DŮVĚŘUJTE SILNÝM

Technické aspekty zákona o kybernetické bezpečnosti

Michal Zedníček
Key Account Manager
CCSSS, ID No.: CSCO11467376
michal.zednicek@alef.com
ALEF NULA, a.s.

Petr Vácha
Team Leader – Security
CCSP, CCSI# 25008, IronPort ICSP, ICSI
petr.vacha@alef.com
ALEF NULA, a.s.

ALEF NULA

COMSYS®

Agenda

- Zákon o kybernetické bezpečnosti
- Technická opatření dle zákona o kybernetické bezpečnosti

ALEF NULA

COMSYS®

Zákon o kybernetické bezpečnosti – kdo

- Řešitelem je Národní bezpečnostní úřad na základě usnesení vlády České republiky ze dne 19. října 2011 č. 781
- gestor problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast

ALEF NULA

COMSYS®

Zákon o kybernetické bezpečnosti – pro koho

- Kritická informační infrastruktura
- Významné informační servery
- A jiní ...

- Dynamický seznam společností

ALEF NULA

COMSYS®

Zákon o kybernetické bezpečnosti – proč

- Hrozba kybernetické kriminality/kybernetického terorismu/kybernetické špionáže
- Ekonomické dopady kybernetických incidentů
- Tlak okolního světa na řešení kybernetické bezpečnosti formou závazné právní regulace.
- Více viz důvodová zpráva NBÚ

ALEF NULA

COMSYS®

Zákon o kybernetické bezpečnosti – stav

- Přerušené jednání Legislativní rady vlády
- Dle NBÚ korekce návrhu zákona v terminologické rovině
- Čekáme na novou vládu/poslaneckou sněmovnu
- Prováděcí právní předpis není (zatím) k dispozici

ALEF NULA

COMSYS®

Zákon o kybernetické bezpečnosti – obsah

- ZÁKLADNÍ USTANOVENÍ
- SYSTÉM K ZAJIŠTĚNÍ KYBERNETICKÉ BEZPEČNOSTI
- STAV KYBERNETICKÉHO NEBEZPEČÍ
- VÝKON STÁTNÍ SPRÁVY
- KONTROLA, DOHLED A SANKCE
- PŘECHODNÁ A ZMOCŇOVACÍ USTANOVENÍ
- ÚČINNOST

ALEF NULA

COMSYS®

SYSTÉM K ZAJIŠTĚNÍ KYBERNETICKÉ BEZPEČNOSTI

- Organizační opatření
- Technická opatření

ALEF NULA

COMSYS®

Organizační opatření jsou zejména

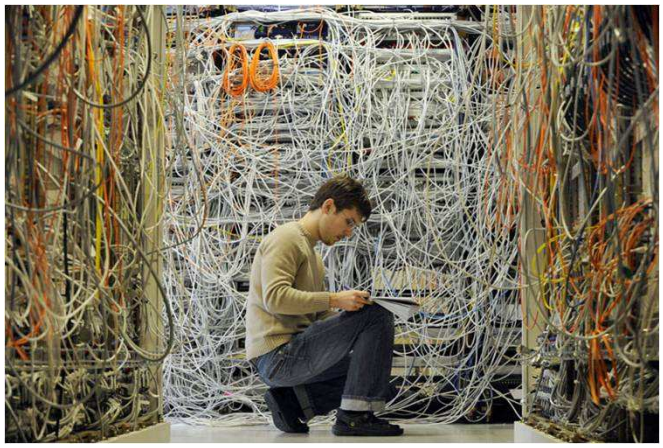
a) systém řízení bezpečnosti informací
b) hodnocení rizik
c) bezpečnostní politika, jež určuje cíle, pravidla a požadavky bezpečnosti informací
d) organizační bezpečnost, která určuje strukturu, role a funkce řízení bezpečnosti informací
e) stanovení bezpečnostních požadavků pro dodavatele
f) řízení aktiv
g) bezpečnost lidských zdrojů
h) řízení provozu kritické informační infrastruktury nebo významného informačního systému
i) řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému
j) akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů
k) systém zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů
l) řízení kontinuity činností
m) provedení kontroly a auditu kritické informační infrastruktury a významných informačních systémů a
n) plán připravenosti na řešení kybernetických bezpečnostních incidentů.

Vychází z ISO 27000

ALEF NULA

COMSYS®

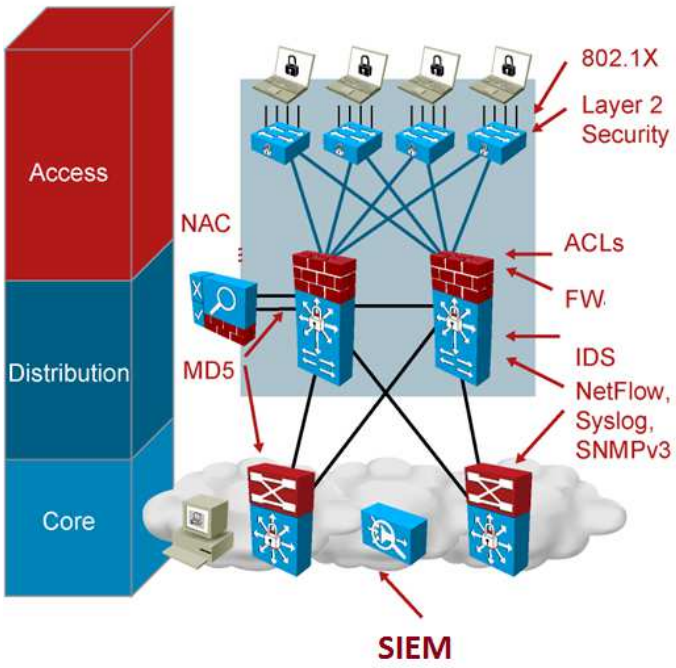
Technická opatření jsou zejména



ALEF NULA

COMSYS®

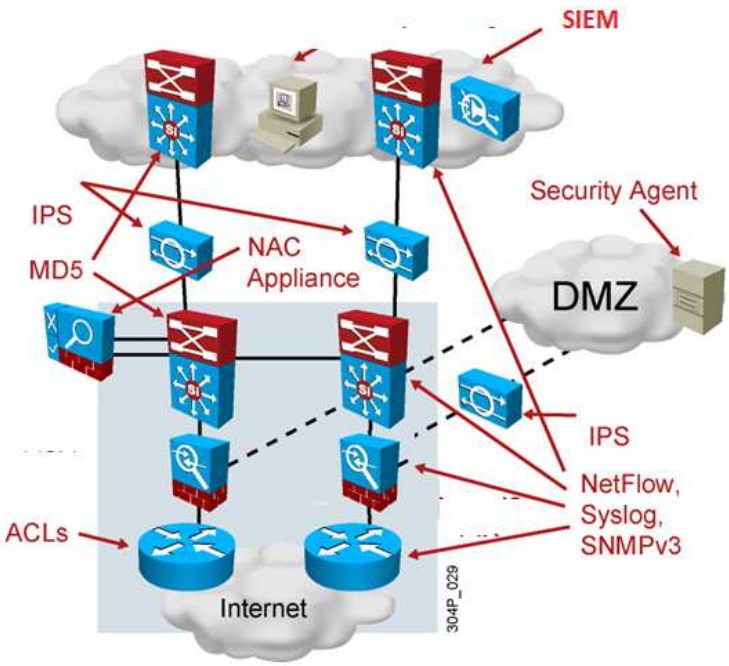
Interní bezpečnost



ALEF NULA

COMSYS®

Externí bezpečnost



ALEF NULA

COMSYS®

Firewall

- Filtrování provozu na úrovni TCP/IP
- Aplikační hloubková inspekce
- Normalizace TCP
- Vysoká dostupnost a virtualizace

- Integrace s dalšími funkcemi – IPS, VPN, Antivirus, Antispam ...
- Hodně kombinovaných funkcí = negativní vliv na výkon

ALEF NULA

COMSYS®

Intrusion Prevention System

- Hloubková inspekce aplikačního provozu
- Hlubší a komplexnější analýza provozu, než od firewallů
- Plnohodnotná integrace IPS funkcionalit do firewallů
- Rozpoznávání známých útoků pomocí signatur
- Rozpoznávání síťových virů a červů
- IPS se u zákazníků neinstaluje, ale implementuje !
- IPS je nutné vyladit podle potřeb sítě zákazníka a neustále ho udržovat

ALEF NULA

COMSYS®

VPN

› SSL VPN pro mobilní uživatele
- Integrace s MS AD/LDAP
- Vícefaktorová autentizace uživatelů
- Důležitá je podpora uživatelských OS Windows XP,Vista, 7, 8 (32/64 bit,), Linux 32/64, MAC OS, Android, iOS ...

› Site – to – site VPN
- podpora silných bezpečnostních mechanizmů - SHA-2, IKEv2 atd.

ALEF NULA

COMSYS®

Bezpečný přístup do internetu

› Filtrování na základě URL kategorií
› Rozpoznávání aplikací v HTTP/HTTPS
› Integrace s MS AD/LDAP pro autentizaci a autorizaci uživatelů
› Detekce malwarem nakažených počítačů
› Vícenásobná kontrola antivirem a antimalwarem
› Z hlediska uživatele komfortní kontrola stahovaného obsahu
› Reporting provozu z pohledu bezpečnosti i z hlediska uživatelského chování

ALEF NULA

COMSYS®

Emailová bezpečnost

- Extrémě nízký počet „false positive“
- Možnost integrace s MS AD/LDAP
  - lze definovat politiky podle skupin v MS AD/LDAP
- Virtualizace SMTP identit
- Vysoký výkon a inteligentní hloubková inspekce SMTP = odolnost proti DoS a DDoS útokům
- Date Lost Prevention
- Uživatelské šifrování emailů

ALEF NULA

COMSYS®

Ochrana proti Distribuovaným DoS útokům

- Řešení pro veřejně poskytované služby
- “Vyčistí legitimní provoz od falešného
- Nutno kooperovat s ISP nebo hosting centrem při nasazení
- Jedná se o sofistikovaná řešení => nákladné
- Stejně jako u IPS se toto řešení musí implementovat dle lokálních požadavků sítě/provozované služby
- Je nutné neustále udržovat systém ve vyladěném stavu

ALEF NULA

COMSYS®

802.1x řízení přístupu v LAN síti a BYOD

- Zajistí se připojování pouze korporátních zařízení do LAN a WiFi sítě
- Ověřování pomocí PKI i uživatelským jménem a heslem
- Lze přidělovat dynamicky VLANy, ACL na přepínačích na základě autentizace uživatelů nebo zařízení
- Je možné přídělovat různá úrovně síťových oprávnění podle typu zařízení, lokality, způsobu přístupu atd.
- Nasazení 802.1x výrazně ovliňuje i ostatní procesy ve firmě, které s tím na první podhled ne zcela souvisejí
- Procesní část je vždy výrazně složitější než ta technologická

ALEF NULA

COMSYS®

Autentikace, autorizace a účtování

- Autentizace – heslo, certifikát, otisk
- Autorizace – co se smí dělat
- Accounting – co, kdy, kde ...

- Řízení přístupu pro administraci síťových prvků
- TACACS a RADIUS server
- Přidělování administračních práv i na úrovni příkazů ...

ALEF NULA

COMSYS®

SIEM a behaviorální analýza provozu sítě

- Vyhodnocování a korelace událostí ze síťových prvků a síťových aplikací
- Zobrazování incidentů při nestandartních událostech na základě signatur a vlastních pravidel
- Při behaviroální analýze se snímá síťový provoz pomocí externích sond nebo se vyhodnocuje NetFlow protokol posílaný ze síťových prvků
- Dlouhodobé uchování logů o síťovém provozu
- Nutné provést implementaci na lokální podmínky sítě a následně tento stav udržovat

ALEF NULA

COMSYS®

DŮVĚŘUJTE SILNÝM

Děkuji za pozornost

Petr Vácha
petr.vacha@alef.com

Michal Zedníček
michal.zednicek@alef.com

ALEF NULA