Zkušenosti z řešení vzdáleného přístupu z mobilních zařízení v rozsáhlé organizaci

podplukovník Ing. Martin Hlaváček

Agentura komunikačních a informačních systémů
Armáda České republiky

KONTEXT

- **10 000 uživatelů mobilních služeb**
- **2 neutajované a oddělené domény**
  - Internet (komunikace, G2G/G2B, welfare)
  - Vnitřní síť (administrativně správní procesy, 90% komunikace)
- **Hraniční zóna mezi DMZ Internetu a vnitřní sítí**
  - Datové schránky, státní pokladna
  - PKI, …

OD ZAČÁTKU …

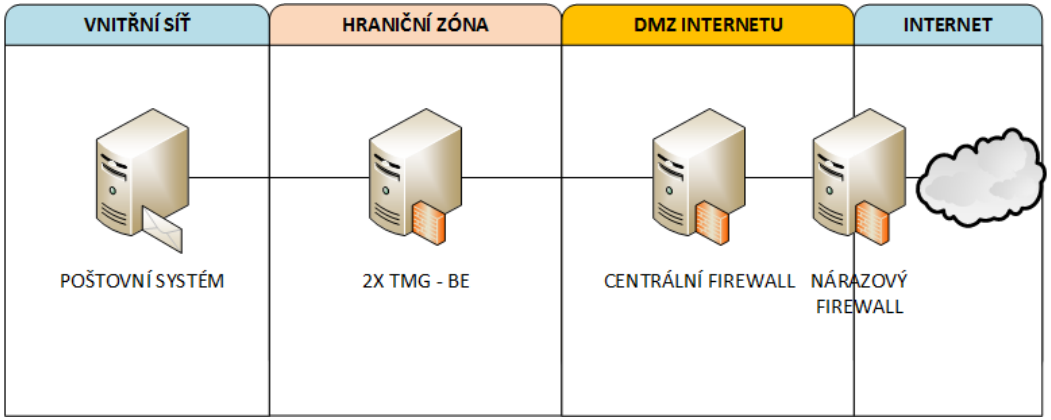
- **2010 – formulace operačního požadavku, testování**
- **2011 – první provoz**
  - » **Nokia E61i**
  - » **E90**
  - » **Nokia 6303**

Využití přes ActiveSync

- Přenos a synchronizaci kontaktů
- Kalendář
- Pošta přes rozhraní OWA
  - OWA bez captcha – zamykání účtů

Žádný software pro správu zařízení
Připojení vůči MS Exchange
Publikace vybraných účtů do DMZ
Nativní aplikace telefonů
Device Wipe přes OWA činností administrátora nad účty jednotlivce

Stav 2011



- Pouze omezené služby ŠIS (ActiveSync, OWA, SharePoint)
- Nelze definovat povolená zařízení
- Základní definice bezpečnostních politik(MS Exchange 2007)
- Nedostatečný audit/logování (zařízení, uživatel)
- Nízká úroveň zabezpečení (TMG)
- Nelze provést vzdálené nastavení na SMZ
- Problematická uživatelská podpora

VYHODNOCENÍ 2012

- **Požadavky na MDM**
  - Umístění v Magic Quadrant v Leaders
  - On – Premise řešení
  - Detekce root/Jailbreak
  - Výmaz zařízení
  - Uzamknutí SMZ
  - Podpora změny hesla ve vnitřním systému
  - Analýza logů
- **Testované produkty**
  - MobileIron,
  - McAfee,
  - BlackBerry,
  - Tivoli EndPoint Manager,
  - AirWatch

Magic Quadrant

Figure 1. Magic Quadrant for Mobile Device Management Software

Source: Gartner (May 2012)

DEFINICE POŽADAVKŮ

- **Zabezpečení –** možnost nastavení hesla, vzdálené uzamknutí, mazání nebo obnova výrobního nastavení.
- **Zálohování a obnova –** zajistit vzdálené zálohování mobilních dat a jejich případnou obnovu.
- **Nastavení –** vzdálené nastavení vlastností mobilního zařízení směrem k uživateli.
- **Data/soubory/aplikace –** vzdálená správa dat, souborů a softwarových aplikací.
- **Správa –** kontrola zařízení podle umístění, typu, výrobce, současného majitele apod.
- **Stav a diagnostika –** možnost na dálku dohlížet na kondici zařízení (stav baterie, paměti apod.).

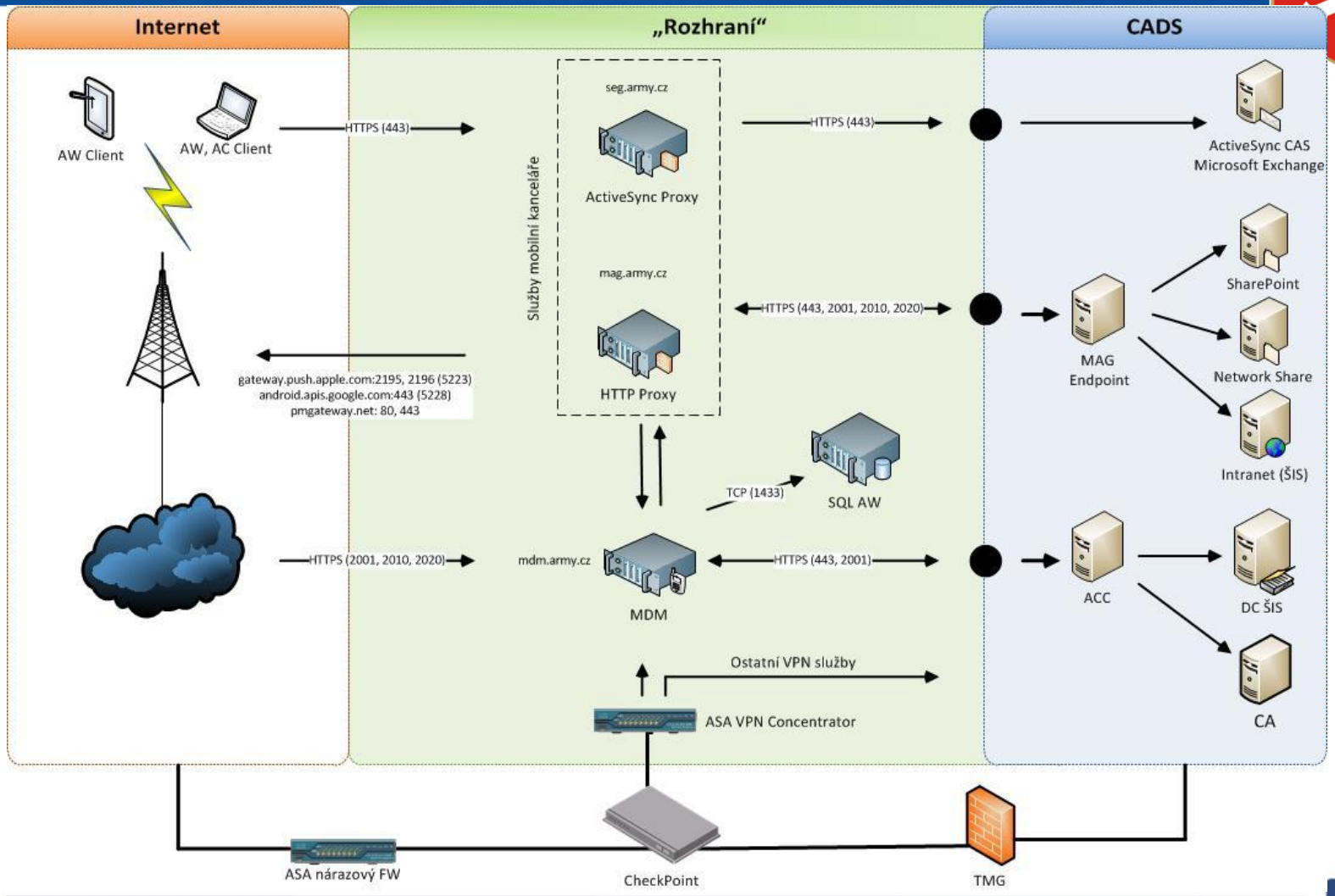
- Šifrování, vynucení TCP portu
- Pošta ve funkci proxy
- Politiky na zařízení
- Virtuální „appliance“
- Možnost dělení na vnitřní a vnější komponenty
- Vzdálené zamykání a nulování/vymazání mobilních zařízení
- Poskytování informací o zařízení
- Ochrana proti škodlivému kódu

Stav 2015

- **Zabezpečená, se souhlasným stanoviskem NBÚ**
- **Synchronizace poštovní schránky**
- **Přístup k resortním zdrojům (Sharepoint, síťové disky…)**
- **Přístup k intranetovému webu**
- **Vzdálené nastavení**
- **Vzdálená správa mobilních zařízení (provisioning)**
- **BYOD Ready**
- **User Portál, Inhouse Store…**

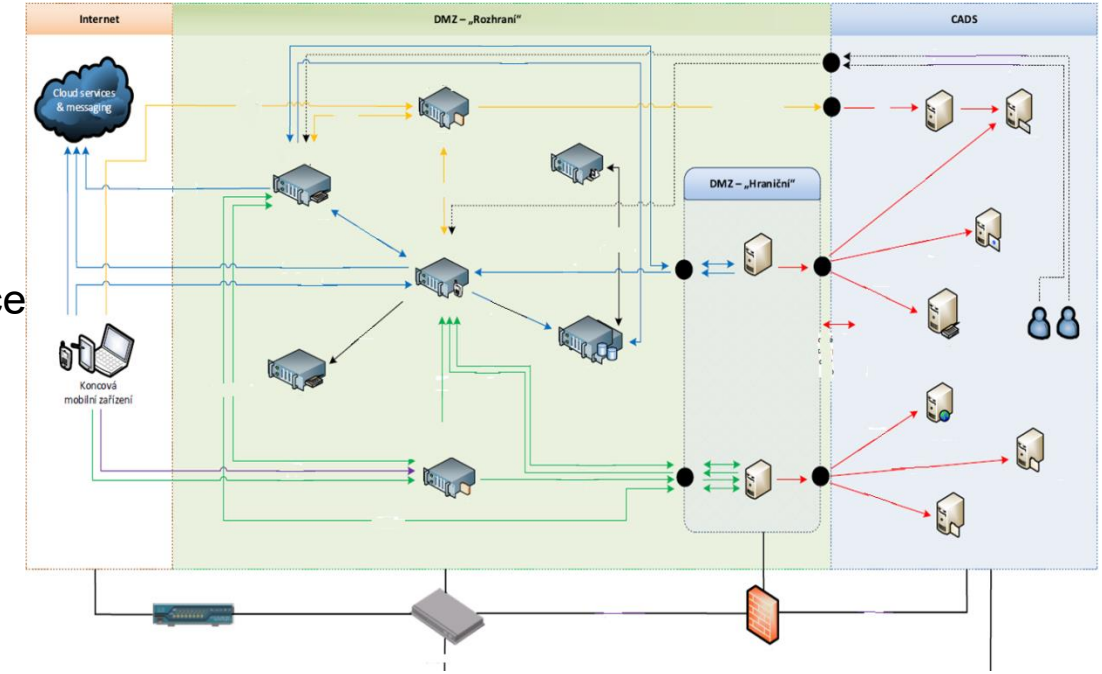
- **Obchodováno v rámci smlouvy na GSM**
  - V rámci dojednávání koncové ceny „ústupky“ na straně dodávaných zařízení
  - Plánovaná výměna MT po 2 letech zrušena na úkor spotřeby služeb GSM
- Lumia 640, Samsung A5, S-715/S-815, iPad Air 2
  - Apple:
    - mimo DEP,
    - 2FA versus vnitřní autentizace
  - Android:
    - účty u vendora,
    - jiný produkt – jiné chování,
    - od verze 7 mění chování MDM
  - Microsoft:
    - účty u vendora,
    - nevyzrálost platformy
    - ukončení podpory
- **Uživatelská tvořivost (SIM, device wipe)**
- **Desktop správa nedostatečně vyzrálá**

Stav 2015


Internet
„Rozhraní“
CADS
AW Client
AW, AC Client
HTTPS (443)
seg.army.cz
ActiveSync Proxy
HTTPS (443)
ActiveSync CAS
Microsoft Exchange
Služby mobilní kanceláře
mag.army.cz
HTTP Proxy
HTTPS (443, 2001, 2010, 2020)
MAG
Endpoint
SharePoint
Network Share
Intranet (ŠIS)
gateway.push.apple.com:2195, 2196 (5223)
android.apis.google.com:443 (5228)
pmgateway.net: 80, 443
TCP (1433)
SQL AW
HTTPS (2001, 2010, 2020)
mdm.army.cz
HTTPS (443, 2001)
MDM
ACC
DC ŠIS
CA
Ostatní VPN služby
ASA VPN Concentrator
ASA nárazový FW
CheckPoint
TMG

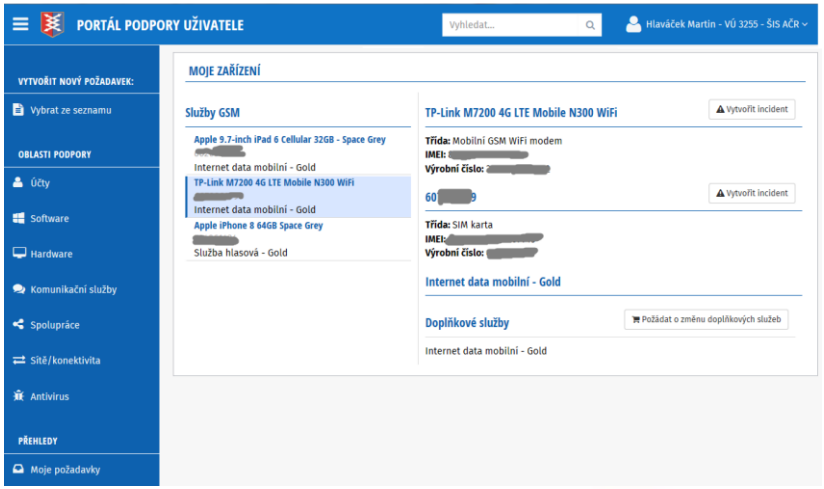
HW – jednotné OS platforma

Zařízení: smartphony, tablety
Pošta, kontakty, kalendáře
Obsah (file share)
Prohlížení (browser)
Aplikace (interní app store)
Podpora pro soukromá MZ (BYOD)
Bezpečnost (certifikáty, profily, restrikce uzamčení, wipe…)
Jednotná administrátorská konzole
Vlastní APN pro filtrovaný internet



Co nás čeká

- **Optimalizovat architekturu AW**
  - Zabezpečit vysokou dostupnost
  - Změny celkové struktury DMZ Internetu
- **Efektivnější využití informací z DB AW**
  - Vazba na účetní a operativní evidenci majetku
  - Vazba na CMDB
- **Integrace**
  - S dohledovými a ticketovacími nástroji
  - Pokročilá analýza bezpečnostních informací
  - Integrace do Privileged Access Management
  - On premise videokonferenční prostředek
  - Řešení pro Citrix Reciever na tabletech
- **Znovu experimentování s notebooky**
- **Optimalizace využití vlastní APN**
- **Implementace VPN**



Drobné shrnutí

Jinak než MDM si řešení nedovedu představit
On premise – záleží na politice organizace
Více platforem – nesmírně komplikuje správu
Bez (pozitivních) zkušeností se správou desktop OS
Ergonomie mobilního zařízení klíčová
Sledujeme pokles „odporu“ uživatelů
Preferované platformy: Apple + DEP, Android KNOX, SAFE

Vyzrálost řešení

Ad hoc	synchronizační protokoly/web access
Základní	MDM
Pokročilé	MDM + APN + VPN
Plné	integrované řešení (bezpečnost, provoz)

DĚKUJI ZA POZORNOST

podplukovník Ing. Martin Hlaváček
náčelník centra uživatelských služeb
Agentura KIS, Armáda České republiky

m.hlavacek@army.cz