Luděk Novák

Bezpečnost standardně a trochu praxe

15. října 2007

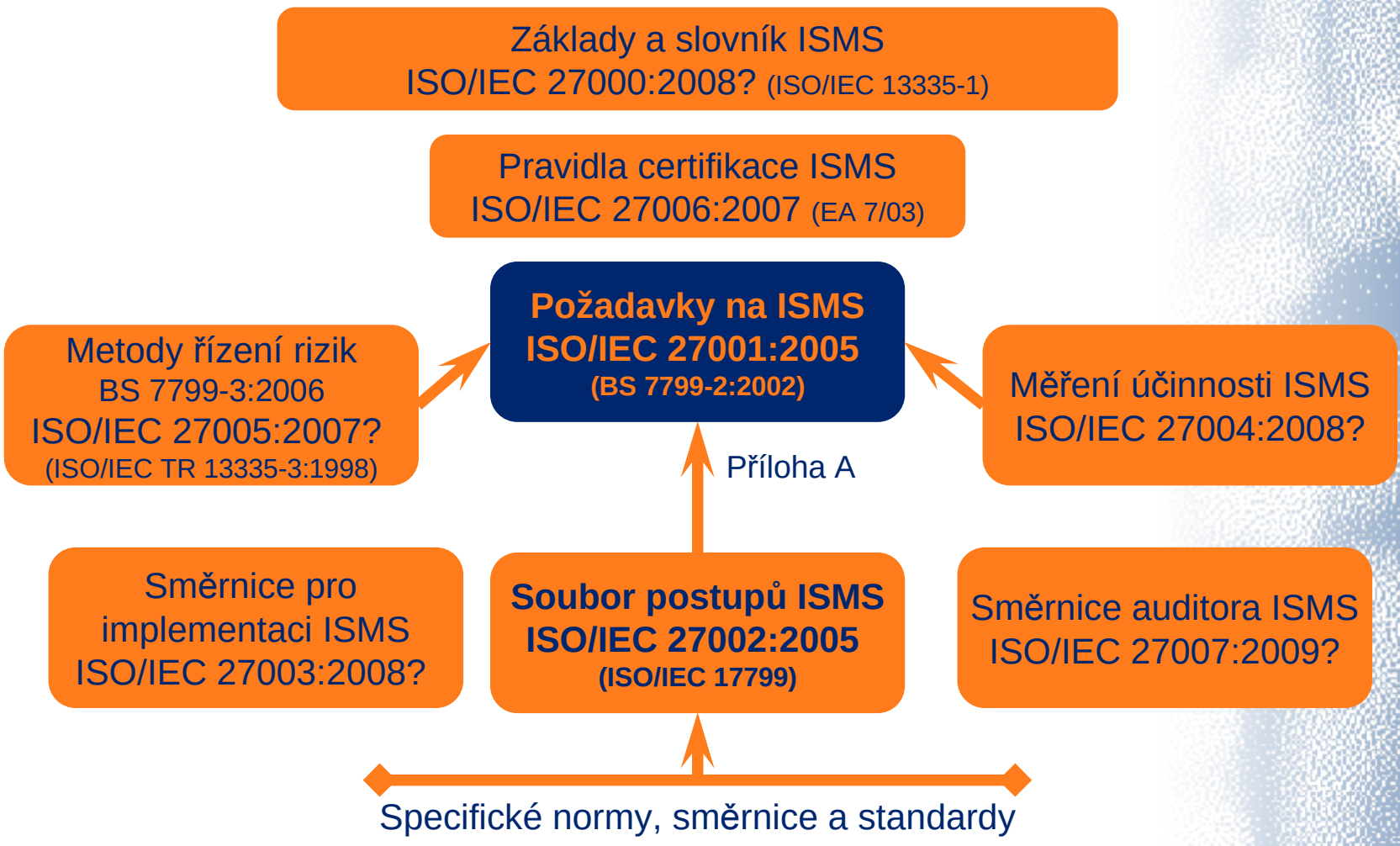
Obsah

- Řízení bezpečnosti informací
  - Koncepce řady ISO/IEC 27000
  - Systém řízení bezpečnosti informací
  - Soubor postupů pro řízení bezpečnosti informací
- Technické normy a doporučení
  - Bezpečnost sítí IT
  - Výběr, nasazení a provoz IDS
  - Zvládání bezpečnostních incidentů
- Případová studie: audit bezpečnosti technologií
- Závěr

Řada norem ISO/IEC 27000

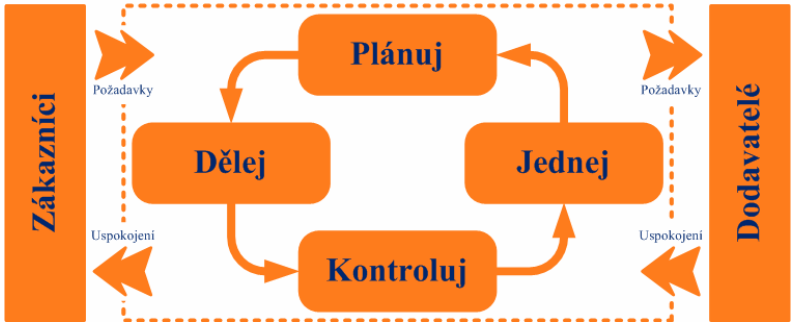
- Vznik řady odsouhlasen na jaře 2005
  - Odlišné číslování přebíraných standardů BS 7799 (ISO/IEC 17799, resp. ISO/IEC 24743)
- Systematická harmonizace dvou existujících konceptů
  - ISO/IEC 13335 – „akademický“ pohled
  - BS 7799 – „pragmatický“ pohled
- Kritéria pro zařazení do série
  - Přímá podpora a podrobnější výklad pravidel pro implementaci procesů definovaných v ISO/IEC 27001
  - Obsahuje přidanou hodnotu vůči ISO/IEC 27001
  - Upřesňuje specifika ISMS pro určitá odvětví
  - Jasně určené vazby na ISO/IEC 27001
  - Nestačí návody či upřesnění spojená s realizací opatření definovaných v ISO/IEC 17799 (ISO/IEC 27002)

Přehled řady norem ISO/IEC 27000



ČSN ISO/IEC 27001:2006 (dříve ČSN BS 7799-2)

- Systém managementu bezpečnosti informací – Požadavky
  - Základem normy jsou pravidla BS 7799-2:2002
  - ISO/IEC 27001 vydána v říjnu 2005
  - Jako ČSN ISO/IEC 27001:2006 publikována v říjnu 2006
- Definice požadavků na systém řízení bezpečnosti informací (Information Security Management System – ISMS)
- Pravidla a postupy pro systematický a odůvodněný výběr, prosazování, kontrolu a zlepšování bezpečnostních opatření (katalog dle ČSN ISO/IEC 27002:2006)
- Proces řízení bezpečnosti informací vycházející z modelu PDCA
  - Plánuj – Plan, Dělej – Do, Kontroluj – Check, Jednej – Act



ČSN ISO/IEC 27002:2006 (ISO/IEC 17799)

Soubor postupů pro management bezpečnosti informací

- Ucelená a vyvážená soustava opatření pro ochranu informačních aktiv
- Mezinárodně respektovaná soustava doporučení
- Publikována v červnu 2005
- Jako ČSN srpen 2006
- Označení ISO/IEC 27002 platí od července 2007

Norma popisuje „nejlepší praxi“

- 11 oddílů bezpečnosti
- 39 cílů opatření
- 133 opatření
- Strukturovaný popis opatření
  - Definice
  - Návod pro implementaci
  - Další informace
- V textu je sloveso „should“

Norma neupřesňuje systém řízení

- Nejsou definovány příslušné manažerské techniky pro výběr a prosazení opatření (obsahuje ČSN ISO/IEC 27001)

Uspořádání ČSN ISO/IEC 27002:2005 (ISO/IEC 17799)

Zdroj: ČSN ISO/IEC 17799:2006

ISO/IEC 18028 – Bezpečnost sítí IT

- ISO/IEC 18028-1:2006
  Část 1: Řízení bezpečnosti sítí
- ISO/IEC 18028-2:2006
  Část 2: Architektura bezpečnosti sítí
- ISO/IEC 18028-3:2005
  Část 3: Bezpečná komunikace mezi sítěmi za použití bezpečnostních bran
- ISO/IEC 18028-4:2004
  Část 4: Bezpečný vzdálený přístup
- ISO/IEC 18028-5:2005
  Část 5: Bezpečná komunikace mezi sítěmi za použití virtuálních privátních sítí

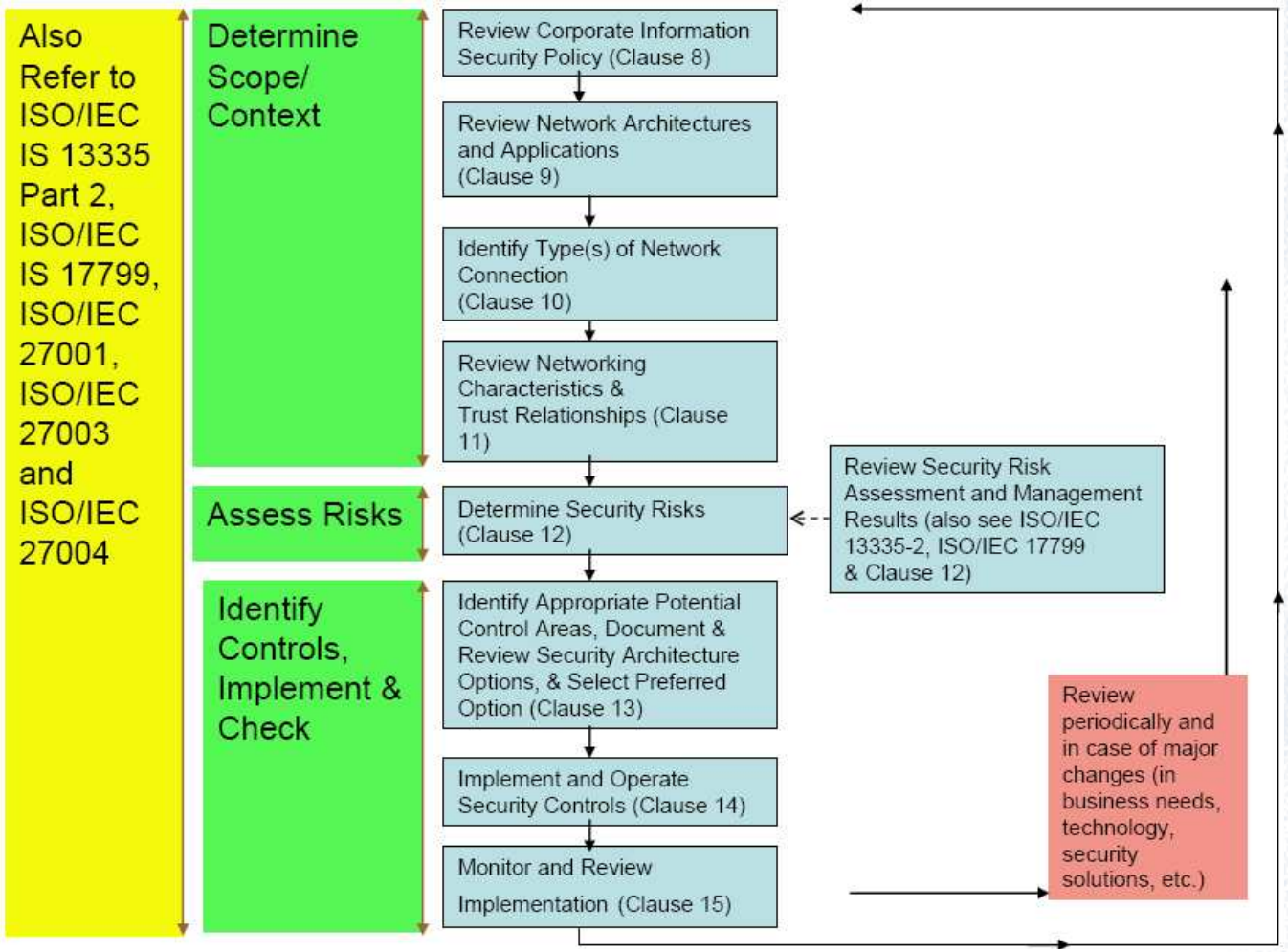
Proces řízení bezpečnosti sítí

ISO/IEC 18028-1:2006 – IT network security

Part 1: Network security management

- Využití modelu PDCA (Plan – Do – Check – Act)
- Harmonizace s obecnými přístupy pro řízení bezpečnosti
- Bezpečnostní opatření sladěna s obecným katalogem ISO/IEC 17799
- Upřesnění bezpečnostních rizik a opatření pro různé typy sítí
  - Lokální sítě
  - Globální sítě
  - Bezdrátové sítě
  - Rádiové sítě
  - Broadband Networking
  - Konvergentní sítě (data, hlas, video)

Model řízení bezpečnosti sítí



Vhodná bezpečnostní opatření

- **Architektura bezpečnosti sítě (ISO/IEC 18028-2)**
- Řízení bezpečnosti služeb
- Řízení bezpečnosti sítě
- Řízení technických zranitelností (ISO/IEC 27002:12.6)
- Identifikace a autentizace (ISO/IEC 27002:11.4)
- Zaznamenávání událostí na síti a monitoring (ISO/IEC 27002:10.10)
- Detekce průniku (ISO/IEC 27002:13)
- Ochrana před škodlivým kódem (ISO/IEC 27002:10.4)
- Služby infrastruktury založené na kryptografii (ISO/IEC 27002:12.3)
- Řízení kontinuity činností sítě (ISO/IEC 27002:14)

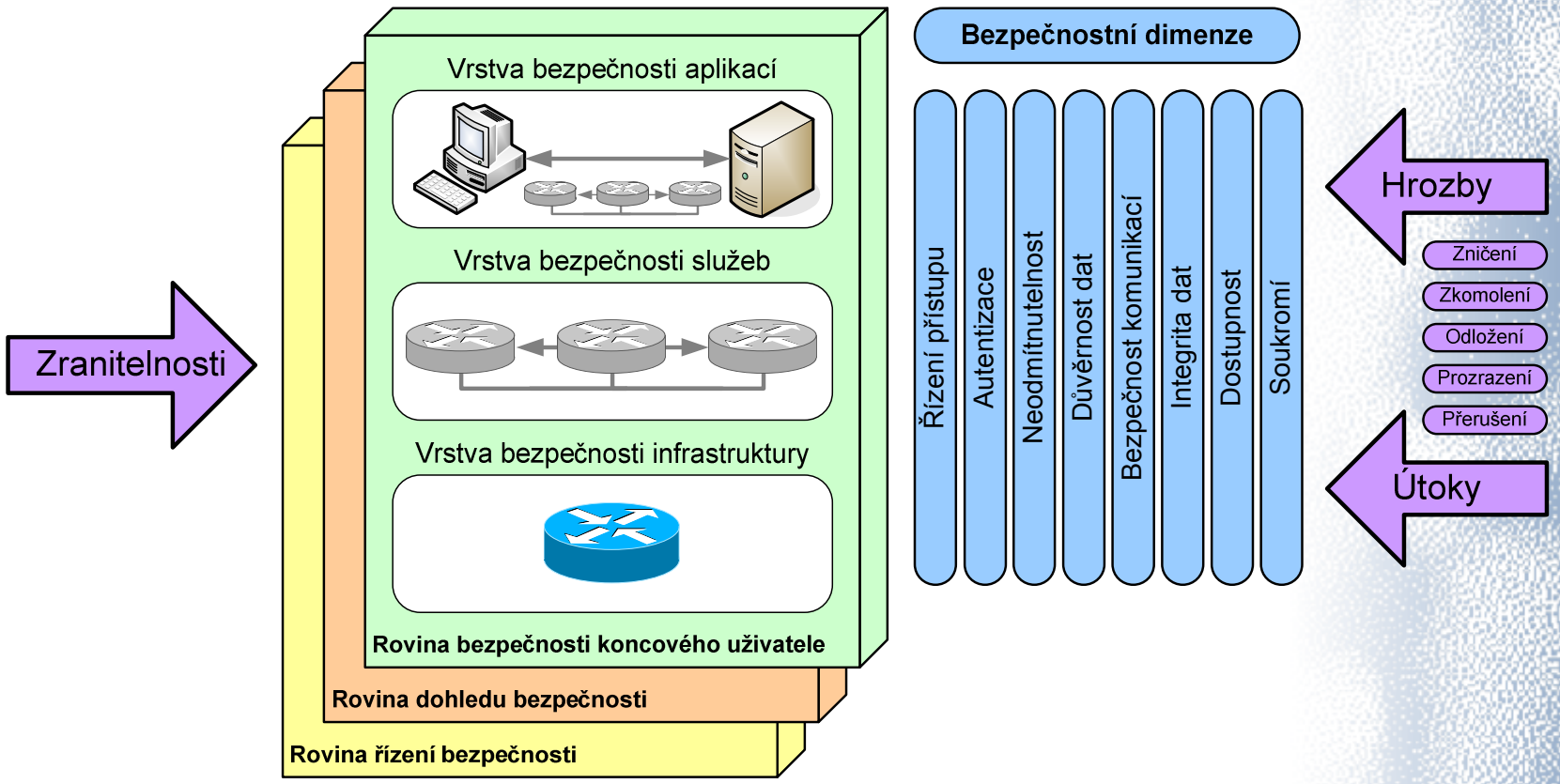
Tři pohledy referenční architektury

ISO/IEC 18028-2:2006 – IT network security

Part 2: Network security architecture

- Bezpečnostní dimenze (Security Dimension)
  - Množina bezpečnostních opatření prosazujících určitý aspekt bezpečnosti sítě
- Vrstva bezpečnosti (Security Layer)
  - Představuje hierarchii zařízení a prostředků sítě
- Rovina bezpečnosti (Security Plane)
  - Představuje určitý typ činností sítě

Zobrazení referenční architektury bezpečnosti

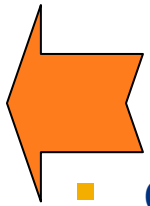


to co nás spojuje...

ANECT

Obsah bezpečnostní politiky sítí

- Úvod
- Východiska
- Definice základních pojmů
- Oblasti působnosti bezpečnosti sítí
  - Bezpečnost aplikačních služeb
  - Bezpečnost komunikačních služeb
  - Bezpečnost komunikační infrastruktury
  - Dohled bezpečnosti sítí
  - Řízení bezpečnosti sítí
- Aktualizace politiky



- Cíle bezpečnosti
- Aplikovaná opatření

Použití bezpečnostních bran

ISO/IEC 18028-3:2005 – IT Network Security

Part 3: Securing communications between networks using security gateways

Techniky

- Packet filtering
- Stateful packet inspection
- Application proxy
- Network Address Translation (NAT)
- Content analyzing and filtering

Architektury nasazení

- Packet filter firewall
- Dual-homed gateway
- Screened host
- Screened subnet

Doporučení pro výběr a provoz

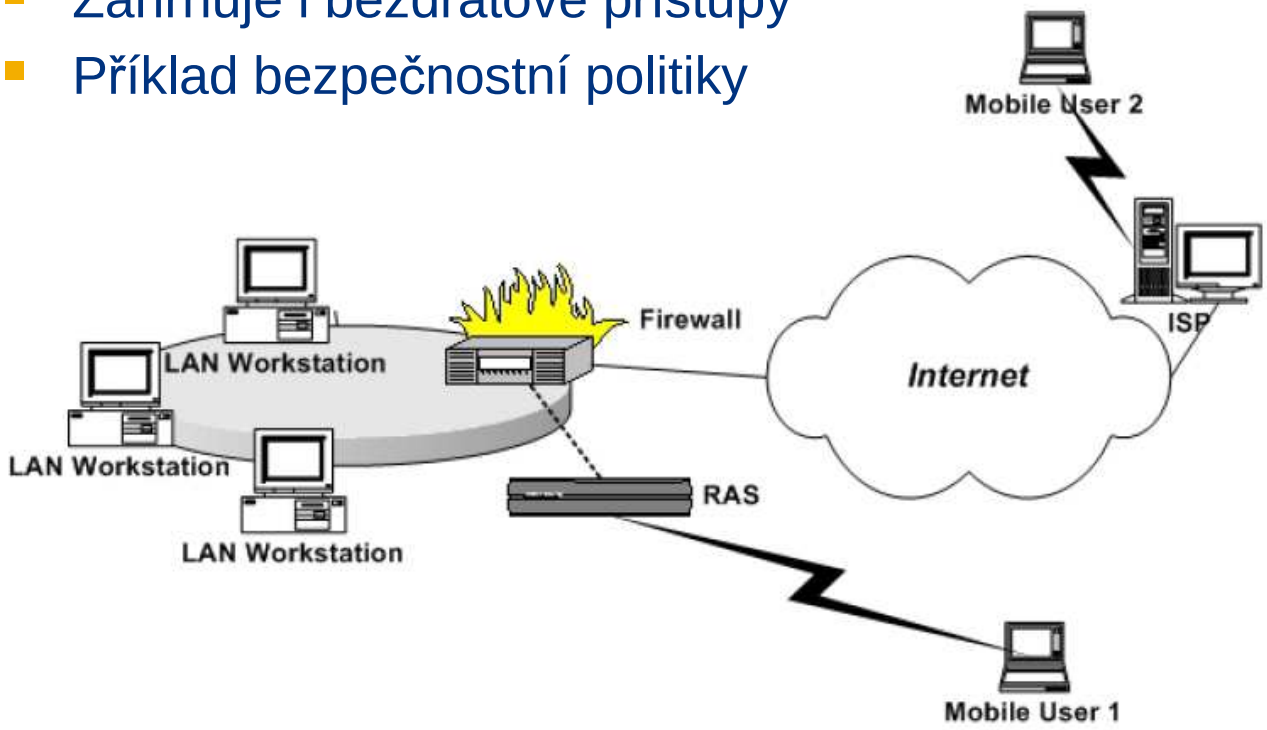
- Konfigurace
- Bezpečnostní vlastnosti a jejich nastavení
- Administrace
- Zaznamenávání událostí
- Dokumentace
- Audit
- Výcvik a vzdělávání

Bezpečný vzdálený přístup

ISO/IEC 18028-4:2004 – IT Network Security

Part 4: Securing remote access

- Upřesnění možných bezpečnostních technik, jejich výběr a provozování
- Zahrnuje i bezdrátové přístupy
- Příklad bezpečnostní politiky

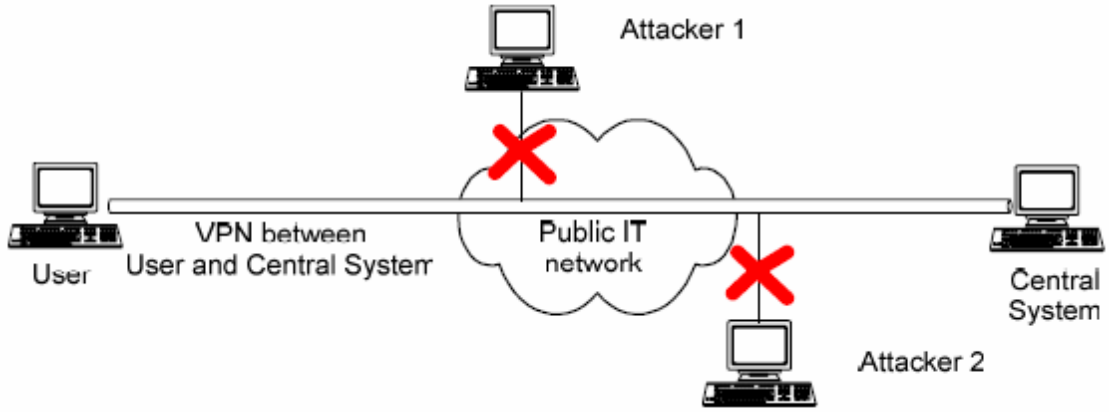


Použití virtuálních privátních sítí

ISO/IEC 18028-5:2005 – IT Network Security

Part 5: Securing communications across networks using Virtual Private Networks

- Cíle a požadavky na VPN
- Výběr a implementace VPN
- Techniky a protokoly pro budování VPN
  - 2. vrstva, 3. vrstva, vyšší vrstvy
  - FR, ATM, MPLS, PPP, L2F, L2TP, IPsec, SSL, SShell

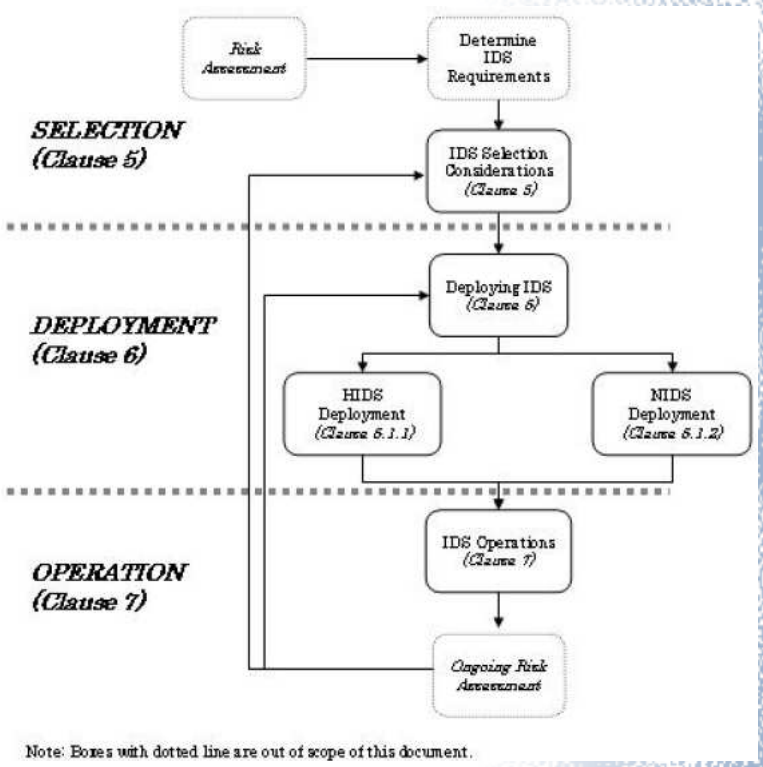


Výběr, nasazení a provoz IDS

ISO/IEC 18043:2006

Selection, deployment and operations of intrusion detection systems

- Výběr IDS
  - Ohodnocení rizik
  - Síťové a hostované IDS
  - Provozní souvislosti
  - Bezpečnostní politika IDS
  - Související nástroje (SIM, …)
- Nasazení IDS
  - Výhody/nevýhody různých typů
- Provozování IDS
  - Ladění IDS
  - Zvládání varování IDS
  - Typy a způsoby reakce



Zvládání bezpečnostních incidentů

ISO/IEC TR 18044:2004
Information Security Incident Management

- Plan – Příprava a implementace
  - Zavedení schématu a pravidla řízení bezpečnostních incidentů
  - Vybudování infrastruktury (procesy – lidé – nástroje)
  - Informování manažerů, zaměstnanců, uživatelů, …
- Do – Provoz monitoringu
  - Detekce, sběr informací pro došetření, pravidelné reportování
  - Reakce na incidenty a náprava případných škod
- Check – Kontrola přínosů a výstupů
  - Vyhodnocení a ponaučení z incidentů
  - Identifikování možností pro vylepšování preventivních opatření
- Act – Trvalé zlepšování bezpečnosti
  - Promítnutí výsledků do celkového managementu bezpečnosti
  - Vyšší objektivita podkladů pro analýzu a zvládání rizik
  - Optimalizace schématu řízení incidentů

Případová studie – poptávka

- Audit firewallů a IDS jako součást celofiremního auditu.
- Vymezení rozpočtu auditu odpovídajícímu práce 20 člověkodnů.
- Zadavatel požadoval provést:
  - zhodnocení architektury firewallů, pravidel a konfigurace firewallů s ohledem na současné hrozby, kterým společnost čelí
  - zhodnotit nasazení IDS s ohledem na konfiguraci firewallů a s ohledem na doporučení výrobce
  - zhodnocení dokumentace týkající se následujících procedur:
    - konfigurace a úprava firewallových pravidel
    - logický přístup k firewallům a IDS
  - zhodnocení monitorování logů firewallů a IDS
  - posouzení úplnosti a aktuálnosti provozní dokumentace

Nabídka

- Identifikace metodik a norem, které budou našim vodítkem
- Jasná specifikace nabídky, co a jak budeme auditovat – specifikace průběhu auditu
- Vzorkování – důležitý prvek všech auditů

Použité principy a metody

- Využití existujících norem a standardů
  - ČSN EN ISO 19011:2003 – Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu
  - ISO/IEC 18028 – bezpečnost sítí IT
  - ISACA, 2003, IS auditing procedure – Firewalls
  - ISACA, 2003, IS auditing procedure – Intrusion Detection Systems Review

ČSN EN ISO 19011:2003

- *Etické provedení* - základem profesionality jsou principy zachování důvěrnosti.
- *Objektivní prezentace* - zjištění auditu prezentovat pravdivě a přesně včetně všech překážek během auditu.
- *Princip práce podle nejlepšího vědomí a svědomí*.
- *Nezávislost* – auditor musí být nezávislý.
- *Audit jen podle důkazů* – při auditu je nutné vycházet z doložitelných skutečností tak, aby audit byl opakovatelný. Důkazy musí být verifikovatelné.

ČSN EN ISO 19011:2003

- *Zahájení auditu* – definování cíle, předmětu a kritérií auditu. Je definován auditní tým včetně jmenování hlavního auditora.
- *Přezkoumání dokumentace a příprava činností na místě* – prostudování existující dokumentace, příprava různých pracovních dokumentů (např. dotazníky).
- *Provádění auditu na místě* – jádro celého auditu, vlastní sběr informací o skutečném fungování systému, ověření zjištěných skutečností a shromáždění důkazů.
- *Příprava, schválení a distribuce zprávy z auditu* - důkladné vyhodnocení všech zjištěných skutečností, zformulování stručné a výstižné zprávy z auditu, oponentura zadavatelem, prezentace výsledků a následná diskuze se všemi odpovědnými manažery a administrátory.
- *Dokončení auditu* – vyhodnocení úspěšné i méně zdařilé stránky auditu.

Zahájení auditu

- Jmenování auditního týmu – na straně zadavatele i odběratele
- Jmenování vedoucího auditora
- Definování cílů a rozsahu auditu
- Žádost o dodání dokumentace (konkrétní dokumenty)
- Dohodnutí stupnice závažnosti nalezených skutečností

Přezkoumání dokumentace I

- Předložená dokumentace – velmi omezená a nedostatečná – některé body auditu buď není možné provést nebo je možné provést je pouze částečně.
- Nedodány především:
  - bezpečnostní politika firewallu (která by umožnila zhodnotit design firewallů a pravidla firewallů)
  - detailní analýza rizik a
  - projekt nasazení IDS, který by umožnil zhodnotit vhodnost nasazení IDS

- Princip auditu – založený na evidenci – opakovatelnost.

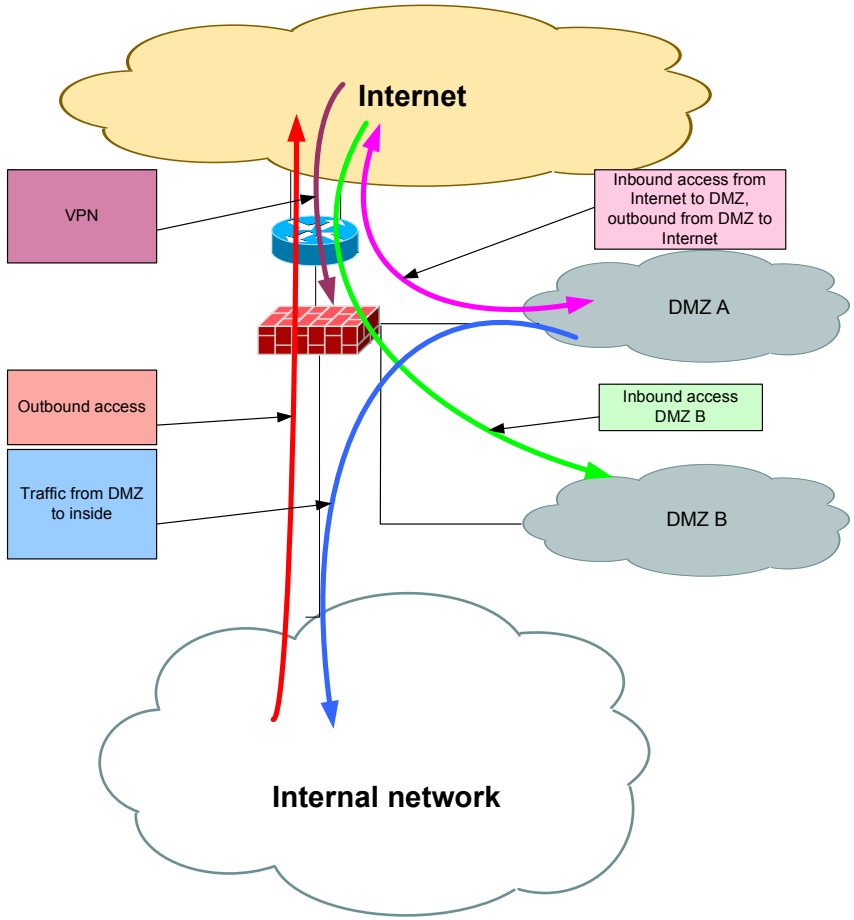
Přezkoumání dokumentace II

- Bylo evidentní, že správci svou síť znají.
- Interview – zformulování neformální politiky firewallu
- Interview – legální metoda sběru dat

- Přehodnocení plánu a rozsahu auditu:
  - IDS – audit výrazně zkrácen z důvodu nedostatečné dokumentace
  - kompenzace:
    - neformální politika firewallu
    - kostry dokumentů
    - doporučení ohledně monitorování bezpečnosti

Přezkoumání dokumentace III

- Neformální bezpečnostní politika firewallu – oponovaná zadavatelem



Audit na místě

- Principy – maximální objektivita
- Auditor by měl být:
  - přístupný názorům - je ochotný připustit jiné alternativy pohledu na věc
  - taktický při jednání s lidmi
  - vnímavý
  - jedná eticky
  - vytrvalý
  - otevřený
  - …

Audit na místě

- Firewally
  - zhodnocení pravidel firewallu s ohledem na IS bezpečnostní politiku
  - zhodnocení designu základních služeb chráněných firewallem (DNS, SMTP, HTTP, proxy); zhodnocení pravidel firewallu vztažené k těmto službám
  - zhodnocení architektury DMZs a firewallových pravidel vztažených k DMZ
  - zhodnocení procedur pro administraci firewallu (zhodnocení fyzického přístupu k firewallu a logických přístupových mechanismů)
  - zhodnocení procedur pro konfiguraci pravidel firewallu, procedur pro schvalování úprav pravidel, kvalitou komentářů
  - zhodnocení základní konfigurace jako operační systém, záplaty, směrování, NTP, …
  - zhodnocení konfigurace nižších vrstev (antispoofing, fragmentované pakety, …)
  - zhodnocení logování a alertování
  - zhodnocení pravidel zálohování
  - zhodnocení úplnosti a aktuálnosti provozní dokumentace

- IDS
  - zhodnocení úplnosti a aktuálnosti provozní dokumentace

Prezentace výsledků

- Předložení auditní zprávy
- Oponentura auditní zprávy (objektivita!!)
- Prezentace výsledků auditu formou workshopu
- Prezentace pozitivních i negativních zjištění!!

Výsledek

- Zákazník spokojený
- Auditoři – pocit dobře odvedené práce

- Normy a metodiky – dobrý zdroj informací
- Vodítko, check-list
- Samotné normy nestačí

Shrnutí

- Bezpečnost je dnes standardní součástí každého informačního a komunikačního systému
  - Ne všichni odborníci to chápou stejně
- Rozsáhlé odborné know-how, které odráží nejlepší praxi, je dostupné v mezinárodních standardech
  - Je potřeba mít představu o tom, z čeho je možné vybírat
- Využívání mezinárodních standardů není nevýhoda řešení, ale naopak prokazuje vysokou profesionalitu

Děkuji za pozornost.

ludek.novak@anect.com

to, co nás spojuje . . .

. . . je inovace a kvalita,

. . . jsou lidé a vztahy,

. . . je odpovědnost a důvěra,

. . . je vůle zlepšovat se.