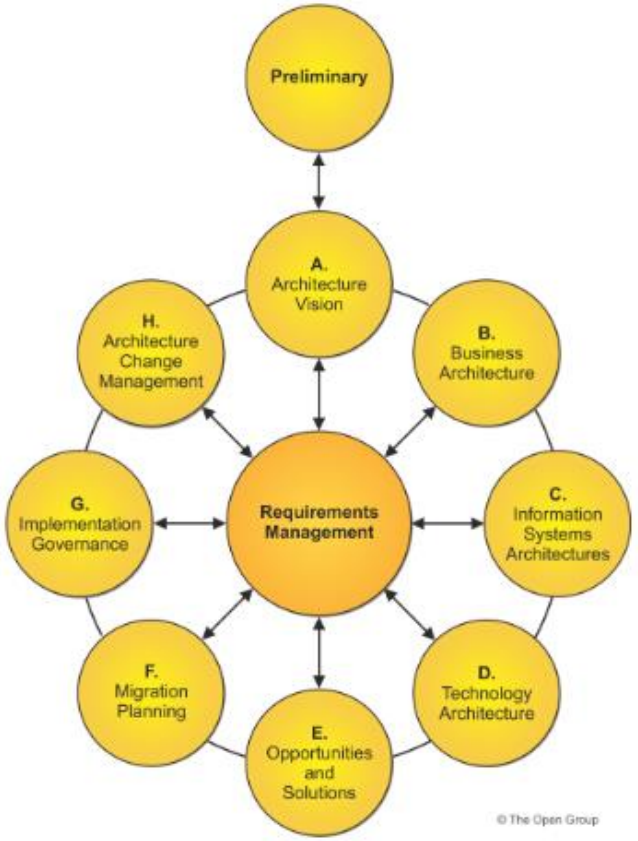
Architekt kybernetické bezpečnosti

- Enterprise architektura

stále se opakující **proces** ověřování shody s **business požadavky** a rozpracování těchto požadavků do oblasti

- Aplikační
- Datové
- Technické oblasti

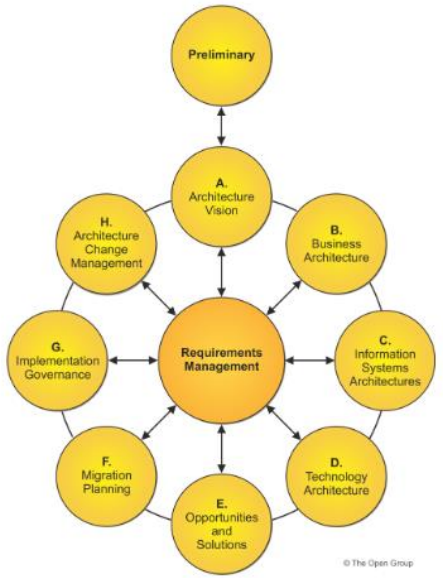
Př. TOGAF

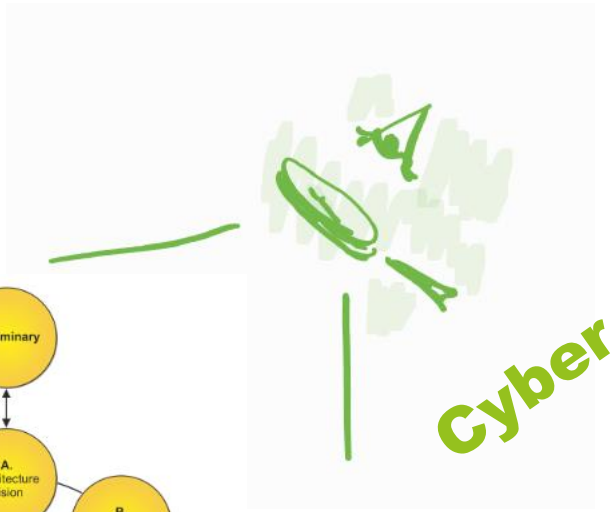


Architekt kybernetické bezpečnosti

- Architektura kybernetické bezpečnosti
  - Součást enterprise architektury

    jeden z možných specializovaných pohledů – tentokrát zaměřený na informační bezpečnost, tj zajištění důvěrnosti, integrity a dostupnosti informací zpracovávaných v IT
  - Různé metodiky/pomůcky
    - SABSA
    - TOGAF
    - **Architektura nulové důvěry** - Zero Trust Architecture





Architekt kybernetické bezpečnosti

- Nulová důvěra (Zero Trust - ZT)

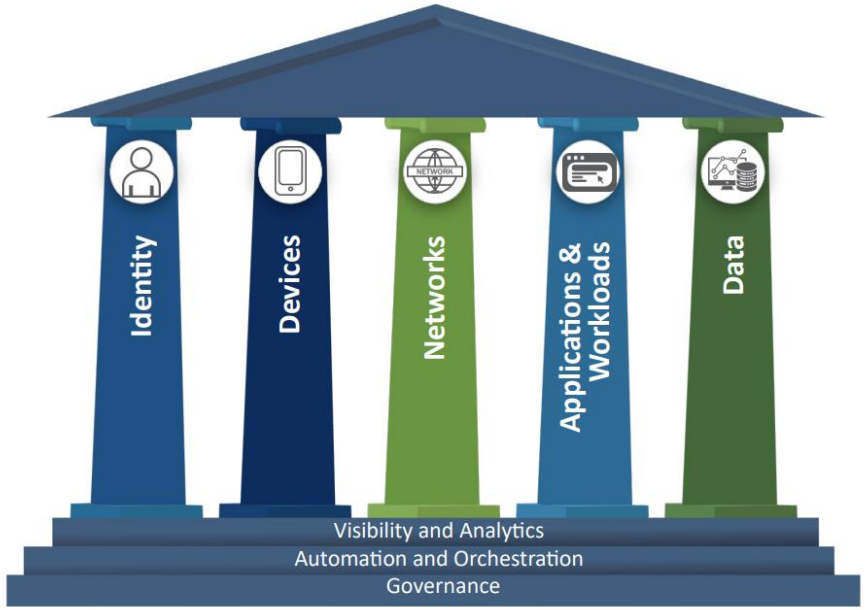
poskytuje sadu konceptů navržených tak, aby byla co nejlépe vynucena zásada nejnižšího oprávnění (least privilege) v informačních systémech a službách. Základním předpokladem tedy je, že celé IT prostředí je pokládáno bez dodatečných opatření za nedůvěryhodné ve všech úrovních podrobnosti.

- Architektura nulové důvěry (Zero Trust Architecture – ZTA)

je architektura kybernetické bezpečnosti využívající koncept nulové důvěry pro návrh fyzické i virtuální infrastruktury, provozních postupů a vazeb mezi komponentami pro celkové zvýšení bezpečnosti

Architekt kybernetické bezpečnosti

- Zdroje
  - Zero Trust Architecture – NIST Special Publication 800-207, 08/2020
  - Cybersecurity and Infrastructure Security Agency (CISA): Zero Trust Maturity Model (ZTMM), v2 04/2023



NÚKIB – CISA: https://nukib.gov.cz/cs/infoservis/aktuality/2024-nukib-s-americkymi-urady-a-dalsimi-zahranicnimi-partnery-vydal-spolecne-doporuceni-k-bezpecnosti-softwarovych-produktu/
ENISA – CISA: https://www.enisa.europa.eu/news/cisa-and-enisa-enhance-their-cooperation

Děkuji za pozornost

Ing. Ondřej Salák

osalak@ngss.cz

+ 420 702 077 068