Bezpečnost: kontroly, bezpečnostní politika, standardy

PV080

Vašek Matyáš

(část slajdů ve spolupráci s Evou Rackovou, KPMG)

Zásadní kroky pro zajištění bezpečnosti

1. Analýza hrozeb

2. Specifikace bezpečnostní politiky a architektury

3. Popis bezpečnostních mechanizmů

Kontroly

- Co vlastně dělat? (Analýza rizik)
- Jak to budeme dělat? (Bezpečnostní politika)
- Jaký systém použít? (Kritéria hodnocení bezpečnosti)
- Děláme to dobře? (Interní audit)
- Dělají to špatně? (Externí, příp. i vynucený audit)

Audit IT

- Naplánování auditu
- Dokumentace a posouzení kontrol
  - Důraz na dokumentaci, ne technologie!
- Výběr testů souladu a jejich provedení
  - Je dokumentace správná?
- Výběr a provedení speciálních testů
  - Skutečná kontrola funkčnosti
- Celkové posouzení systému

- Interní audit: Oddělení nezávislé na IT oddělení!

Připomínka: Od zranitelnosti k riziku

- ***Zranitelnost*** – slabé místo v systému
- ***Hrozba*** – akce/událost, která může ohrozit bezpečnost
  - potenciální využití zranitelnosti
- ***Riziko*** – pravděpodobnost, že se hrozba uplatní (zranitelnost využije)
  - Dva aspekty – pravděpodobnost a výše škody
- ***Útok*** – akt využití zranitelnosti (realizace hrozby)

Analýza rizik v IS obecně

- Často podle standardu pro řízení bezpečnosti (ISO/IEC 27002, dříve 17799, vznik z BS7799)
- Srovnání rizik a kontrol
  - Použití definované stupnice
  - Neoceňuje hodnoty
- Přístup odhadu podle informačních aktiv
  - Vhodnější pro společnosti kriticky závislé na IT a také společnosti se složitější kontrolou. Živnostníkovi stačí v méně formální postup srovnání rizik a kontrol.

Analýza rizik

- Zvážit, co všechno by mělo být chráněno
- Vyhodnotit, jaké hrozby hrozí ochraňovaným hodnotám.
  - Často nelze než vycházet z analýzy empirických poznatků o problémech v okolí, jiných útocích na podobné hodnoty atd.
- Chybně provedená analýza rizik má za důsledek téměř vždy chybně navržená bezpečnostní opatření. Hodnoty pak mohou být chráněny velmi nákladným, ale naprosto nesmyslným a neúčinným způsobem.

Analýza rizik

- Častěji spíše proces odhadu rizik – méně formální a podrobný než skutečná analýza
- Kvantitativní vs. kvalitativní
- Kvantitativní
  - Výstup je velmi srozumitelný
  - Nejčastěji výstup v $$$ (vystavení rizikům)
- Kvalitativní
  - Diskrétní stupnice (ne $$$)
  - Jednodušší postup, automatizovatelný, ale výsledky nejsou lehce srozumitelné

Analýza rizik – metoda ALE

- Annual Loss Expectancy
- ALE = SLE x ARO
- SLE – Single Loss Exposure
- ARO – Annualized Rate of Occurrence

Analýza rizik – BPA

- Business Process Analysis
- Širší pojetí rizik, nejen IT
  - Některá IT rizika tak mohou zůstat neidentifikována (pokud neovlivňují obchodní proces)
- Výstupy
  - Mapa procesů a jejich popisy.
  - Tabulka rizik (kvalitativní) a kontrol
  - Doporučení

CRAMM

- 1985 – Vláda UK – Risk Analysis and Management Method
- Strukturovaný přístup ve třech fázích:
  - Identifikace a ocenění hodnot.
  - Odhad hrozeb a zranitelností hodnot.
  - Výběr vhodných protiopatření.
- Analýza vcelku složitá, používá se zvláštní software a je zde velká časová náročnost, potřeba školených specialistů.

Několik poznámek k analýze rizik

- Sběr informací – dotazníky, pohovory atd.
- Kontrola úplnosti – formální kontroly, ale hlavně zkušenost hodnotitelů!!!
- Zpracování vstupních dat
  - polo/automatizované
- Zpráva s návrhy pro snížení rizik

Bezpečnostní politika

- Co a jak mají dosáhnout ochranná opatření.
- Cíl – minimalizace (kontrola) rizik.
- Strategie – jak dosáhnout cíle – použití bezpečnostních funkcí
  - Zahrnuje požadavky, pravidla a postupy, určující způsob ochrany a zacházení s ochraňovanými hodnotami.
- Většinou psána normálním jazykem, lze ale použít i nějaký druh formalismu.

Bezpečnostní politika

- Celková bezpečnostní politika
  - Určitá míra nezávislosti na použitých IT.
  - Citlivá data, zodpovědnosti, základ infrastruktury.
  - Horizont nad 5 let.
- Systémová bezpečnostní politika
  - Zohledňuje použité IT, konkretizace CBP.
  - Horizont obvykle cca 2-3 roky.
- Příp. další, specifické, politiky – provozní, personální, intranetová...

Bezpečnostní (IT) standardy

- Motivace
  - Kompatibilita, cena implementace a změn
  - Minimalizace problémů
- Standardy oficiální (vyžadovány zákonnými normami) – ČSNI, ISO
- Standardy průmyslové
- Kritéria hodnocení bezpečnosti

ISO/IEC 27002 I.

Dříve BS 7799:

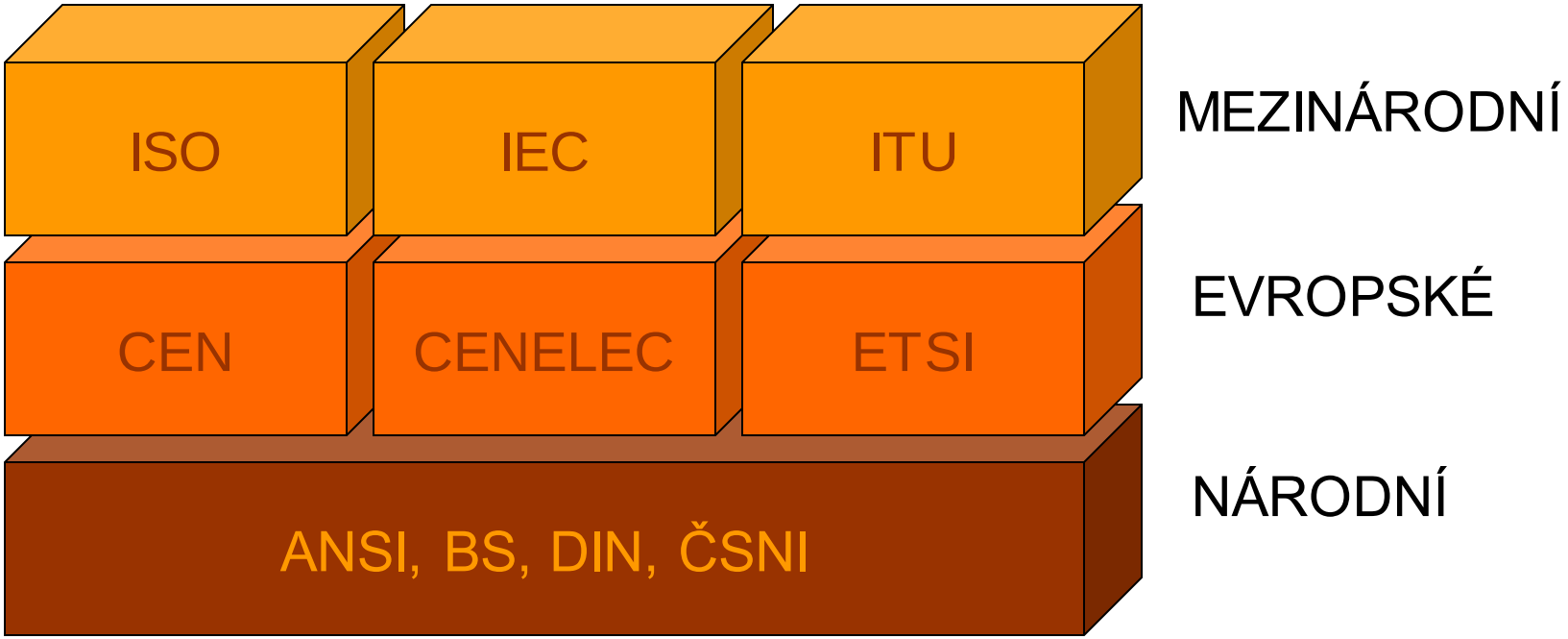
1. Code of Practice for Information Security Management – 1995
2. Specification for Information Security Management Systems – 1998

- Oba doplněny v roce 1999
- ISO/IEC standard 17799, i jako česká norma
- V roce 2007 jako ISO/IEC 27002, rev. 2013

ISO/IEC 27002 II.

- Vznik celé rodiny standardů 27k
- Tento se věnuje zásadám budování a využívání systému řízení bezpečnosti informací (Information Security Management System – ISMS)
- Model PDCA (Plan – Do – Check – Act) používaný např. v řízení kvality

Standardizační organizace



Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ)

- Dříve Český normalizační institut (1993-2008)
  - Státní příspěvková organizace, dnes přímo pod MPO
- Aktivity
  - tvorba, vydávání a řádné distribuce českých technických norem, normalizačních dokumentů a publikací
  - řídí a zabezpečuje státní metrologii podle zákona o metrologii,
  - autorizuje organizace k výkonům v oblasti státní metrologie a k úřednímu měření,
- Realita – normy (obecně) nejsou závazné – vynucování ad hoc specifickými opatřeními (zákon, nařízení aj.)

Pozor na trik – http://csni.cz/ ☺

- Všechny normy jsou k dispozici na úřadě. Pokud máte pocit, že jsou dohledatelné na internetu, tak je vaše domněnka špatná. Na internetu mohou být zveřejněny pouze normy, které se týkají změn či úplně nových norem.
- Zveřejnění jiných norem je trestné a nezákonné.
- Všechny vydané normy jsou platné a jejich dodržování je přísně sledováno a kontrolováno inspekcí.

Bezp. standardy ISO/ČSNI

- Základní standardy – bezpečnost OSI, bezp. architektura, mechanizmy autentizace entit...
- Přejmutí mezinárodních standardů – překlady
- Funkční standardy – jak aplikovat základní standardy
- Kritéria hodnocení bezpečnosti
- Odvětvové standardy a metodologie
- Vysvětlující dokumenty – slovníky, příručky atd.

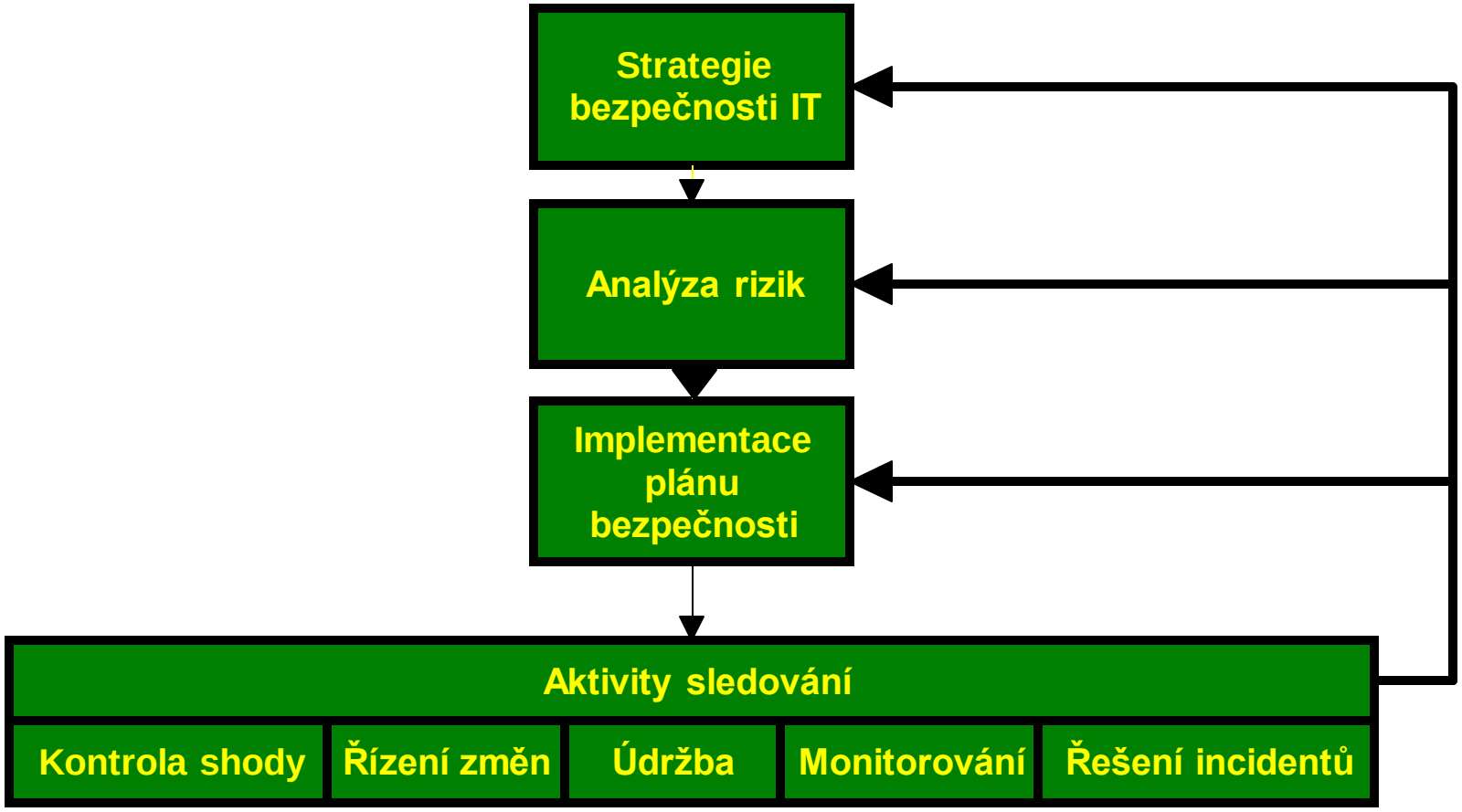
Standardy ISO

- Principy:
  - shoda: jsou vzaty úvahu názory všech zainteresovaných stran (výrobci, dodavatelé, uživatelé, spotřebitelská uskupení, testovací laboratoře, vládní orgány, výzkumná pracoviště)
  - globální řešení: musí vyhovovat požadavkům daného odvětví po celém světě
  - dobrovolnost
- Přezkoumávány alespoň jednou za 5 let
- Také prozatímní (interim) dokumenty

Srovnání ISO standardů v oblasti řízení bezpečnosti

	Systém řízení bezpečnosti	Seznamy protiopatření
ISO/IEC 27k	ANO	ANO
ISO/IEC TR 13335, Část 1-3	ANO	NE
ISO/IEC TR 13335, Část 4	NE	ANO
ISO/TR 13 569	NE	ANO (financial services)

ISO/IEC TR 13335



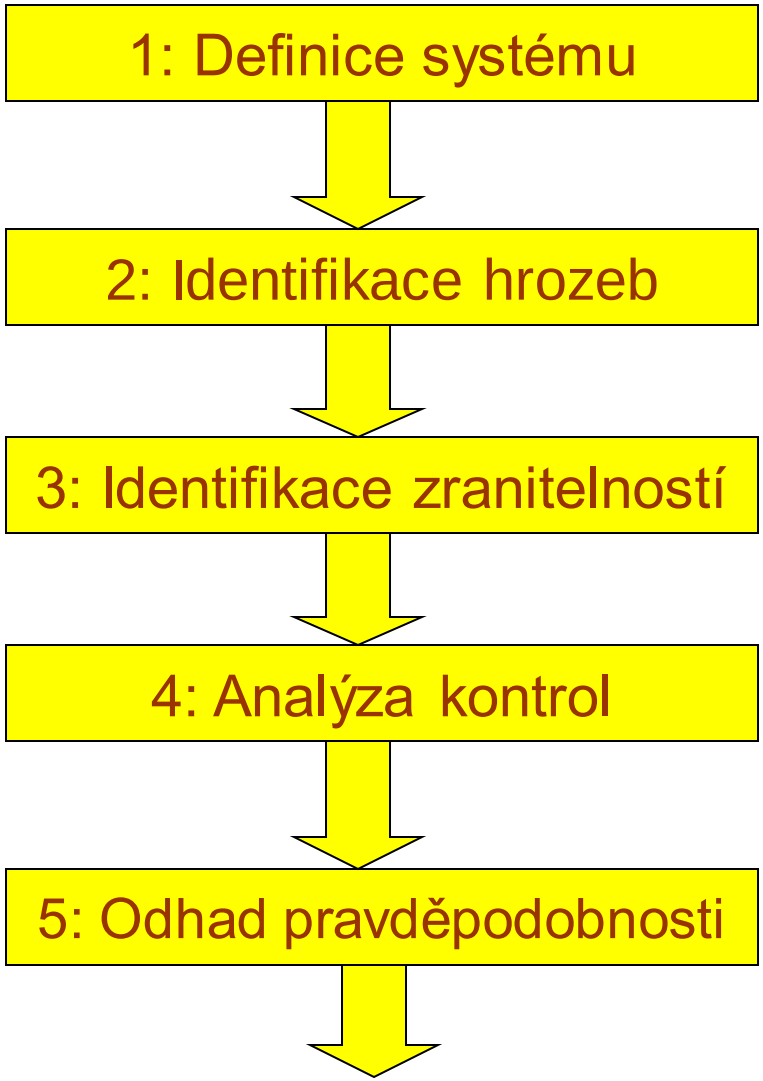
Standardy NIST – Special Publications

- 800-14: Generally Accepted Principles and Practices for Securing Information Technology
- 800-26: Security Self-Assessment Guide for Information Technology Systems
- 800-27: Engineering Principles for Information Technology Security
- 800-30: Guide for Conducting Risk Assessments
- 800-33: Underlying Technical Models for Information Technology Security
- SP 800-39: Managing Information Security Risk: Organization, Mission & Information System View
- SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations

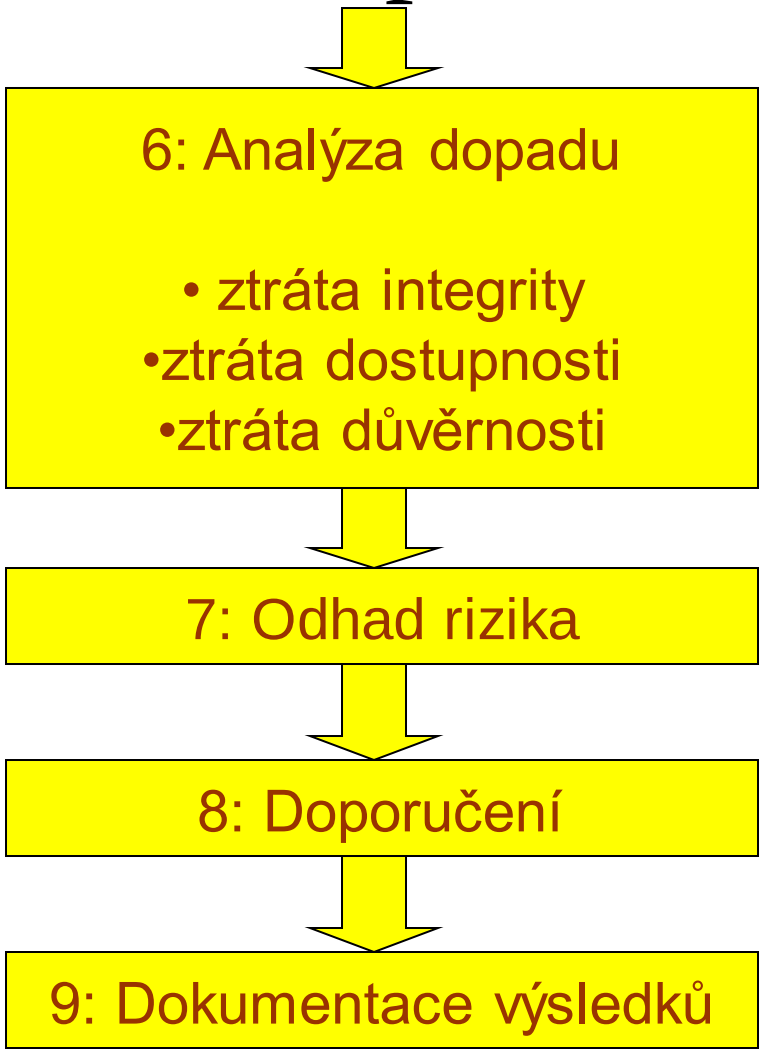
800-27: Engineering Principles for Information Technology Security

- A Baseline for Achieving Security
- 32 základních principů
  - předpokládejte, že externí zdroje nejsou bezpečné
  - usilujte o jednoduchost
  - identifikujte možné kompromisy mezi snížením rizika a vyššími náklady a snížením ostatních aspektů provozní efektivity
  - minimalizujte části systému, které musí být vysoce bezpečné
  - fyzicky nebo logicky oddělte kritické zdroje
  - neimplementujte nadbytečné bezpečnostní mechanizmy

800-30: Postup odhadu rizika



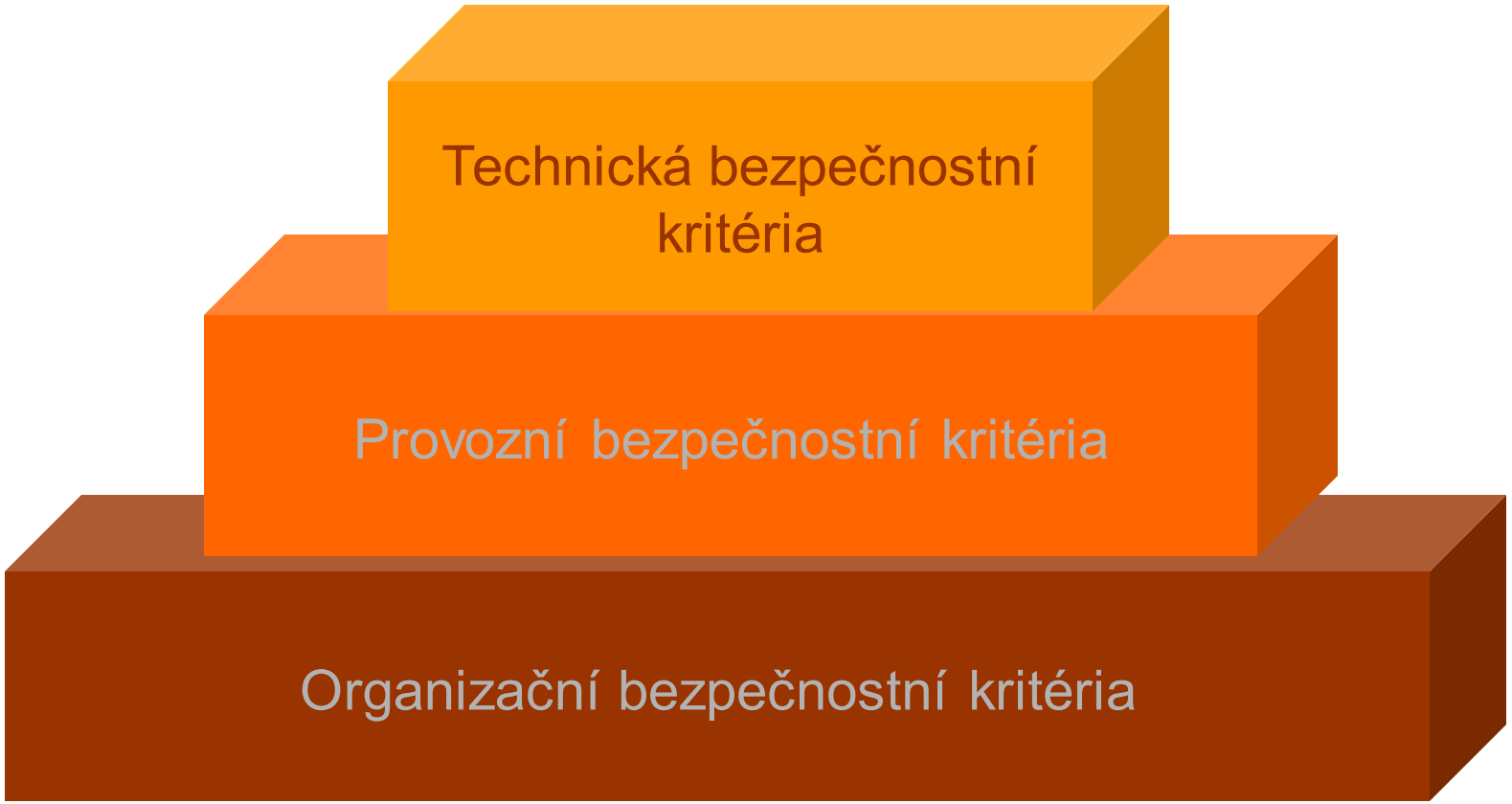
800-30: Postup odhadu rizika



2. Identifikace hrozeb
3. Identifikace zranitelností

Zranitelnost	**Aktivita hrozby**
Účty bývalých zaměstnanců nejsou vymazány ze systému	Vzdálený přístup k síti organizace a přístup k citlivým datům
Firewall umožňuje příchozí telnet službu a účet GUEST je aktivní na serveru XYZ	Využití služby telnet pro přístup k serveru XYZ
Dodavatel identifikoval slabiny v návrhu systému, ale zatím nejsou k dispozici opravy	Získání neautorizovaného přístupu k systému využitím slabin
Výpočetní středisko využívá automatické vodní hasicí zařízení a zároveň není k dispozici zařízení chránící hardware před poškozením vodou	Poškození výpočetní techniky vodou

4. Analýza kontrol



Organizační bezpečnostní kritéria

- Jednoznačné přiřazení odpovědnosti
- Průběžná podpora
- Schopnost reakce na incidenty
- Periodické prověrky bezpečnostních kontrol
- Prověřování zaměstnanců
- Analýza rizik
- Bezpečnostní a technická školení
- Rozdělení pravomocí a odpovědností
- Systém schvalování a autorizací
- Bezpečnostní plán

Provozní bezpečnostní kritéria

- Kontrola možného znečištění vzduchu (kouř, prach, chemické látky)
- Kontroly zajišťující stabilitu dodávky elektrické energie
- Přístup a datovým médiím a metody jejich likvidace
- Externí distribuce dat a jejich označování
- Fyzická ochrana objektů (např. výpočetního střediska, kanceláří)
- Kontroly vlhkosti
- Kontroly teploty
- Zabezpečení pracovních stanic, notebooků a počítačů

Technická bezpečnostní kritéria

- Ochrana komunikací (např. vzdálený přístup, propojení systémů, routery)
- Šifrování
- Kontrola přístupu
- Identifikace a autentizace
- Detekce průniku
- Opakované využití objektů
- Systémový audit

5. Odhad pravděpodobnosti

Pravděpodobnost	Popis pravděpodobnosti
Vysoká	Zdroj hrozby je vysoce motivován a dostatečně schopný, kontroly, které mohou zabránit zneužití zranitelnosti nejsou účinné
Střední	Zdroj hrozby je motivovaný a schopný, ale jsou implementovány kontroly, které mohou zdržovat nebo komplikovat úspěšné zneužití zranitelnosti
Nízká	Zdroj hrozby nemá dostatečnou motivaci ani dostatečné schopnosti nebo jsou implementovány kontroly, které mohou zabránit zneužití zranitelnosti, nebo ho alespoň významně zdržet

6. Analýza dopadu

Dopad	Definice
Vysoký	Využití zranitelnosti může: 1. způsobit značnou finanční ztrátu (ztrátou aktiv nebo zdrojů) 2. významně porušit, poškodit nebo zbrzdit cíle organizace, její pověst nebo zájmy 3. mít za následek závažné zranění nebo smrt osob
Střední	Využití zranitelnosti může: 1. způsobit významnou finanční ztrátu (ztrátou aktiv nebo zdrojů) 2. porušit, poškodit nebo zbrzdit cíle organizace, její pověst nebo zájmy 3. způsobit zranění osob
Nízký	Využití zranitelnosti může: 1. způsobit ztrátu některých aktiv nebo zdrojů 2. ovlivnit cíle organizace, její pověst nebo zájmy

7. Odhad rizika

Pravděp odobnost \ Dopad	Nízký (10)	Střední (50)	Vysoký (100)
Vysoká (1.0)	Nízké (10)	Střední (50)	Vysoké (100)
Střední (0,5)	Nízké (5)	Střední (25)	Vysoké (50)
Nízká (0,1)	Nízké (1)	Nízké (5)	Nízké (5)

Kritéria hodnocení bezpečnosti

- USA – konec 60. let a 70. léta – potřeba minimalizace nákladů na individuální hodnocení
- 1985 – Trusted Computer System Evaluation Criteria – “Orange Book”
  - Třída D – žádná bezpečnost
  - A1 – nejvyšší bezpečnost (matematický formalismus)

Vývoj kritérií

- Evropa – ITSEC – oddělení funkčnosti a záruk (plus metodologie – ITSEM)
- Kanada – CTCPEC – funkčnost rozdělena do skupin důvěrnost, integrita, zodpovědnost a dostupnost (plus krypto)
- US – Federal Criteria – vývoj zastaven
- **Společná kritéria** (Common Criteria) – celosvětový standard
  - ISO/IEC 15408

Pojmy

- **Akreditace** – oficiální souhlas (pověření) s prováděním určité činnosti
- **Certifikace** – vydání daného osvědčení na základě provedného hodnocení
- **Hodnocení** (evaluace) – ověření shody deklarovaných vlastností (dle kritérií)
- **Validace** – ověření platnosti/souladu, v US terminologii „hodnocení“ – viz výše

Důležité pojmy z CC

- **Předmět hodnocení** (*Target of Evaluation*, *TOE*) – produkt nebo systém (nebo jeho část), který je předmětem hodnocení
- **Specifikace bezpečnosti** (*Security Target*, ST) – cílová kombinace komponent spojených s konkrétním produktem nebo systémem
- **Profil bezpečnosti** (*Protection Profile*, *PP*) – implementačně nezávislá skupina bezpečn. požadavků určité skupiny TOE

Společná kritéria

- Zájem uživatelů, výrobců, hodnotitelů
- Profil bezpečnosti (čipové karty, biometriky, DBMS, poštovní razítkovače ap.)
  - „Minikritéria“ – katalogovány jako samostatný hodnotitelský dokument
  - Popisy bezpečnostních potřeb často různorodé ☹
- Security target (ST) – teoretický koncept/cíl
- Hodnocení TOE – odpovídá realita teorii (ST)?
- Požadavky na funkčnost a záruky

Význam a výhody kritérií

- Usnadňují nasazení a používání bezpečných systémů – jednodušší srovnávání a výběr podle skutečných potřeb
- Usnadňují specifikaci požadavků
- Ujasňují požadavky na návrh a vývoj

Základní krypto-standardy

- Symetrická kryptologie – (DES), AES
- Asymetrická kryptologie – šifrování, podpisy, výměna klíčů
  - IEEE P1363 – založené na faktorizaci, diskrétním logratimu, eliptických křivkách
  - NIST FIPS 186-3 – Digital Signature Standard
- Hašovací funkce – SHA-1, RIPEMD, (MD5), SHA-2 (SHA-224, -256, -384, -512)
  - Nedávno doběhla soutěž na SHA-3, více později

Kryptografické algoritmy

- Kritické pro většinu systémů
- Národní zájmy
- Desetiletí úmyslného opomíjení (bojkotování) tohoto tématu v procesu standardizace
- Zásadní pro nasazení DES – nepřímá podpora díky absenci jiných široce uznávaných standardů
- Proto i velké očekávání od AES

„Cvičení“ Advanced Encryption Standard

- Zprávy o veřejné soutěži od NIST – 1996
- Leden 1997 – Oficiální oznámení o projektu
- Září 1997 – Call for Proposals
- Srpen 1998 – oznámeno 15 kandidátů
- Srpen 1999 – 5 finalistů
- 2. října 2000 – Volba algoritmu
- Konec 2000 – První implementace (PGP 7.0.3)
- Listopad 2001 – FIPS 197

AES – Algoritmus Rijndael

- Vstup i výstup: bloky 128b
- Délka klíče: 128, 192 nebo 256 bitů
- Zpracování po bytech
- 10, 12 or 14 rund (podle délky klíče)
  - Přidání Initial Round Key
  - Poslední runda je mírně odlišná

Nová hašovací funkce SHA-3

- Délka prací dle očekávání jako AES
- *Listopad 2007: Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA–3) Family*
- http://www.nist.gov/hash-competition
- Nenahrazuje, ale doplňuje funkce v FIPS 180-2
- 64 návrhů, 16 slabých, 51 postoupilo do dalšího kola
- Kolo 2 (změny povoleny) – 14 kandidátů (mj. bez MD6)
- Finále s 5 finalisty (pochybnosti o jejich výběru)
- Vyhlášení vítěze v říjnu 2012 – Keccak (EU)
- Standard jako takový v srpnu 2015

Standardy aplikované kryptografie

- Digitální certifikáty – X.509 +
- PKCS standardy
- Bezpečnostní/krypto protokoly
  - Nízká úroveň – zákl. standardy (autentizace entit)
  - ISO/IEC – Key Management 11770, Non-repudiation 13888
  - IETF – PKIX, IPSEC, S/MIME

Hodnocení kryptografických prostředků

- použité kryptografické algoritmy
  - schválení převzetí jiných, obvykle mezinár.
  - kryptografický a kryptoanalytický rozbor nově navrhovaných algoritmů
- vlastní implementace kryptogr. algoritmů
- prostředí vlastní implementace
  - správa klíčů, kryptografické protokoly, autentizace uživatelů, odolnost produktu ap.

FIPS 140-1, 140-2 … 3(?)

- Hodnocení kryptografických modulů
  - SW, firmware, ale především HW!
- 4 bezpečnostní úrovně pro 11 požadovaných oblastí
- Verze 2 je jen mírnou změnou verze 1
- Program hodnocení podle *Cryptographic Module Program Validation*
- 2007 zveřejněn draft FIPS 140-3, pak odvolán
  - Náhrada ISO/IEC 19790:2012

Bezp. požadavky FIPS 140-1/2

- Specifikace modulu
- Rozhraní modulu
- Role
- Služby a autentizace
- Fyzická bezpečnost
- Bezpečnost O/S
- Správa klíčů
- Elektromagnetická inference/kompatibilita
- Provádění testování
- Záruky za návrh
- Metody pro zmírnění jiných útoků

FIPS 140-1/2

1. Použitý kryptoalgoritmus schválený ap., není fyzická bezpečnost (lze i SW na PC)
2. Detekce narušení, autentizace podle rolí, víceuživatelské systémy (CC CAPP, EAL2)
3. Nulování kritických hodnot při narušení krytů/dvířek, oddělené porty (EAL3)
4. Detekce průniku odkudkoliv, spolupráce se systémy na EAL4

Standardy

- Standardy umožňují dosažení základní „kvalitativní“ úrovně podobných produktů nebo systémů a jejich interoperabilitu
- Standardy soustředí zásadní poznatky
- Standardy lze použít jako měřítko pro hodnocení nebo srovnání

Volba konkrétního standardu

Standardů je nepřeberné množství proto,
aby si každý vybral podle své potřeby…

…a nevynalézal kolo znovu a znovu!

Úloha manažera bezpečnosti IT

- Zkušenost s bezpečností důležitá, ale...
- Umění přesvědčovat je zásadní!
- Zkušenost: 60 % manažer, 40 % expert
- Místo velmi náročné
  - Kritizován za bezpečnostní incidenty
  - Kritizován za obstrukce "normálnímu" chodu
  - Jak může být oceněn za "nic se neděje!"? ☺