Jak plnit vyhlášku o kybernetické bezpečnosti

Jan Mareš, jan.mares@nku.cz

Nejvyšší kontrolní úřad (NKÚ)

- Audit státního financování
- cca 500 zaměstnanců
- Práce na externích místech
- Provoz systému spadající pod významný informační systém (VIS)

Jak je to u nás

- Maximálně se snažíme uživatele omezit
- Bez ohledu na místo, tak síti nevěříme
- **Uživatel nezná heslo** (interně měníme každých 14 dnů)
- Dopady bezpečnostních opatření se snažíme minimalizovat automatizací
- Administrátor má navíc vyčleněný virtuální desktop pro administrativní práci

Lokální bezpečnost - NTB

- Data šifrována BitLockerem, klíč v TPM čipu
- Upraveno logování, kdy povoleno pouze přihlášení pomocí OTP
- Pomocí AppLockeru dovoleno spuštění pouze podepsaných aplikací nebo z daného umístění
- Plocha uzamčena (překryta aplikací měnící dostupné aplikace)
- Spouštění aplikací omezeno pomocí oprávnění

Připojování do IS úřadu

- Uživatelé bez ohledu na místo vždy budují VPN
  - Buď IKEv2 (certifikát) nebo SSL VPN (OTP kód)
- Dodavatelé pouze přes SSL VPN za pomoci hesla a SMS OTP
- Pro uživatele vytvořena aplikace za uživatele řeší připojení ke vzdálenému připojení, kdy při IKEv2 je vše „bezobslužné“
- Limitováno možnostmi firewallu (FortiGate FG-600D)

Práce v IS úřadu

- Aplikována stejná politika jako u lokální bezpečnosti
- Práce pouze ve virtuálním desktopu mající přístupné interní zdroje s hodinovou zálohou
- Virtuální desktop je v týdenních cyklech recyklován
- Využívána interní certifikační autorita

Ochrana informačního systému

- Centrální log management (Elasticsearch + Kibana)
- Centrální konzole pro aktualizace (WSUS)
- Centrální správa počítačů (System Center configuration management + defender + GPO)
- Testovací a provozní prostředí
- Monitoring sítě (Cisco Prime Infrastructure, SolarWinds Orion) a aplikací (SCOM, Zabbix)

Jak postupovat s implementací

- Stanovte si aktiva a jejich vlastnosti
  - Rizika (zranitelnosti a hrozby)
  - Významnost systému
  - Zodpovědnost a všechny procesy
- Stanovte akceptovatelnost rizik a nápravná opatření
- Implementujte nebo naplánujte do plánu zvládání rizik

Aktiva

- Stanovit rizika
- SLA
- Zodpovědnost
- Garant
- V BD uvést aktivum a garanta, zbytek vést mimo
- Volit aktiva více obecnější kvůli možným změnám

Životní cyklus uživatele

- Nejdůležitější
- Centralizovat osobní data
- Zautomatizovat životní cyklus uživatele
  - Hlavní je ukončení života
- Zbavit se hesel

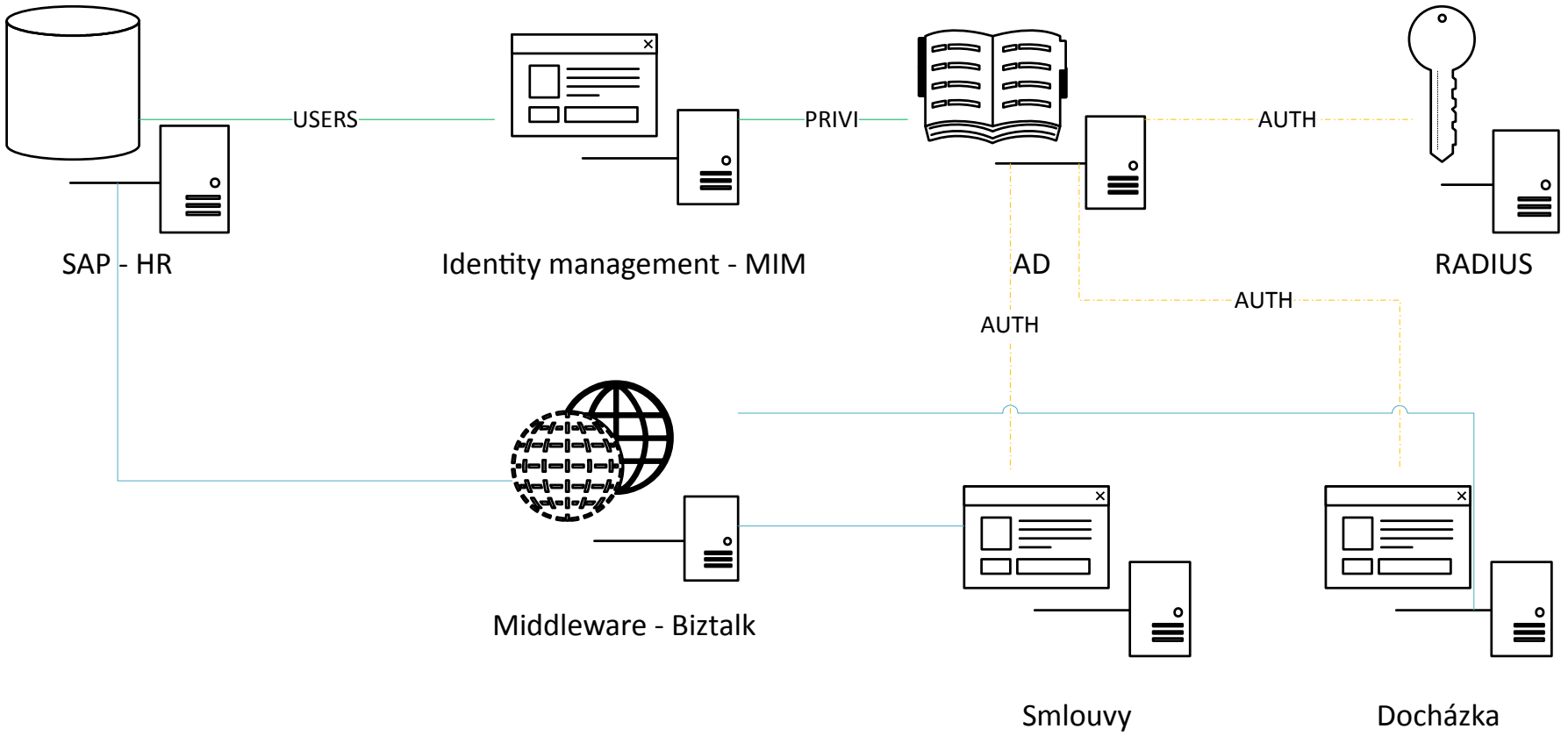
Živ. cyklus - centralizovat

- **Jedna** centrální databáze s veškerými údaji
  - u nás v rámci HR v SAPu
  - Lze odůvodnit uchovávání dat i po odchodu zaměstnance
- Distribuce do ostatních systémů pomocí middleware
  - Např. MS Biztalk
- Odmazávání při odchodu
- Vhodné i s ohledem na GDPR

Automatizace uživatelských účtů

- V závislosti na příznaku jsou uživatelé přesouvány a účty blokovány
  - Při odchodu je účet v AD automaticky zablokován a přesunut do vyčleněné větve
- Na jednom místě řízení přidělování oprávnění
- Např. MS Forefront Identity Management

Ukázka


USERS
PRIVI
AUTH
AUTH
AUTH
SAP - HR
Identity management - MIM
AD
RADIUS
Middleware - Biztalk
Smlouvy
Docházka

Živ. cyklus - hesla

- Ideálně vůbec nepoužívat hesla, pouze dynamická
  - Nová vyhláška bude vynucovat používání dvou-faktorové autentizace
- Požadavky na délku hesla se bude neustále zvyšovat
  - Nyní 8 znaků, s novou vyhláškou 13/17 znaků
- Lze použít OTP generovaný na mobilním telefonu
  - Telefon spravovaný pomocí MDM (MobileIron)
  - OTP ověřováno přes RADIUS server (Micro Focus NetIQ)

Bezpečnostní politiky

- Zpracujte všechny politiky dle §5 odst. 1 (a-u)
- Každá část na samostatný papír
- Přizpůsobte vašim současným procesům
- Například u nás se problém eskaluje stylem uživatel → administrátor → vedoucí oddělení → další vedoucí → ředitel OI → kybernetický manažer
- Vhodné rozlišit garanta aktiv na provozního (administrátor) a rozvojového (metodik)

Řízení provozu a komunikací

- Dle §10
- Provozní věci odkazovat do dokumentace, kterou lze libovolně měnit
- Obecně procesy kdo komu a co říká

Řízení přístupu

- Dle §11
- Vše musí být v síti jednoznačně identifikováno, tj. pro vše unikátní jméno včetně dodavatelů
- Rozmyslet způsob přidělování práv, zda na osobu nebo pracovní pozici
- Vhodné obecně formulovat:
  - Heslo svojí složitostí musí být odolné vůči možným útokům včetně:
    - i. útoku hrubé síly v časovém horizontu několika let,
    - ii. uhodnutí pomocí slovníku nebo nejčastějších hesel,
    - iii. odvození ze znalosti informací o uživateli.
  - Heslo musí plnit obecná doporučení stanovená ZKB a VKB.

Bezpečné chování uživatelů

- Nejlepší uživatel = bezmocný uživatel ;)
- Informujte uživatele o aktuálních rizicích
- Předpokládejte vždy nejhorší možnou variantu a systém na to připravte

Zálohování a obnova

- Stanovte si co bude zálohováno a základní proces

Dlouhodobé ukládání a archivace

- Je důležité správně klasifikovat data neboť dle zákona o archivnictví je nutné držet data po dobu 10 let

Fyzická bezpečnost

- Implementovat 802.1x – celkem náročné
- Ideálně oddělit/zabezpečit prostory s IT věcmi

Detekce kyber. událostí

- V základu stačí mít nastaveny filtry, které zobrazí/odešlou upozornění při vyšší aktivitě/neoprávněném přihlášení

Sběr a vyhodnocování bezp. událostí

- Lze použít kombinace Elasticsearch + Kibana + Logstash

Kryptografická ochrana

- Odkažte se na vyhlášku stanovující bezpečné šifry.

Co je potřeba pro tech. splnění ZKB

- Next-Gen Firewall – aplikační kontrola, ssl inspekce, IPS/IDS, antivir kontrola
- Identity management – nastavování oprávnění a zajištění životního cyklu uživatele
- Centrální autentizační zdroj – např. Active Directory spolu s RADIUS servery pro připojování dalších systémů
- Log management pro ukládání všech událostí

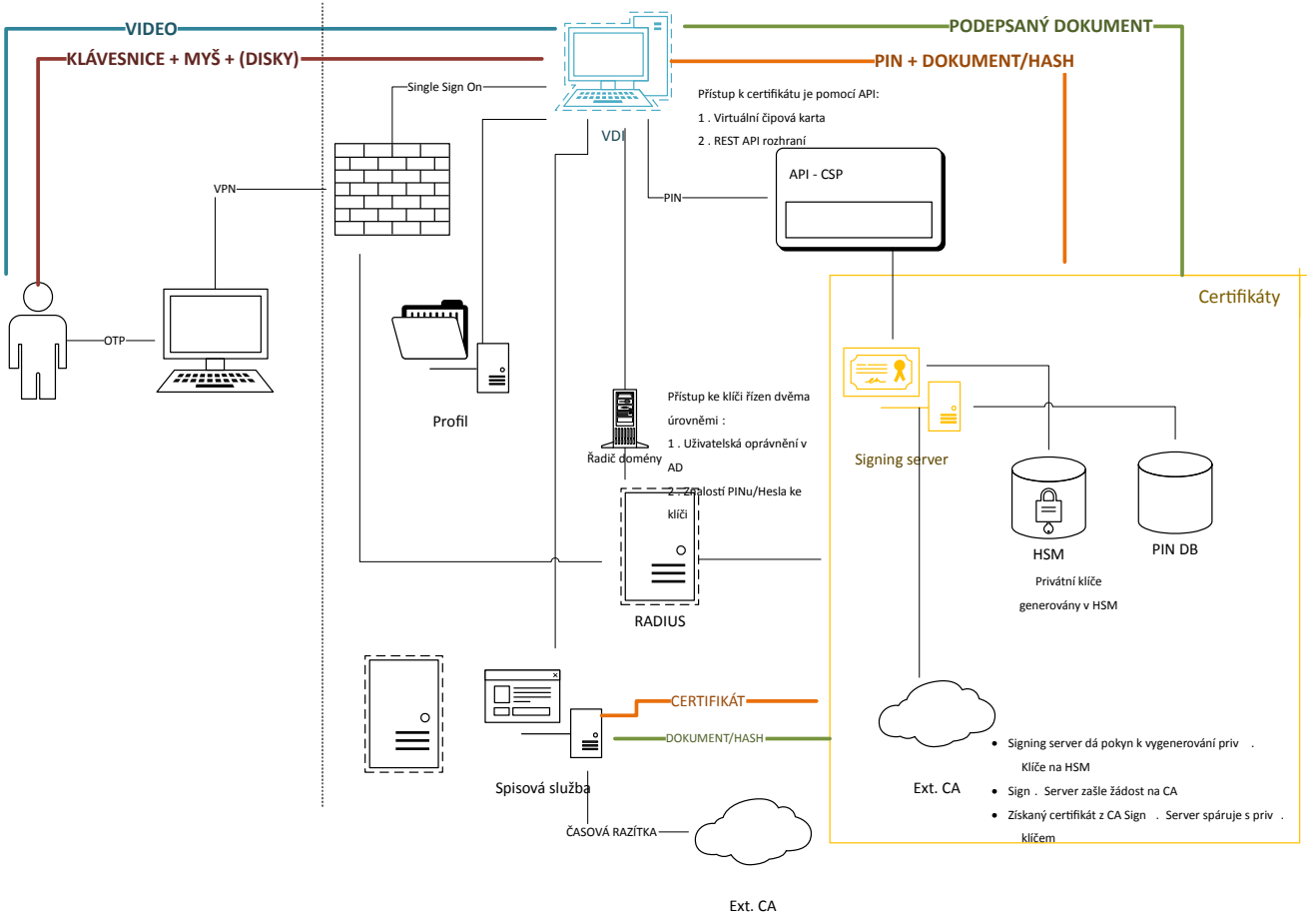
Co je potřeba pro tech. splnění ZKB

- Ověřování vstupních portů pomocí 802.1X

Co je vhodné nasadit

- Řízení privilegovaných účtů
- Netflow na okrajích sítě (kvůli NÚKIB)
- Centrální řízení vnitřních firewallů
- Provést úvahu nad centrální správou certifikátů (kvůli eIDASu)

Příklad řešení certifikátu



Náklady spojené s implementací

- Změny spojeny s pravidelnou odměnou technologií
- V rámci plánu zvládání rizik se operuje se slabinami nebo chybějícími částmi a je naplánována jejich implementace
- Přímé investice pro splnění ZKB se pohybují kolem 5 miliónů korun bez DPH