AoM33PIS - Průmyslové informační systémy

Přednáška č. 13

18. 5. 2016

Katedra Kybernetiky K13133
Centrum znalostního managementu K13393

Agenda

- Bezpečnost informací
- Rizika IT
- Bezpečnost při vývoji informačních systémů
- Bezpečnostní normy a standardy
- Výhled do budoucna

Motto

Celý systém je tak bezpečný, jako je bezpečný jeho nejslabší článek!

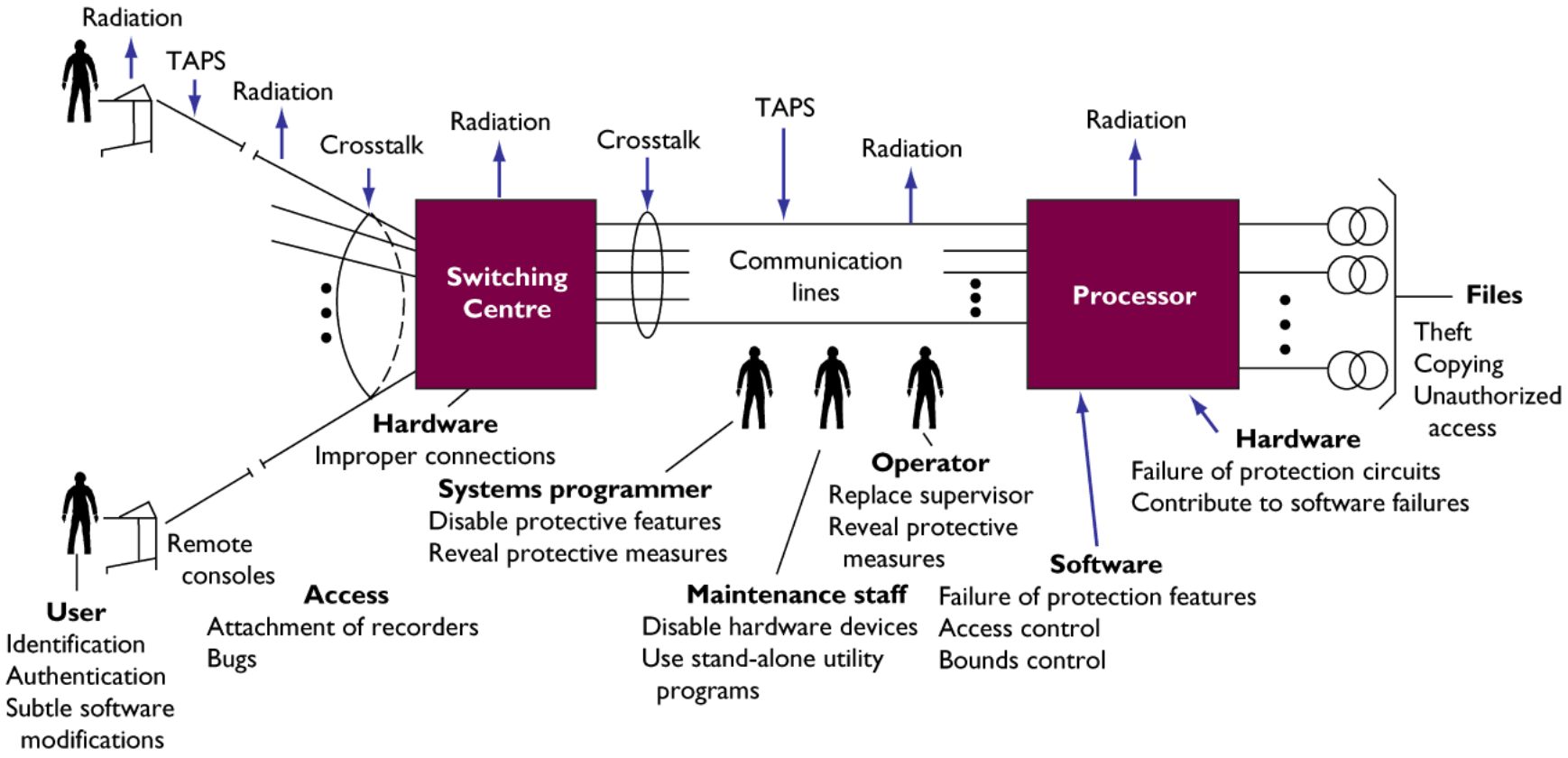
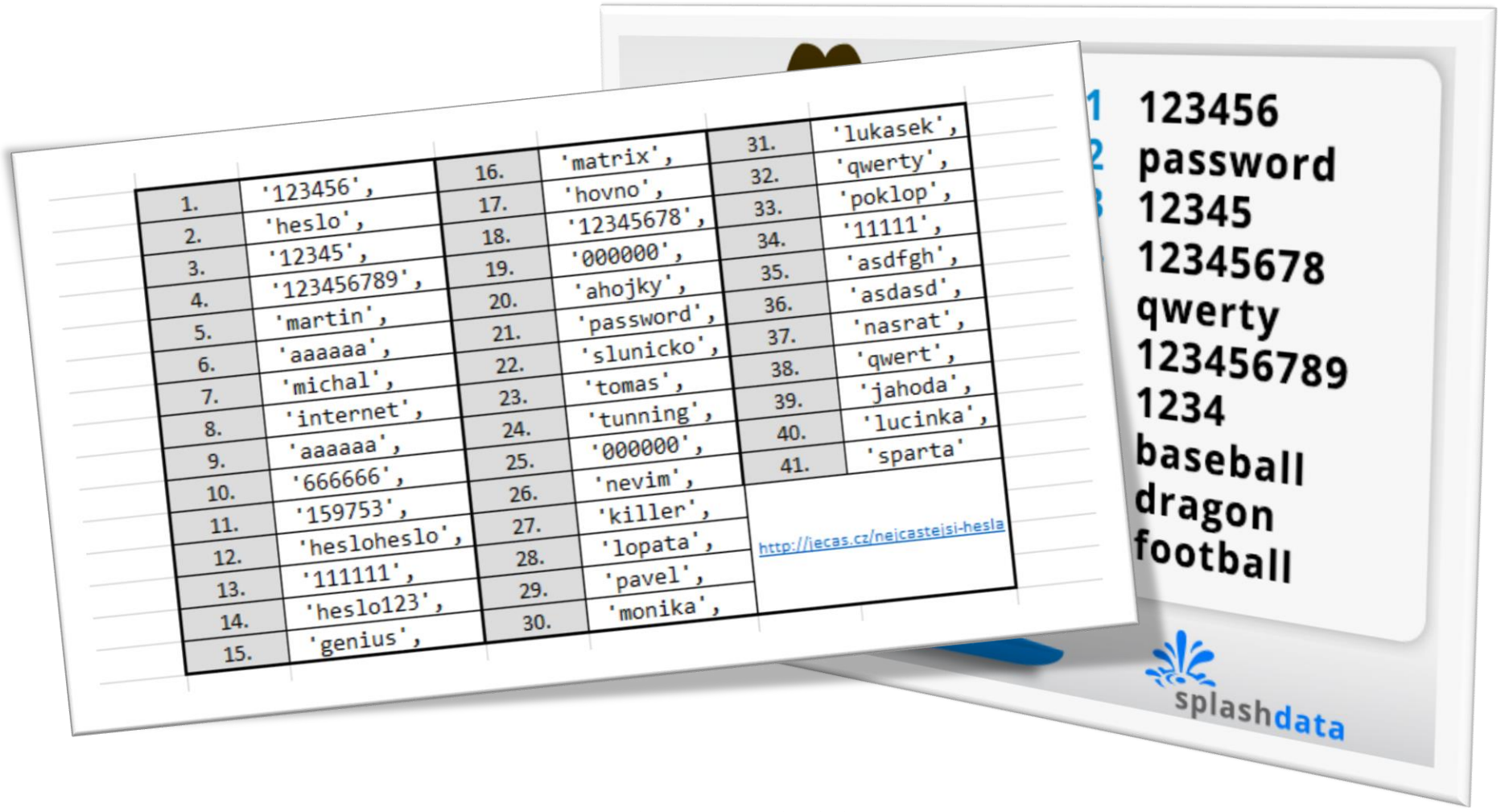


Figure 11.1 Telecommunications network vulnerabilities. Telecommunications networks are highly vulnerable to natural failure of hardware and software and to misuse by programmers, computer operators, maintenance staff, and end users. It is possible to tap communications lines and illegally intercept data. High-speed transmission over twisted wire communications channels causes interference called crosstalk. Radiation can disrupt a network at various points as well.

Nejoblíbenější hesla



1.	'123456',	16.	'matrix',	31.	'lukasek',
2.	'heslo',	17.	'hovno',	32.	'qwerty',
3.	'12345',	18.	'12345678',	33.	'poklop',
4.	'123456789',	19.	'000000',	34.	'11111',
5.	'martin',	20.	'ahojky',	35.	'asdfgh',
6.	'aaaaaa',	21.	'password',	36.	'asdasd',
7.	'michal',	22.	'slunicko',	37.	'nasrat',
8.	'internet',	23.	'tomas',	38.	'qwert',
9.	'aaaaaa',	24.	'tunning',	39.	'jahoda',
10.	'666666',	25.	'000000',	40.	'lucinka',
11.	'159753',	26.	'nevim',	41.	'sparta'
12.	'hesloheslo',	27.	'killer',		
13.	'111111',	28.	'lopata',		
14.	'heslo123',	29.	'pavel',		
15.	'genius',	30.	'monika',		

http://iecas.cz/nejcastejsi-hesla

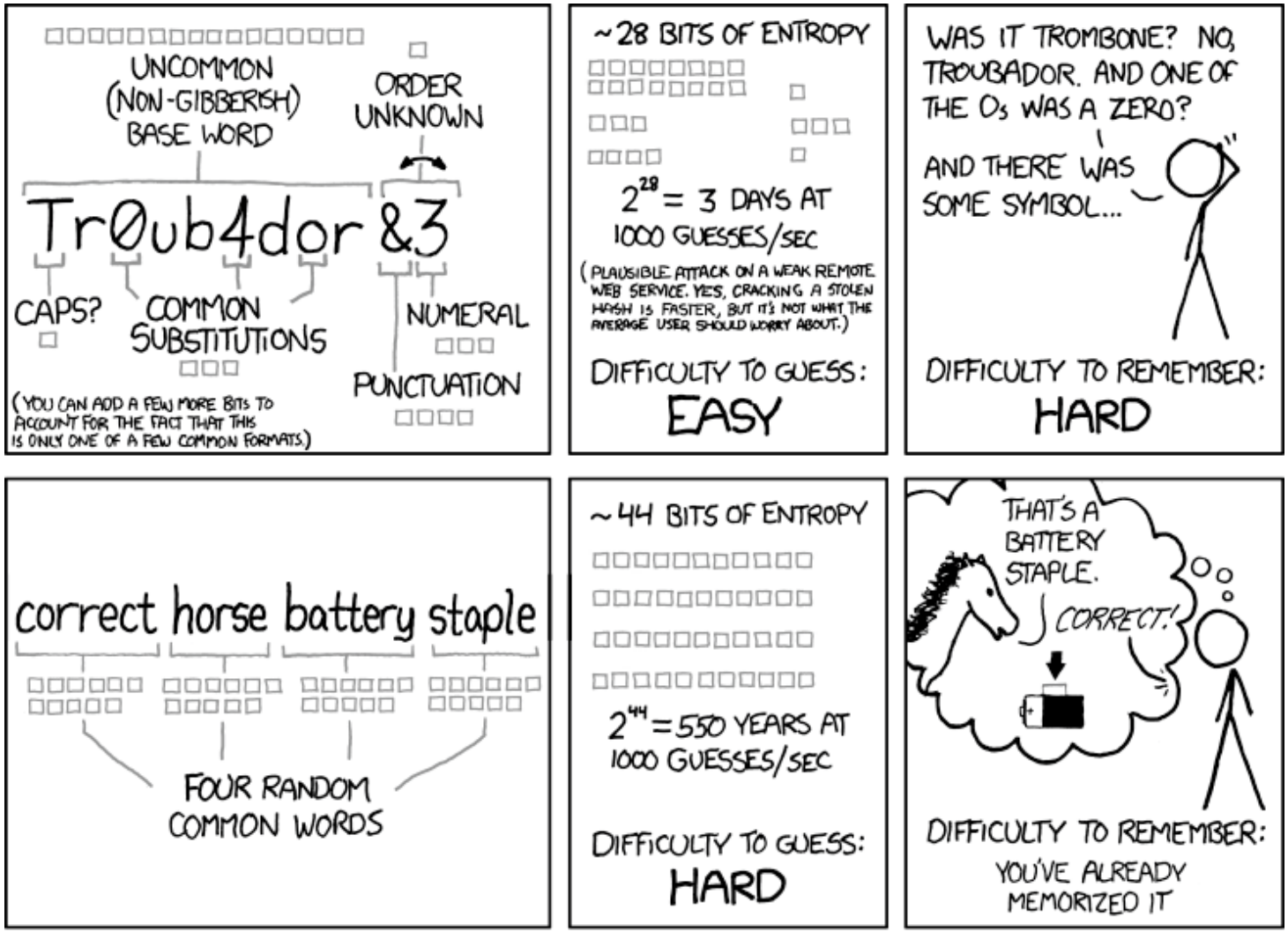
1 123456
2 password
3 12345
12345678
qwerty
123456789
1234
baseball
dragon
football

splashdata

Kvíz bezpečného hesla

- Heslo první: *cVa-2h!u*
- Heslo druhé: *sKakalpEspResoVes*

Co je bezpečnější a PROČ?



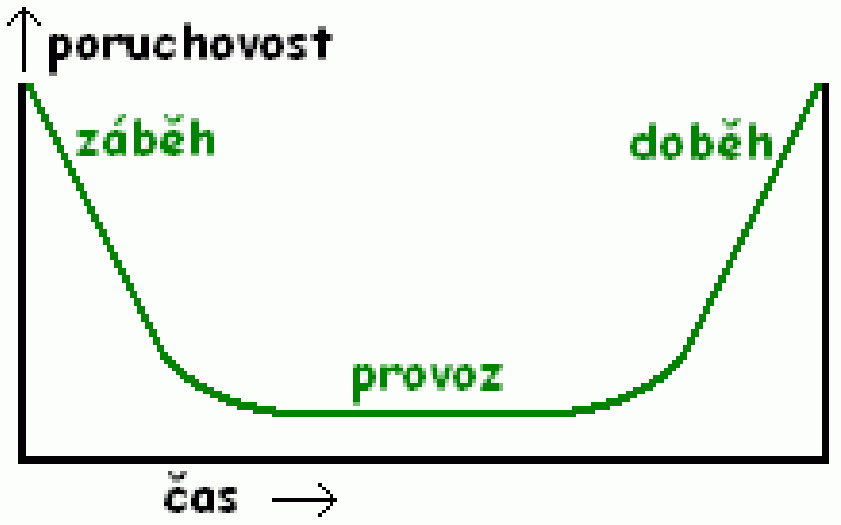
http://xkcd.com/936/

Základní pojmy bezpečnosti

- **Aktivum**
  - *„Něco“, co má pro držitele hodnotu.*
- **Hrozba**
  - *Skutečnost nezávislá na vůli majitele aktiva.*
- **Riziko**
  - *Výslednice působení hrozby na aktivum.*
- **Zranitelnost**
  - *slabé místo aktiva, nebo skupiny aktiv, které může být využito hrozbou.*
- **Dopad**
  - *výsledek nežádoucího incidentu.*

Míra hrozby

- Při stanovení míry hrozby zohledňujeme:
  - četnost výskytu hrozby (viz statistiky),
  - příležitost (lze ovlivnit organizačními a technickými opatřeními),
  - motivace útočníka,
  - nezbytné schopnosti útočníka,
  - náklady realizace hrozby,
  - nároky na hw/sw vybavení útočníka,
  - časová složitost,
  - atraktivita aktiva,
  - stáří aktiva („vanová“ křivka rizika),
  - počet uživatelů s přístupem.



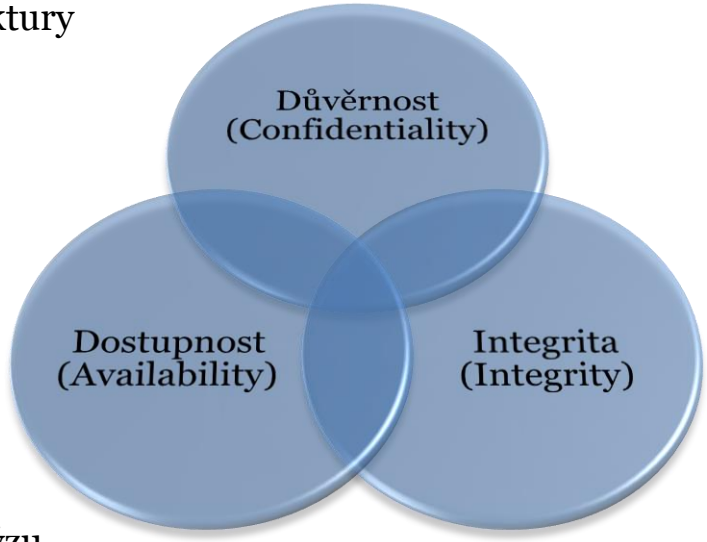
3 sudičky posuzování bezpečnosti informace

- **Důvěrnost**
  - *K informaci se dostane právě jen ten, kdo je oprávněn.*
- **Integrita**
  - *Informaci mohu důvěřovat.*
- **Dostupnost**
  - *K informaci se dostanu, když to budu potřebovat.*

- **Čtvrtá vzadu** – *nepopiratelnost původu.*

C-I-A: Důvěrnost-Integrita-Dostupnost

- **Důvěrnost**
  - zajištění, že informace jsou dostupné pouze oprávněným uživatelům.
  - řešení: organizačními opatřeními (klasifikace např. veřejné/interní/důvěrné) a technickými prostředky (hierarchie přístupových práv, šifrování)
- **Integrita**
  - zajištění správnosti a úplnosti informací, přičemž k nežádoucí změně dat může dojít
    - technickým selháním, náhodou, nebo úmyslně
  - řešení: logováním všechny změn; použití vícevrstvé architektury (data šifrována aplikací před uložením do db, v aplikaci kontrola hash fcí).
- **Dostupnost**
  - zajištění, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby, parametrizována
    - dostupnost v % za rok
    - RTO (Recovery Time Objective) - za jak dlouho po výpadku musí být systém funkční (časová tolerance výpadku)
    - RPO (Recovery Point Objective) - kolik hodin práce, resp. Objem dat, může být ztraceno (objemová tolerance výpadku)
  - RTO a RPO jsou základní kritéria pro business impact analýzu



Kategorizace IT hrozeb

- Hrozba - náhodná nebo úmyslně vyvolaná událost, která může mít negativní dopad na ***důvěrnost***, ***integritu*** a ***dostupnost*** aktiv. Kategorizace IT hrozeb:
  - Podle úmyslu:
    - náhodné hrozby (accidental threat);
    - úmyslné hrozby (deliberate/intentional threat).
  - Podle zdroje:
    - vnitřní hrozby (internal/insider threat);
    - vnější hrozby (external/outsider threat).
  - Podle dopadu na systém:
    - aktivní hrozby (active threat) – dochází ke změně stavu systému v důsledku narušení integrity a dostupnosti
    - pasivní hrozby (passive threat) – nedochází ke změně stavu systému, dochází k úniku informací (e-mail, internet.úložiště, webové aplikace, soc.sítě, chat, instant messaging; přenosná média; notebooky; tisk)
  - Podle dotčeného aktiva:
    - prostory, lidé, hw, sw, síť, média, data

Hranice soukromého

- **Hranice fyzická**
  - Privátní síť
  - Veřejné sítě (Internet)
  - Část privátních zdrojů určená ke zveřejnění (DMZ)
  - Řízení pohybu mobilních zařízení s citlivými daty

- **Hranice logická**
  - Pouze pro vyjmenované osoby
  - Interní (vnitrofiremní)
  - Důvěryhodní partneři (zákazník, dodavatel, stát)
  - Anonymní veřejnost

Rizika veřejných dat

- Veřejné informace nemají rizika spojená s důvěrností
- Velký potenciál pro narušení integrity
- Obtížně se stanoví rozdíl mezi
  - Cílenou dezinformací
  - Omylem
  - Útokem na pravdivost
- Zneužívání cizího obsahu (autorská práva)

- Jiná oblast: Soukromé informace na veřejných portálech
  - Facebook, chat, blog
  - Inzerce
  - Nevysychající studnice zneužitelných informací

Rizika soukromého

- Soukromým myslíme především firemní soukromí.
- Z výzkumů priorita (podle IT manažerů)
  1. Ztráta dat
  2. Omezení dostupnosti služeb (pro uživatele rovno ztrátě dat)
  3. Vynesení informace „insiderem“
  4. Problémy s kvalitou interních programů
  5. Viry, červy
  6. Napadení cíleným útokem zvenčí

- Rizika řešená IT nejsou vždy bezpečnostní.
- Po provedení analýzy rizik mnohdy dochází ke změně pořadí.

Mediální obraz a skutečnost

- Mediálně podávané problémy bezpečnosti: Hackeři, viry, bankomaty, phishing.

- **Realita**: Výše uvedené je jen malý zlomek péče o bezpečnost.
- Reálné pracovní úkoly
  - Ztráta zálohy.
  - Vynesení informace „vnitřním nepřítelem“.
  - Sabotáž.
  - Ztráta mobilního zařízení s citlivými daty.
  - Vypracování předpisů, audit, obhajoba před externím auditem.

Vliv velikosti subjektu

- Malé podniky (do 100 osob) a korporace řeší velmi odlišnou problematiku.
- V malém podniku funguje personifikace
  - Lidé se navzájem znají.
  - Každý zná kolegu, kterého potká na chodbě .
- V korporaci nastupuje davová anonymita
  - Znám pouze lidi, se kterými se stýkám.
  - Znám kolegu z USA, ale nevím, kdo sedí o patro výš.

- V malém podniku může fungovat „selský rozum“
- Korporace potřebuje systém, proces, definované postupy.

Vzor živnostník

- Pocit „není tu co ukrást“
- Velmi cenově citlivý
- Hlavní předmět podnikání nebývá závislý na IT
- Informační bezpečnost bývá zcela opomíjena

- O to horší je situace, když k něčemu dojde
  - 90% jsou ztráty dat
  - 9% viry a jiná havěť
  - 1% vše ostatní

Vzor banka

- Životně závislá na datech v počítačích
- Silný vnitřní i vnější nepřítel
- Silná role auditu (vnitřní i vnější)
- Neochota vlastníků dat převzít za ně odpovědnost
- Komplikované prostředí

- Prakticky neexistuje nevratná ztráta dat
- Strach z neúspěchu při auditu
- Všudypřítomný alibismus a neochota k osobní odpovědnosti

Role CISO

- **CISO = Chief Information Security Officer**
- Osoba (role) odpovědná za **řízení** informační bezpečnosti
- Identifikuje a katalogizuje informační aktiva
- Řeší strukturu vlastnictví dat (sám není vlastník)
- Stanovuje cíle a politiku informační bezpečnosti

- Výkon je úlohou IT operativy a případně ostatních
- Kontrola je úlohou auditora

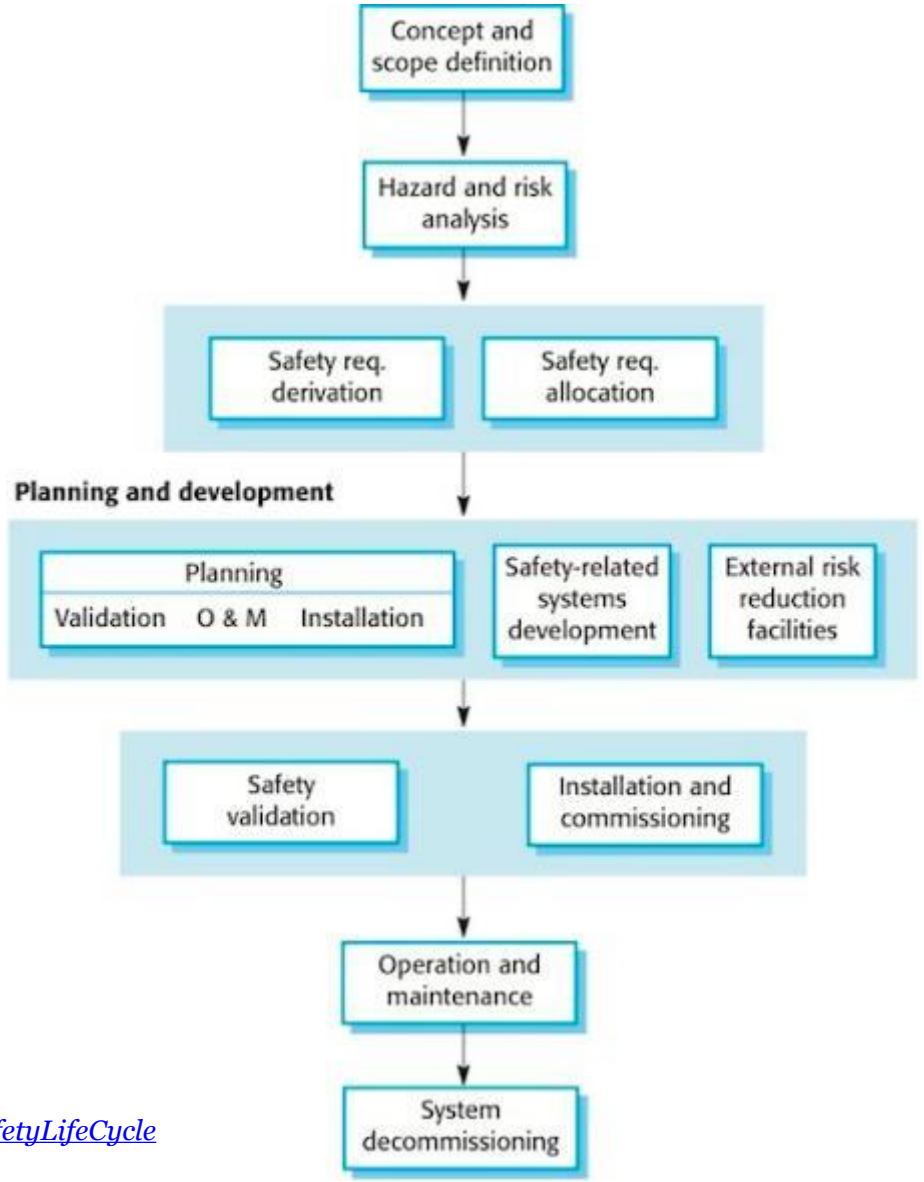
- Role podle definice neslučitelná s rolí IT manažera

Věčné dilema IT manažera

- **Funkčnost nebo bezpečnost?**
- Snadnost použití a zabezpečení jsou mnohdy proti sobě
  - *Bezpečnost uživatele obtěžuje*
- Když dojde k narušení bezpečnosti, je vina svalována na IT
  - *Neexistuje strukturální podpora*
  - *Neví se, co a jak chránit*
- Mnohdy intuitivní přístup z vlastní inciativy

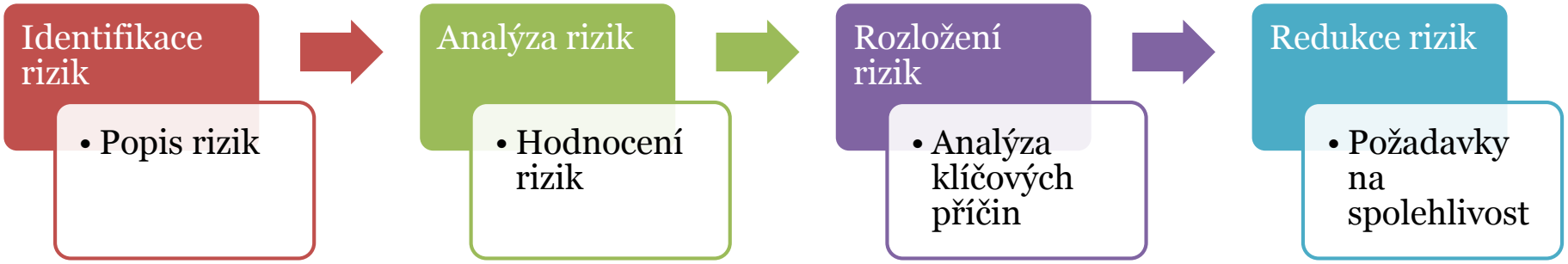
- Existují kladné výjimky, obzvlášť velké korporace a banky

The IEC 61508 safety life cycle



Zdroj: http://www.softwareengineering-9.com/Web/SafetyLifeCycle

Rizika a jejich vliv na návrh/realizaci systému



Zdroj: http://www.softwareengineering-9.com/

Matice rizik

LIKELIHOOD (probability) **How likely is the event to occur at some time in the** *(Linear Scale time specific matrix)*	**CONSEQUENCES** **What is the Severity of injuries /potential damages / financial impacts (if the risk event actually occurs)?** *(Logarithmic Scale, property industry specific matrix)*				
	Insignificant	Minor	Moderate	Major	Catastrophic
	No Injuries First Aid No Envir Damage << $1,000 Damage	Some First Aid required Low Envir Damage << $10,000 Damage	External Medical Medium Envir Damage <<$100,000 Damage	Extensive injuries High Envir Damage <<$1,000,000 Damage	Death or Major Injuries Toxic Envir Damage >>$1,000,000 Damage
Almost certain - expected in normal circumstances (100%)	MODERATE RISK	HIGH RISK	HIGH RISK	CRITICAL RISK	CRITICAL RISK
Likely – probably occur in most circumstances (10%)	MODERATE RISK	MODERATE RISK	HIGH RISK	HIGH RISK	CRITICAL RISK
Possible – might occur at some time. (1%)	LOW RISK	MODERATE RISK	HIGH RISK	HIGH RISK	CRITICAL RISK
Unlikely – could occur at some future time (0.1%)	LOW RISK	MODERATE RISK	MODERATE RISK	HIGH RISK	HIGH RISK
Rare - Only in exceptional circumstances 0.01%)	LOW RISK	LOW RISK	MODERATE RISK	MODERATE RISK	HIGH RISK

Zdroj: http://www.risk8.com

Bezpečnost je automaticky zahrnuta?

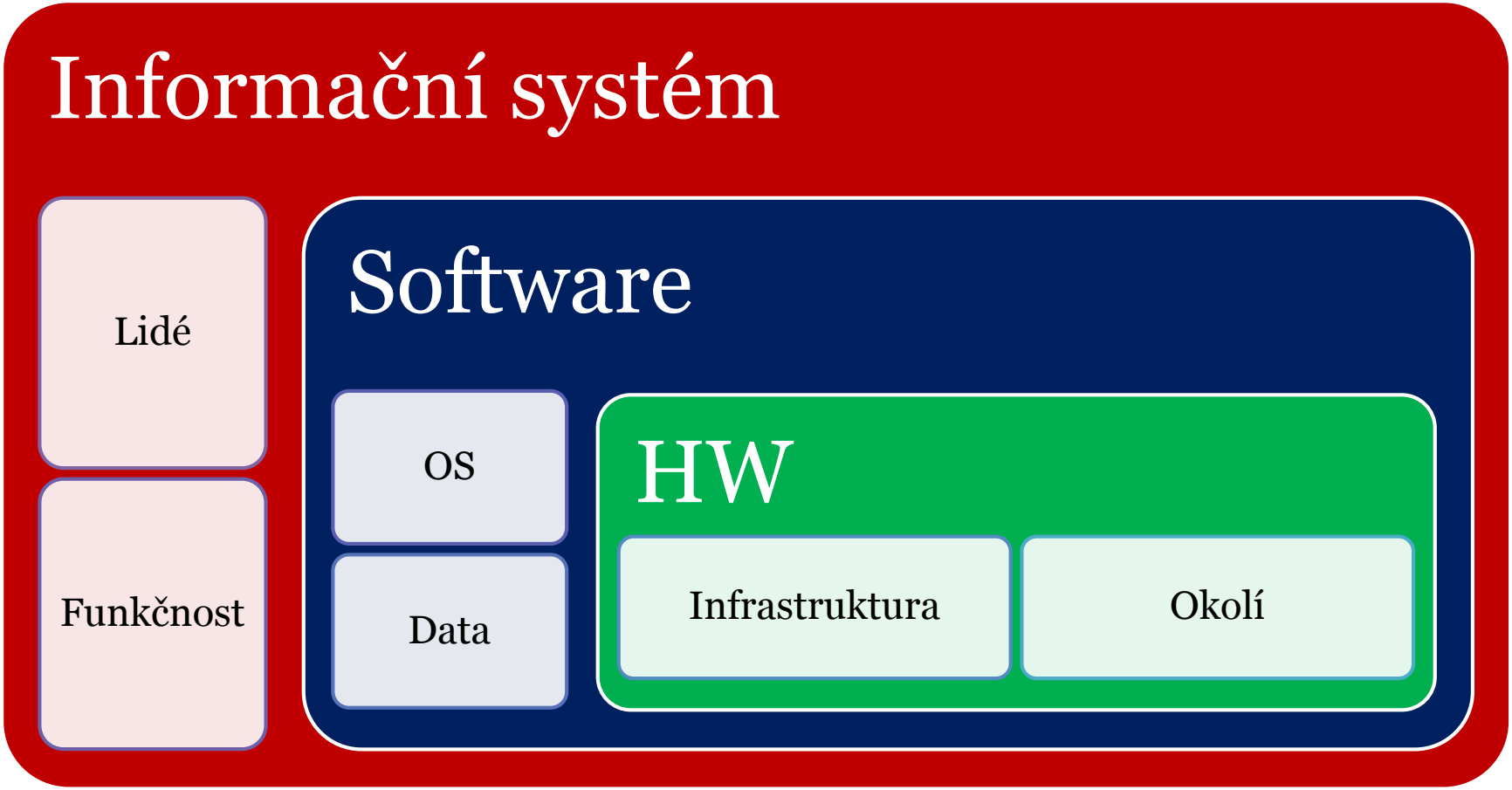
- ***Okřídlená věta ředitelů:***

„Je to počítač (systém, síť …), stálo to strašně MOC peněz, tak očekávám, že to SAMOZŘEJMĚ bude BEZPEČNÉ samo od sebe.“

- **Co s tím?**
  - *Edukace*
  - *Zavedení systému (ISMS, proces)*
  - *To však znamená NÁKLADY navíc !*

  - *Výsledek: Rezignace dodavatele a zahrnutí bezpečnosti do ceny?*

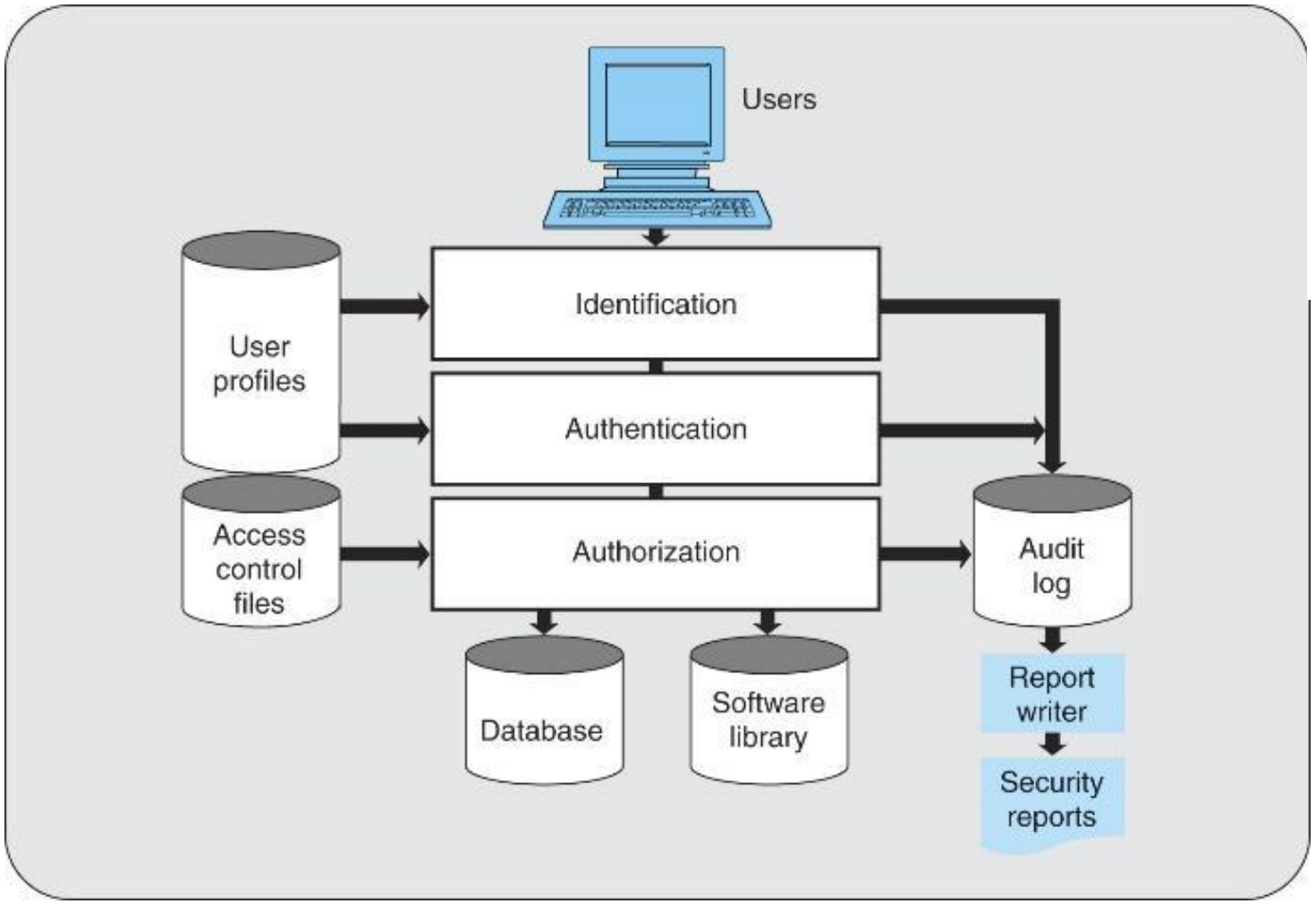
Bezpečnost v informačních systémech



Řízení zabezpečení systémů

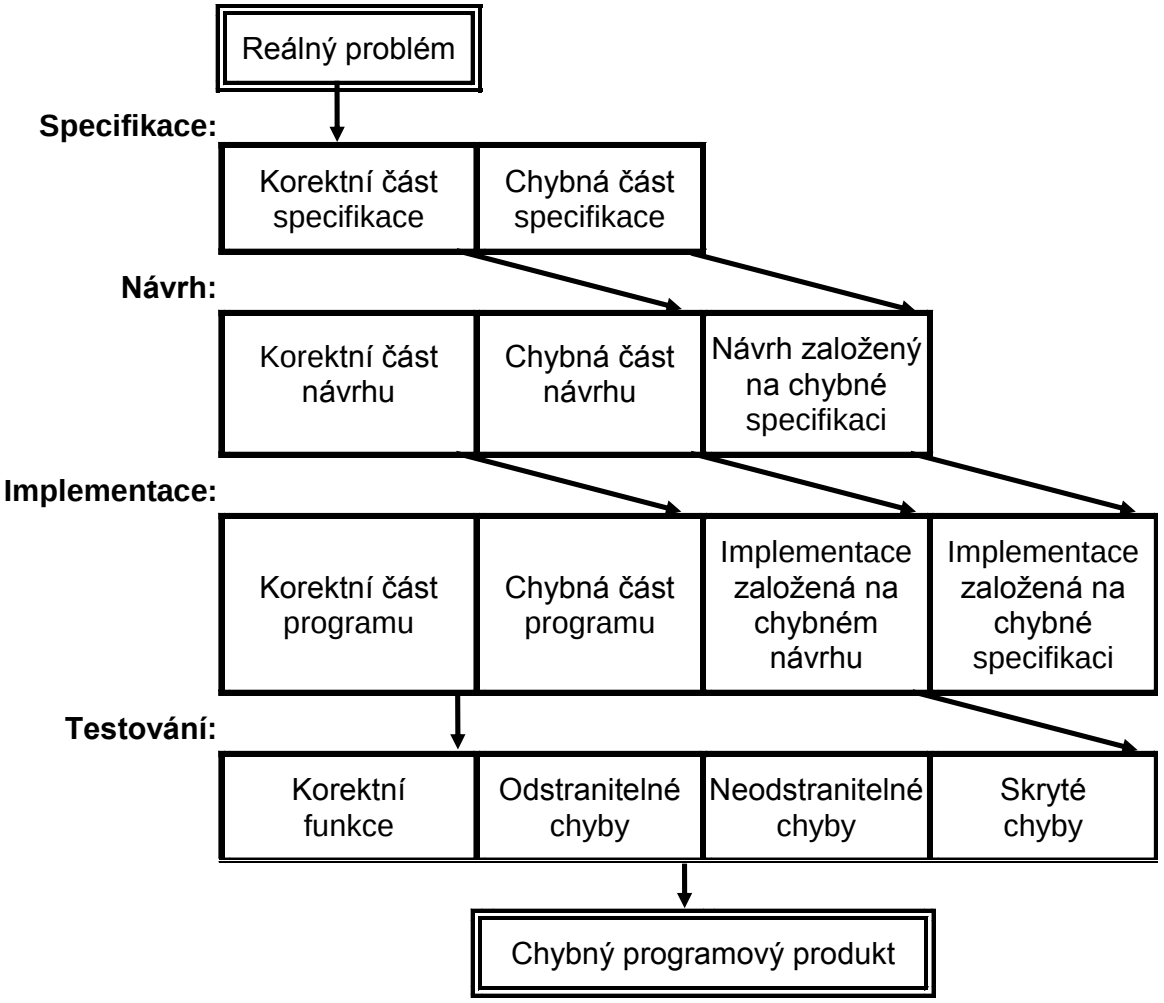
1. **Správa uživatelů a oprávnění**
   a. Vytvoření a správa vhodných přístupových mechanismů.
   b. Přidávání / odebírání uživatelů do / z systému.
   c. Nastavování odpovídajících přístupových práv.
2. **Nasazení a údržba systému**
   a. Instalace a konfigurace všech součástí systému (včetně OS a middleware) s ohledem na bezpečnost.
   b. Pravidelná aktualizace a instalace bezpečnostních oprav.
3. **Monitorování, detekce a zotavení z útoků**
   a. Monitoring a detekce neautorizovaného přístupu, strategie obrany a reakce na útoky.
   b. Strategie zálohování a obnovy do rutinního (normálního) provozu.

Správa uživatelů a oprávnění



Source: Ken Cutler, "Hackers, Viruses, Thieves, and Other Threats to Your Information Assets," in *Computer Security Seminar Course Material* (New York: ACM, 1991).

Kumulace chyb při vývoji SW

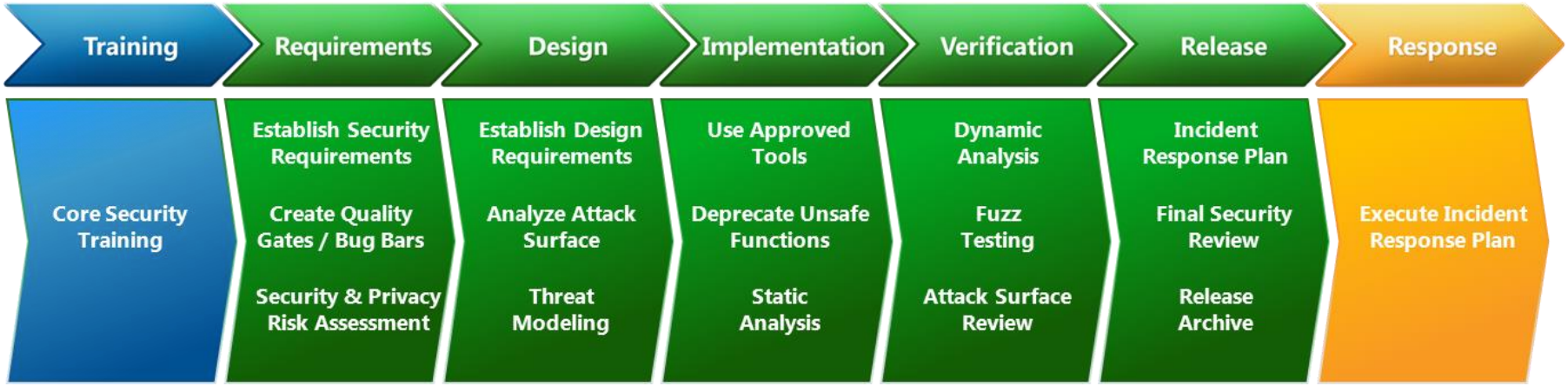


Metody kontroly zabezpečení systémů

- **Validace založená na zkušenostech**
  - Sestavení validačního týmu expertů.
  - Testování na základě znalostí a zkušeností členů týmu.
- **„Tiger teams“**
  - Sestavení „útočného“ týmu expertů.
  - Tým má za úkol „narušit“ systém formou simulace útoků.
- **Validace za použití nástrojů**
  - Použití nástrojů pro kontrolu zabezpečení.
  - Například: https://www.owasp.org/index.php/Appendix_A:_Testing_Tools
- **Formální verifikace**
  - Verifikace systému s ohledem na formální specifikaci bezpečnosti.

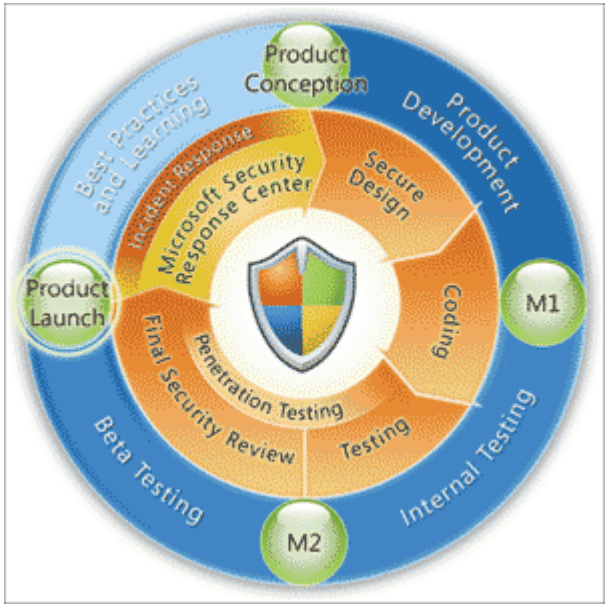
Metodiky bezpečného vývoje

Microsoft®
Security Development Lifecycle



Zkušenosti z bezpečného vývoje SW

- It's Not Just the Code
- Fix Old Code First
- Deprecate! Eliminate! Eradicate!
- Tools Are Critical ... to a Point
- Automate!
- You'll Never Reach Zero Security Vulnerabilities
- Security Is a Never-Ending Battle
- There Is No Security Silver Bullet
- The "Many Eyeballs" Mantra Is Right!
- Today's Denial of Service Is Tomorrow's Exploit



Zdroj: MSDN

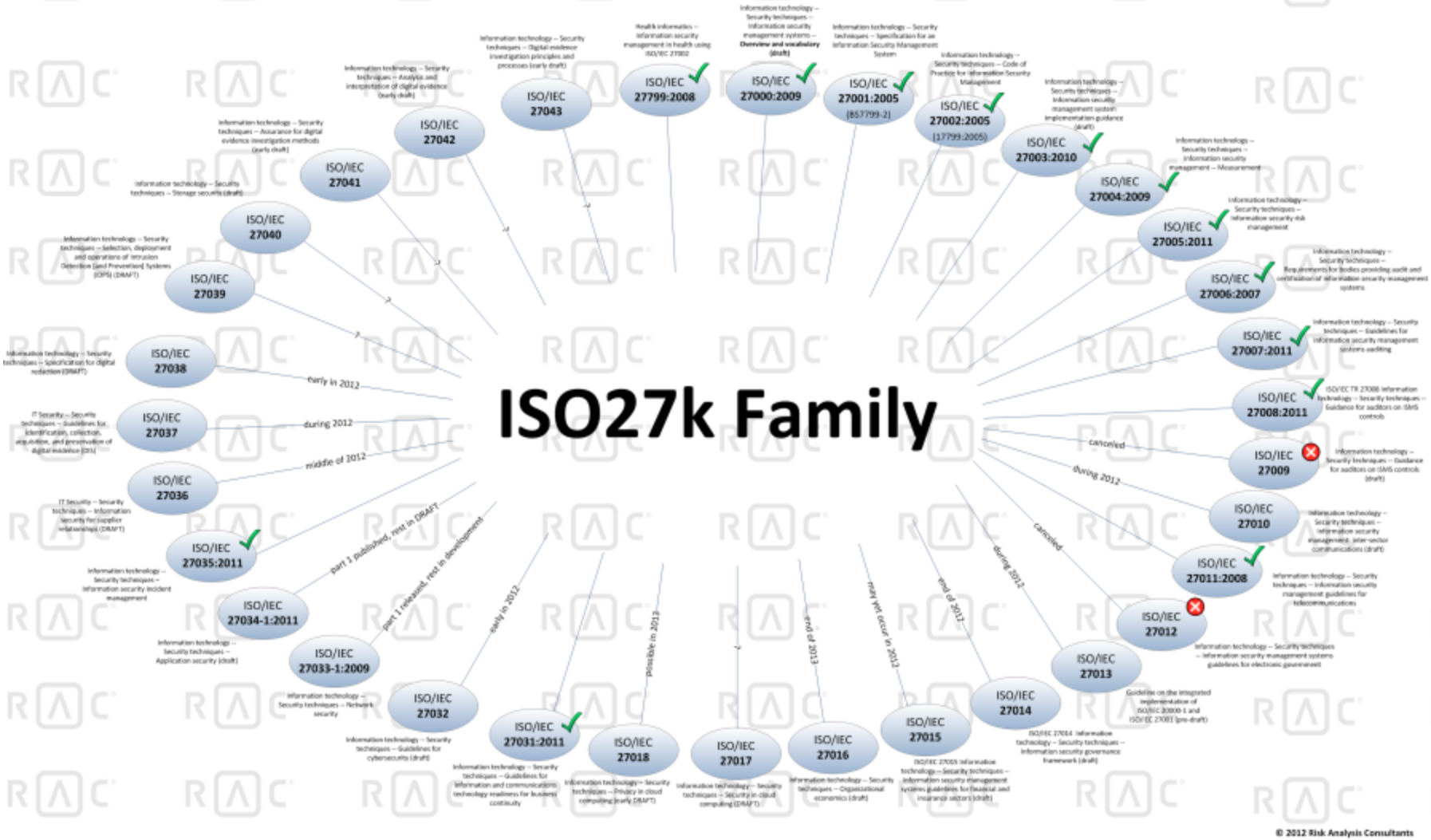
Historie Řízení bezpečnosti dat

- První počítače – pro zpravodajské služby

  (druhá strana mince: nejen informaci získat, ale také nevyzradit)
- První požadavky na bezpečnost systémů v 60. letech
- První sítě neřeší zabezpečení, bezpečnost na úrovni „stroje“
- První reálná norma BS 7799 (1995)
- Mezinárodní vydání jako ISO 17799
- Postupné revize
- Finalizace do „rodiny“ norem ISO 27000 (2005)

ISO 27000 – řada standardů bezpečnosti informací

- ISMS - Information Security Management system



ITIL - Praktické návody pro provozování IT

- Kořeny v 70. letech ve Velké Británii (státní správa, efektivita)
- Koncem 80. let osamostatnění a komercializace
- ITIL v2 (konec 90. let)
  - Sepsáno lidmi z praxe
  - Jak řešit incidenty, jak vést evidenci, jak plánovat atd.
  - Neteoretizuje, ale dává praktické šablony chování
  - Velká část převedena do normy ISO 20000
- ITIL v3 (2007) přidává hodně „business pohledu“
  - Stále se však jedná o primárně soupis „best practice“

COBIT - Strukturovaný přístup k řízení IT shora

- První verze 1996
- Jako reakce na .COM krizi (2001) vydán SOX (Sarbanes-Oxley Act)
- COBIT jako nástroj řízení IT v souladu se SOX
- Top->Down přístup
  - Potřeby businessu
  - IT Cíle
  - IT procesy
- Neřeší JAK, ale určuje CO se má dělat
- Pro manažery a auditory

Právní aspekty bezpečnosti informačních systémů

- Zákon č. 563/1991 Sb., o účetnictví.
- Zákon č. 101/2000 Sb., o ochraně osobních údajů.
- Zákon č. 154/2000 Sb., o šlechtění, plemenitbě a evidenci hospodářských zvířat a o změně některých souvisejících zákonů (plemenářský zákon).
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy.
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti.
- Technické normy
- Nařízení EU

http://www.fi.muni.cz/~smid/bezpecnostIS.html

Bezpečnost informační systémů dle NBÚ

- Vyhláška č. 523/2011 Sb. o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb.
- Personální bezpečnost (zákon č. 412/2005 Sb. a §§ 16,17, 18 VYHLÁŠKY).
- Bezpečnostní způsobilost fyzických osob:
  - Vyhrazené – oznámení (ověření odpovědnou osobou nebo poskytovatelem informace).
  - **Důvěrné – osvědčení (NBÚ).**
  - **Tajné - osvědčení (NBÚ).**
  - **Přísně tajné - osvědčení (NBÚ).**

Common Criteria

- Common Criteria for Information Technology Security Evaluation CC – ISO/IEC 15408
- Common Criteria jsou celosvětově uznávaným standardem pro hodnocení počítačové bezpečnosti produktů včetně SW řešení
- Podle CC uživatelé (uživatelské organizace) specifikují své požadavky na bezpečnost pro určitý typ řešení (produktu);
- Dodavatelé mohou tyto požadavky splnit a prohlásit o svém řešení (produktu), že splňuje specifikované požadavky;
- Ověření pravdivosti tohoto prohlášení dodavatele je certifikace provedená nezávislou akreditovanou certifikační autoritou, která na základě formalizovaného testování vyhodnotila soulad prohlášení a skutečnosti;
- Common Criteria poskytují záruku, že veškeré procesy (specifikace požadavků, implementace požadavků a vyhodnocení souladu (testování, verifikace) řešení (produktu) byly provedeny přesným a standardním postupem.

Úroveň záruk Evaluation Assurance Level (EAL1 - EAL7)

- **EAL1:** Funkčně testováno, poskytuje jistou míru důvěry na základě funkční specifikace, vymezení rozhraní a zpracování dokumentace;
- **EAL2:** Strukturovaně testováno - nezávislé testování. Vývoj rozšířen o neformální popis architektury a popis ošetření běžných útoků;
- **EAL3:** Metodicky testováno a kontrolováno. Maximální záruky na základě osvědčeného svědomitého přístupu k vývojovému procesu (bez navýšení náročnosti);
- **EAL4:** Metodicky navrženo, testováno a kontrolováno. Vyžaduje velmi kvalitní vývojové praktiky, které ale nevyžadují speciální znalosti a zdroje. Detailní popis návrhu s doložením odolnosti protiútoků s omezenými zdroji;

Regulatorní nařízení (Regulatory Compliance)

- **GLBA Compliance**
  - Gramm-Leach Bliley Act
  - Confidentiality and integrity of personal financial information stored by financial institutions.
- **HIPAA Compliance**
  - Health Insurance Portability & Accountability Act
  - Confidentiality, integrity, and availability of health care information.
- **SOX Compliance**
  - Sarbanes-Oxley
  - Privacy and integrity of financial data in publicly traded corporations.
- **PCI Compliance**
  - Payment Card Industry
  - Confidentiality of credit card information stored and used by merchants.
- **BASEL Compliance**
  - International Convergence of Capital Measurement and Capital Standards
  - Confidentiality and integrity of personal financial information stored by financial institutions. Availability of financial systems. Integrity of financial information as it is transmitted. Authentication and integrity of financial transactions.

Bezpečnostní trendy pro rok 2013

1. The volume of malicious and high-risk Android apps will hit 1 million in 2013.
2. Windows 8 offers improved security—but only to consumers.
3. Cybercriminals will heavily abuse legitimate cloud services.
4. As digital technology plays a larger role in our lives, security threats will appear in unexpected places.
5. Consumers will use multiple computing platforms and devices. Securing these will be complex and difficult.
6. Politically motivated electronic-based attacks will become more destructive.
7. Cloud storage or not, data breaches will remain a threat in 2013.
8. Efforts to address global cybercrime will take two or more years to reach full implementation.
9. Conventional malware threats will only gradually evolve, with few, if any, new threats. Attacks will become more sophisticated in terms of deployment.
10. Africa will become a new safe harbor for cybercriminals.

Zdroj: TrendMicro

Bezpečnostní trendy pro rok 2014

1. Mobile banking will suffer from more MitM attacks; basic two-step verification will no longer be sufficient.
2. Cybercriminals will increasingly use targeted-attack-type methodologies like open source research and highly customized spear phishing, along with multiple exploits.
3. In the context of targeted attacks, we will see more clickjacking and watering hole attacks, new exploits of choice, and attacks via mobile devices.
4. We will see one major data breach incident a month.
5. Attacks leveraging vulnerabilities in widely used but unsupported software like Java 6 and Windows XP will intensify.
6. The Deep Web will significantly challenge law enforcement, as the latter struggles to build capacity in order to address cybercrime on a large scale.
7. Public distrust will ensue, especially after the exposure of state-sponsored monitoring activities, resulting in a period of disparate efforts to restore privacy.
8. We will not yet see large-scale, widespread IoE threats. This requires a “killer app,” which may appear in the area of AR in the form of technology like heads-up displays.

Bezpečnostní trendy pro rok 2015

1. More cybercriminals will turn to darknets and exclusive-access forums to share and sell crimeware.
2. Increased cyber activity will translate to better, bigger, and more successful hacking tools and attempts.
3. Exploit kits will target Android, as mobile vulnerabilities play a bigger role in device infection.
4. Targeted attacks will become as prevalent as cybercrime.
5. New mobile payment methods will introduce new threats.
6. We will see more attempts to exploit vulnerabilities in open source apps.
7. Technological diversity will save IoE/IoT devices from mass attacks but the same won't be true for the data they process.
8. More severe online banking and other financially motivated threats will surface.

Nebezpečí číhají i na řídící systémy!

- **SCADA (Supervisory Control and Data Aqusition)**
- Příklady napadení systémů
  - 2009 – **červ Stuxnet pro SCADA systémy Siemens** – napadeno cca. 100.000 počítačů, z nichž 60% bylo v Íránu.
  - 2009 - **Integral Energy (Austrálie)** – bylo napadena virem celá podniková síť, což mělo za následek nutnou reinstalaci více než jednoho tisíce desktopů, aby byla nákaza izolována od řídícího systému.
  - 2009 - **Zdravotnické zařízení, Texas (USA)** – útočník převzal kontrolu nad klimatizačním systémem.
  - 2005 – **Mezinárodně operující energetická společnost** – malware infikoval SCADA, důsledkem bylo zneschopnění funkce bezpečnostního protokolu.
  - 2003 – **Atomová elektrárna Davis – Besse, Ohio (USA)** - selhání bezpečnostního systému způsobilo výpadek na dobu delší pěti hodin.
  - 1998 – **Gazprom (Rusko)** – hackeři převzali kontrolu nad plynovodem dodávajícím do Evropy pomocí trojského koně.

Zdroj: www.logica.cz

BCM a BCP podnikových činností

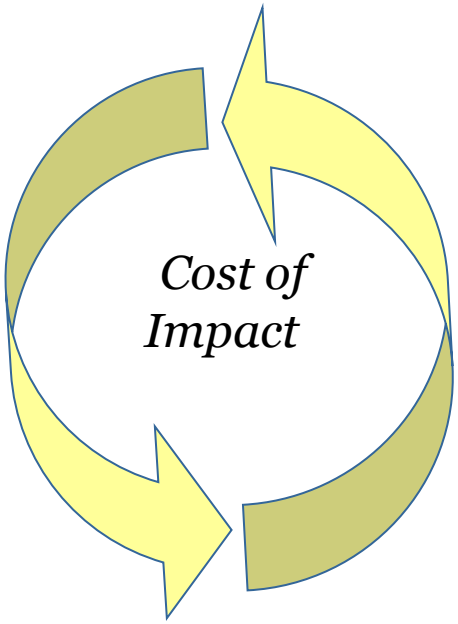
- **Plánování kontinuity činností - Business continuity planning (BCP)** definuje strategii řešení krizových situací, opatření pro předcházení krizím a efektivní a ekonomický způsob návratu společnosti do normálního chodu.
- Nezbytné součásti BCP**:**
  - **identifikace hrozeb a dalších rizik**, které mohou ohrozit chod organizace a jejich zhodnocení podle pravděpodobnosti výskytu a velikosti dopadu na chod společnosti,
  - **analýza dopadů (Business Impact Analysis),** identifikující kritické procesy a určuje dopad nedostupnosti jednotlivých procesů na organizaci,
  - **strategie obnovy** jednotlivých procesů.
- Aktualizace BCP (pravidelná revize v souvislosti se změnami procesů, infrastruktury apod.)
- Motivace k zavedení BCP
  - **požadavky regulačních orgánů** – např. pro banky
  - obchodní důvody – např. u IT poskytovatelů služeb pro zajištění SLA
  - **začlenění BCP do systému řízení kvality**
  - profesní pojištění - požadavek pojišťovny
- Důležité komponenty přípravy IT BCP - snížení rizik, která představují hrozby pro IT procesy:
  - **strategie zálohování a obnovy** dat, včetně off-site úložiště
  - **návrh flexibiní IT infrastruktury** s redundantními systémy (zrcadlení, replikace, geografická dislokace)
  - **posílení slabých míst** infrastruktury (tzv. **single points of failure**) – např. jediného zdroje napájení, jediného připojení WAN apod.

Business Impact Matrix

Lost Revenue
- *Billing Loss on 24/7 projects*
- *Lost Future Revenues*
- *Compensatory Payments*
- *Suboptimal Investment Utilization*

Productivity Loss
- *Lost man hours*
- *Compensatory Overtime*
- *Lost in progress data*
- *Lost momentum*

Damaged Reputation
- *Customer, Suppliers, Partners. Banks, Financial Markets*
- *Employee morale*
- *Credit Rating*
- *Customer Confidence*



Extra Expense
- *Cost to Recover*
- *Increased Fraud Risk*
- *Increased Error Rate*
- *Travel Expenses*
- *Temporary Employees*

Legal & regulatory liabilities
- *Contractual Penalties per contract clause*
- *Regulatory Issues*
- *Legal Issues*

Delayed Collections
- *Billing Losses*
- *Missed documents*
- *Report Outs*

Závěr

Celý systém je tak bezpečný, jako je bezpečný jeho nejslabší článek!

Dotazy, připomínky, názory…

Doporučená literatura

- Předáška J. Bareš, Corpus Solutions, Úvod do problematiky informační bezpečnosti, ČVUT FEL
- http://www.microsoft.com/security/sdl/default.aspx
- http://www.fi.muni.cz/~smid/bezpecnostIS.html
- Přednáška RNDr. Igor Čermák, CSc., Certifikace ISMS, hodnocení bezpečnosti, ČVUT FIT
- http://msdn.microsoft.com/en-us/magazine/cc163310.aspx
- http://www.nbu.cz/cs/ochrana-utajovanych-informaci/personalni-bezpecnost/obecne-k-personalni-bezpecnosti/
- http://www.rac.cz
- http://msdn.microsoft.com/en-us/library/aa480484.aspx
- *http://www.risk8.com*
- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/spotlight-articles/sp-trend-micro-predictions-for-2013-and-beyond.pdf
- http://www.logica.cz/we-are-logica/media-centre/articles/hn-energetika-scada/
- http://www.businessit.cz/cz/kyberneticka-kriminalita-iii-hacktivismus-a-kyberterorismus.php
- Sommerville, Ian; Softwarové inženýrství, Computer press, 2013