SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Moderní řešení bezpečnosti infrastruktury

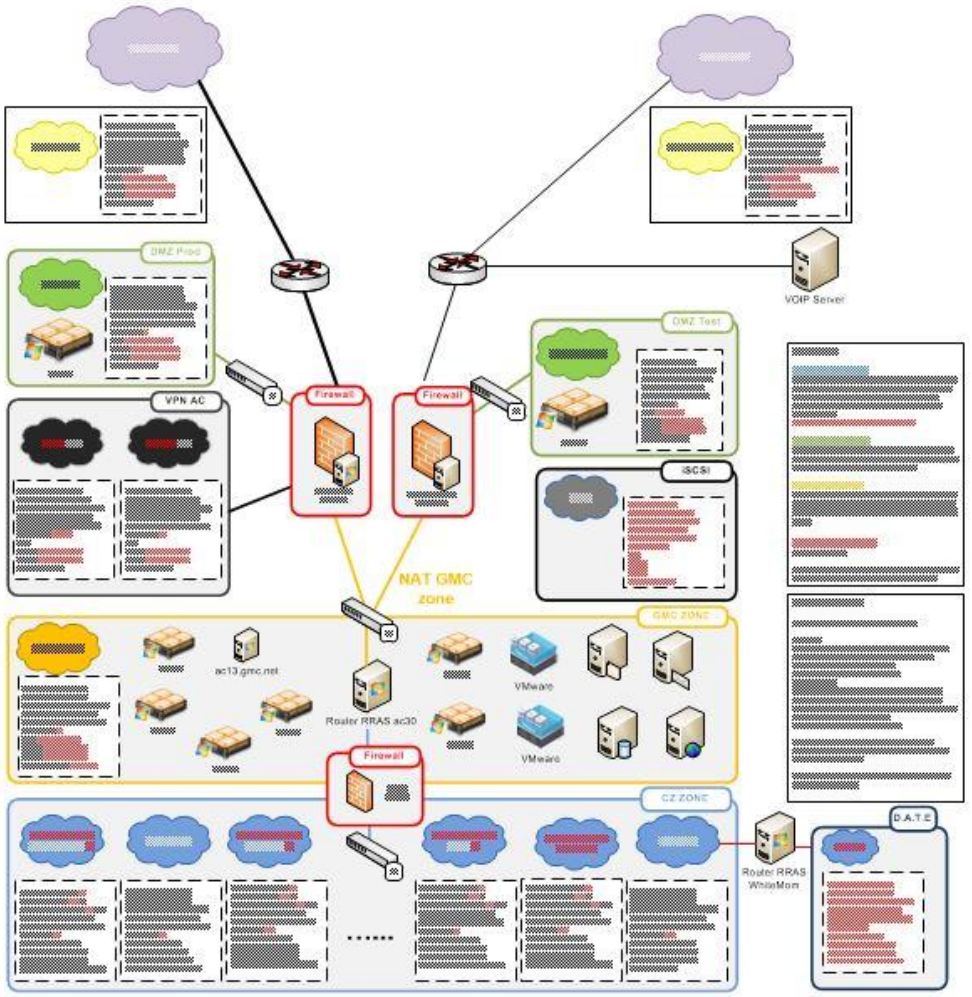
Marek Podlešák
GMC Software Technology s.r.o.
Tomáš Vobruba
AEC, spol. s r.o.

Jak to všechno u Náš začalo

- Rozhodnutí pro certifikaci ISO 27001
- Interní penetrační testy
- Nevyhovující stav infrastruktury – plochá síť, omezená kapacita a výkon
- Absence řízení provozu a stabilita.
- Nevyhovující bezpečnostní model

Naše prostředí

- 80 vývojářů
- Minimální omezení
- Více platforem
- Nadstandardní požadavky a potřeby
- Vysoká práva



Pohled dodavatele

- Moderní infrastrukturní bezpečnost musí řešit požadavky velké mobility
- Paketové filtry již nestačí
- IPS jsou samy o sobě slabé
- Kontrola vzdáleného přístupu
- Kontrola management zón
- Inspekce HTTP/HTTPS
- Kontrola aplikací cloudového typu
- Problémy virtualizace
- Monitoring

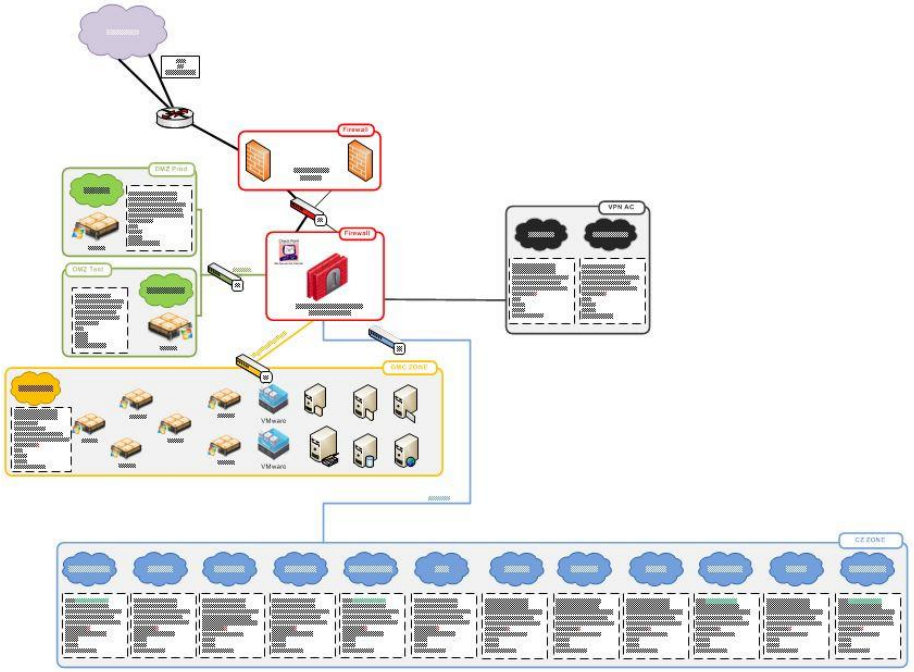
Co s tím?

- Konzultant
- Dlouhé rozhodování
- Důkladná analýza stávajícího stavu

Návrh nového řešení

Cílem bylo:

- Nové řešení navrhlo členění na základní VLAN-y
- Umožnilo odstranit nedostatky stávajícího modelu
- Zvýšilo propustnost a stabilitu
- Otevřelo síť snadnému implementování nových bezpečnostních prvků
  - Technologická abstrakce bezpečnosti
  - Plná kontrola nad odchozím provozem
  - Zlepšení podpory mobility



Implementace

- **Informační kampaň pro uživatele**
- Důkladná Příprava
- Implementace v krocích
- Záložní plán
- Testování, testování a testování
- Ladění
- Zpětná kompatibilita funkčností

Nasazené řešení I

Shrnutí za dodavatele

- Kompletní restrukturalizace vyžadovala aktivní přístup objednavatele i dodavatele

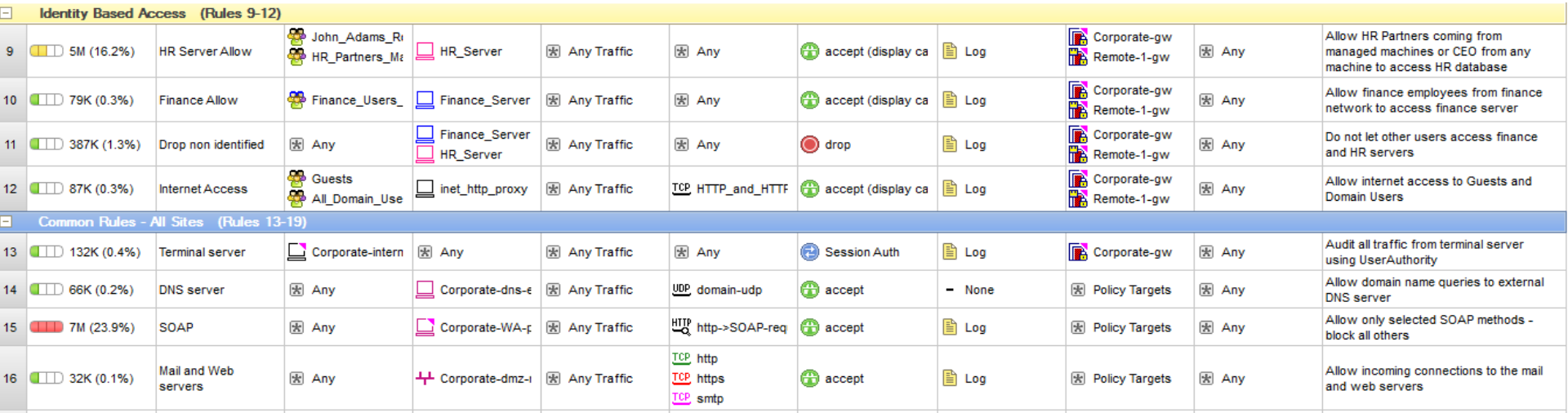
- Rozsah provedené restrukturalizace potřeboval cca 180MD celkové práce celého týmu.
- Segmentace byla vedena ve stylu FTFP projektu
- Změna nebyla bezbolestná a bezproblémová:
  - Technické problémy
  - Organizační problémy
  - Procesní problémy

Nasazené řešení II

- 1 rok implementace …nejsme u konce, změny mají přesah samotného projektu.
- 5 fází (rušení Router, FW, zřízení nové, VPN)
- 1 školení na Checkpoint
- Zjišťujeme co jsme si koupili
- Objeví se problémy, které nebyly vidět
- Změna logiky – vše je zakázané a co je potřeba povoluje se

Přínosy a výhody pro GMC

- Spolehlivost (HA)
- Vyšší stupeň řízení komunikace
- Rozšiřitelnost řešení – umožňuje nám růst
- Víme kde jsme
- Enterprise řešení s kvalitním suportem
- Výrazně se posunula bezpečnost sítě



	Identity Based Access (Rules 9-12)										
9	5M (16.2%)	HR Server Allow	John_Adams_R HR_Partners_Ma	HR_Server	Any Traffic	Any	accept (display ca	Log	Corporate-gw Remote-1-gw	Any	Allow HR Partners coming from managed machines or CEO from any machine to access HR database
10	79K (0.3%)	Finance Allow	Finance_Users_	Finance_Server	Any Traffic	Any	accept (display ca	Log	Corporate-gw Remote-1-gw	Any	Allow finance employees from finance network to access finance server
11	387K (1.3%)	Drop non identified	Any	Finance_Server HR_Server	Any Traffic	Any	drop	Log	Corporate-gw Remote-1-gw	Any	Do not let other users access finance and HR servers
12	87K (0.3%)	Internet Access	Guests All_Domain_Use	inet_http_proxy	Any Traffic	HTTP_and_HTTF	accept (display ca	Log	Corporate-gw Remote-1-gw	Any	Allow internet access to Guests and Domain Users
	Common Rules - All Sites (Rules 13-19)										
13	132K (0.4%)	Terminal server	Corporate-intern	Any	Any Traffic	Any	Session Auth	Log	Corporate-gw	Any	Audit all traffic from terminal server using UserAuthority
14	66K (0.2%)	DNS server	Any	Corporate-dns-s	Any Traffic	domain-udp	accept	None	Policy Targets	Any	Allow domain name queries to external DNS server
15	7M (23.9%)	SOAP	Any	Corporate-WA-p	Any Traffic	http->SOAP-req	accept	Log	Policy Targets	Any	Allow only selected SOAP methods - block all others
16	32K (0.1%)	Mail and Web servers	Any	Corporate-dmz-i	Any Traffic	http https smtp	accept	Log	Policy Targets	Any	Allow incoming connections to the mail and web servers

Nevýhody a ztráty

- Cena (vstupní náklady)
- Podpora - závislost na dodavatelích
- Přechod z Microsoftu na Linux
- Nové a méně pod kontrolou
- Ladění pravidel

SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Marek Podlešák
GMC Software Technology
m.podlesak@gmc.net