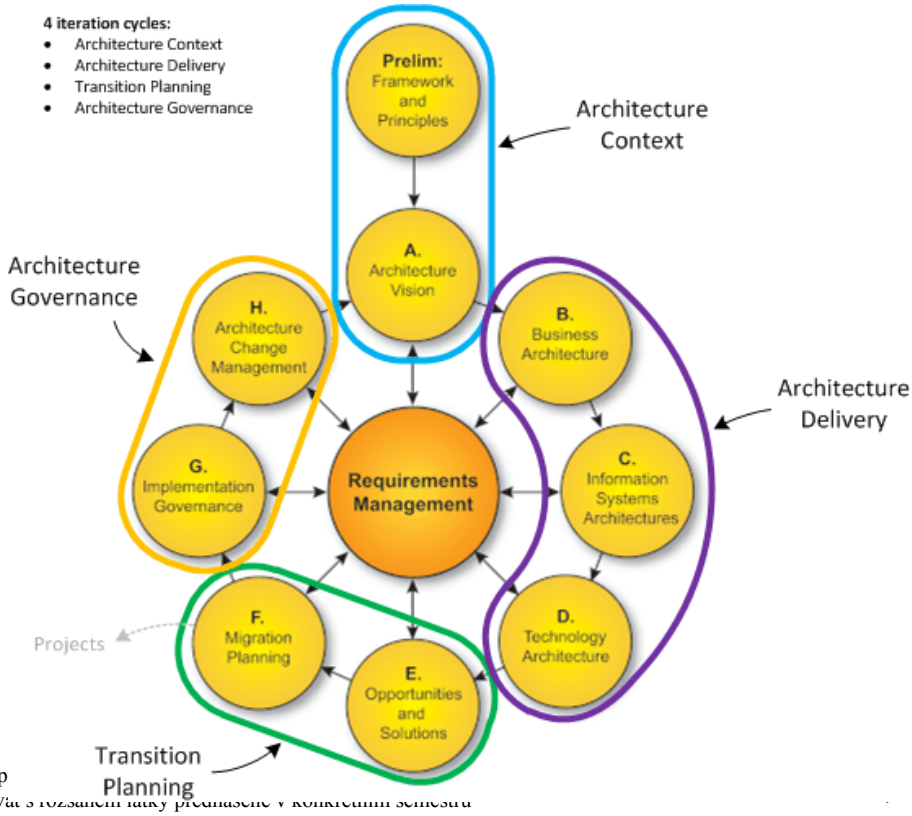
Motivační úvaha

1886 …

… a po necelých 140 letech.

IT po necelých 40 letech:



Literatura

- http://www.obluda.cz/iprednasky/index.html
- ISO17799
- ITILv3
- ISO2700x
- PFLEEGER, "*Security in Computing*", Prentice-Hall, 1989 … ve znění následujících vydání
- RFC 2504 - Users' Security Handbook
- RFC 2196 - Site Security Handbook
- https://archi.gov.cz/start
- $(ISC)^2$ – Certified Information Security Professional – The Official $(ISC)^2$ CISSP CBK Reference
- ISACA – Certified Information Security Manager – CISM Review Manual
- JACKSON, HRUSKA, "*Computer Security Reference Book*", Butterworth-Heineman, 1992
- RUSSELL, GANGEMI, "*Computer Security Basics*", O'Reilly&Associates, 1991
- SCHNEIER, "*Applied Cryptography*", John Wiley & Sons, 1994, 1996 https://www.schneier.com/books/applied-cryptography-toc
- PŘIBYL, "*Ochrana dat v informatice*", scriptum ČVUT, 1993
- Frequently Asked Questions About Today's Cryptography, http://www.rsasecurity.com/rsalabs/faq/index.html

Zcela základní pojmy

Informačním systémem(IS) rozumíme soubor technických prostředků, softwaru a jeho konfigurací, záznamových medií, postupů, dat a personálu, který daná organizace používá ke správě svých informací.

Korektní stav IS odpovídá situaci, kdy systém je schopen v definovaném rozsahu poskytovat zajišťovat všechny požadované vlastnosti zpracovávaných informaci, či poskytovaných služeb, například:

- utajení
- dostupnost
- integrita
- nepopiratelnost
- včasnost
- současnost
- autenticita
- anonymita
- pseudonymita
- …

Uvedený výčet není v žádném případě vyčerpávající, nebo reprezentativní. Výběr služeb vždy individuální

Bezpečnostní incident je stav, kdy došlo k (potenciálnímu) porušení alespoň jedné z požadovaných vlastností.

Pravidla hry

Vlastník IS buduje spoustu mechanismů – tzv. *bezpečnostních protiopatření* pro zabránění vzniku incidentu

Základní princip ochrany informačních systémů.
O peníze jde až v první řadě.

→ Chráněné objekty mají svoji cenu, pro kterou jsou chráněny. Cena může být různá pro majitele a útočníka.
→ Ochrana není, ani přibližně, zadarmo.

Princip nejsnazšího průniku.
Je třeba očekávat, že útočník použije libovolný způsob průniku.

Fanatismus nepřináší dobré výsledky

Bezpečnost je souboj mezi zdroji (čtěte penězi, znalostmi, důvtipem, ..) útočníka a zdroji provozovatele systému. Kdo jich má víc, pravděpodobně zvítězí.

Proč se tato hra hraje

Základem úspěchu je uvědomit si, **proč** chceme dosáhnout bezpečnosti

- víra v právo na …
  - soukromí
  - ochranu osobnosti
  - listovní tajemství
  - obchodní tajemství
  - právo se bránit
- nedůvěra v …
  - státní moc
  - obchodní partnery
  - okolí
- povinnosti
  - legislativa
  - závazky (smlouvy, sliby, …)

O co se hraje

Ve skutečnosti by se mělo hrát o myšlenky tj. informace, zpravidla se ovšem opatření soustředí na jejich technickou reprezentaci
Informační systém je tvořen souborem tzv. *aktiv*. Jejich společným cílem je poskytovat vám služby v požadované kvalitě. Mezi aktiva patří mimo jiné:

- záznamová media
- počítače
- tiskárny
- programy
- konfigurace
- vlastní informace
- sklad spisů
- napájení
- komunikační linky
- administrátoři
- uživatelé
- zálohy
- provozní prostory
- ...

Svůj soupis aktiv si každý musí provést sám.

Dobrým trick-em je začít od toho, proč systém máte, tedy soupisem poskytovaných služeb a postupovat směrem dolů k dalším aktivům, které potřebujete, aby služby fungovaly.

Váš útočník hledá *expozici* tj. místo potenciálního poškození.

Zranitelností rozumíme nedostatek bezpečnostního systému, může být použit k narušení některé z definovaných vlastností systému.

Př: Data o novém výrobku jsou z pohledu útočníka expozicí, když si naplánuji, že je budu svým pobočkám posílat nešifrované majlem, je to zjevná zranitelnost.

Bezpečák by měl vidět samé *hrozby* tj. skutečnosti, které potenciálně mohou být původci bezpečnostního incidentu. Zdaleka nejstrašnější hrozbou jsou vlastní uživatelé. Kromě nich sem patří ještě:

- povodně a záplavy
- požáry
- zloději
- rozvědky
- konkurence
- hackeři
- vandalové
- nešikové s bagrem
- viry a červi
- závady techniky
- výpadky napájení
- teplota
- vlhkost
- vibrace
- soud
- ...

Přehled relevantních hrozeb si musí každý sestavit sám. Někdy se tomu učeně říká *model ohrožení*.

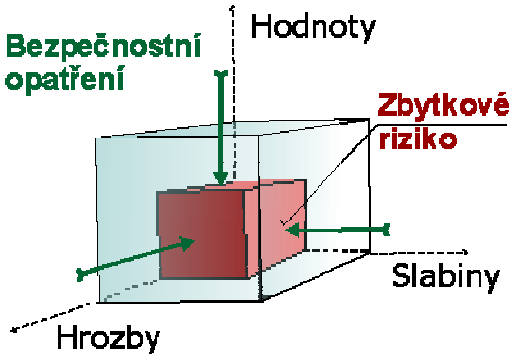
Cíl hry

Cílem překvapivě **není** zbavit se útočníka, ani eliminovat všechny potenciální incidenty - prostě proto, že se to nevyplatí.

Naplněním hrozby vznikne bezpečnostní incident jehož finančnímu vyjádření se říká *dopad.*

Rozsah hrozeb spolu s pravděpodobností jejich realizace udává celkovou míru *rizika*.

Riziko vztažené k určitému období = *očekávaná ztráta*.



Cílem najít místo, kde se bezpečnostní opatření přestávají vyplácet.

Nevyloučili jsme zcela riziko incidentu – zbylo *zbytkové riziko*

Stav, kdy vám někdo nebo něco prostřelilo bezpečnostní opatření, je nutno brát jako další z provozních režimů IS.

Takže shrnuto: cílem je minimalizovat celkové náklady na provoz:

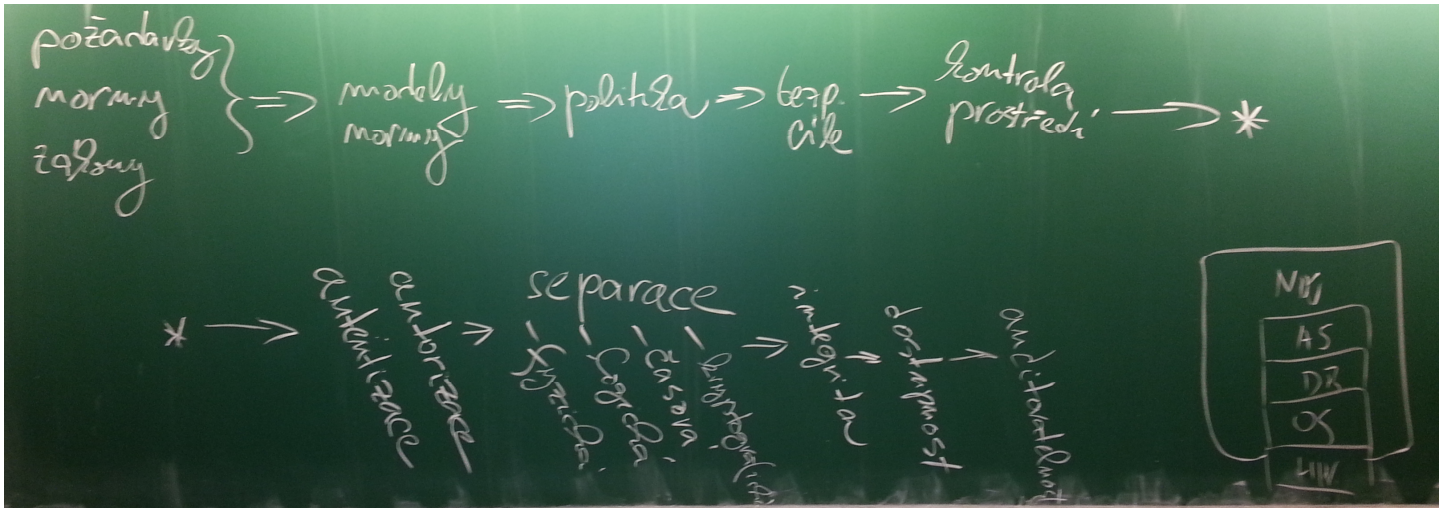
- **Investice**
- **Provozní náklady**
- **Očekávané ztráty**

… za sledované období.

Bezpečnost

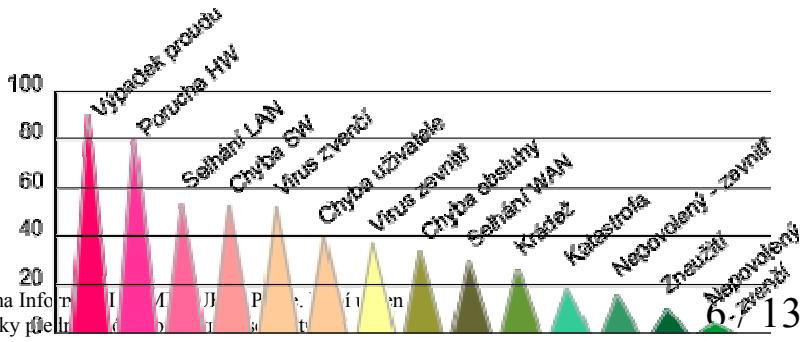
Hlavní komponenty bezpečnosti lze rozdělit takto:

- kontrola prostředí
- autentizace / identita
- autorizace
- separace
  - fyzická
  - časová
  - logická
  - kryptografická
- integrita, důvěryhodnost
- dostupnost
- auditabilita



Krok stranou

Bezpečnost je naprosto netriviální propletenec povětšinou velmi triviálních záležitostí. Obrázek byl namalován před zhruba čtrnácti lety podle průzkumu který činil Národní Bezpečnostní Úřad ve spolupráci



s časopisem DSM a společnosti PriceWaterhouseCoopers. Bez velkých změn platí dodnes.

Jak na to – třeba podle BS7799

bezpečnost není stav, ale proces, technika/technologie je jen podpůrným nástrojem nutno

- plánovat
- řídit
- školit a rozvíjet
- provozovat
- kontrolovat
- vyhodnocovat
- ověřovat / auditovat
- reagovat na změny

Rozsah pokrytí politiky

…tzn. co a proti čemu to má chránit

- seznam aktiv
- uvažované hrozby

Požadavky na bezpečnost

Je řada důvodů, proč vytvářet bezpečnostní opatření

- zákonné požadavky
- obecné standardy
- resortní normy
- ochrana obchodního tajemství
- dosažení provozní kontinuity
- požadavky protistrany
- zajištění konkurenčních výhod
- ...

Okruh možných řešení

Pomoci může celá řada technických norem a certifikátů

Plán

Potřebujete *bezpečnostní politiku*. – zde se naplánuje, jak budete řešit všechny oblasti bezpečnosti, kdo je za co zodpovědný a jak to budete implementovat a provozovat.

Nebo podle ISO/IEC2700x

- Stanovíte politiku zabezpečení
- Organizujete informační bezpečnost
- Řídíte aktiva
- Zavedete bezpečnostní postupy pro řízení lidských zdrojů
- Zavedete prostředky prostorové a environmentální bezpečnosti
- Spravujete (řídíte) komunikace a provoz
- Zavedete kontrolu přístupu
- Zavedete formální pořizování, vývoje a údržby bezpečnostních opatření
- Provádíte řízení bezpečnostních incidentů
- Zajistíte řízení kontinuity obchodních operací
- Kontrolujete a udržujete shodu

A ISACA to vidí takhle:

- **Efektivní řízení informační bezpečnosti**
  - Obchodní cíle a záměry
  - Určení přijatelného rizika a schopnosti absorbovat riziko
  - Rozsah a cíle řízení informační bezpečnosti
  - Řízení, Sprava rizik a shoda
  - Obchodní model pro informační bezpečnost
  - Dynamiké vazby
  - Zajitění procesní integrace—konvergence
- **Role a odpovědnosti**
- **Kompetence, kultura**
  - Board of Directors
  - Senior Management
  - Vlastníci obchodních procesů
  - Řídící výbor
  - Chief Information Security Officer

- **Role a odpovědnosti správy rizik**
  - Klíčové role:
  - Získat závazek vrcholného vedení, Vývoj a prezentce obcohdních případů (business case), Ustavení repportingu a komunikačních kanálů

- **Řízení vztahů s třetími stranami**

- **Metriky řízení informační bezpečnosti**
  - Metriky efektivity opatření
  - Metriky implementace správy (governance)
  - Metriky konformity (Alignment)
  - Metriky řízení rizik
  - Metriky poskytování hodnoty (Value Delivery)
  - Metriky správy zdrojů
  - Měření výkonu
  - Zajištění procesní integrace (Convergence)
- **Přehled strategie informační bezpečnosti**
  - Vývoj strategie
  - Obvyklé chyby a problémy
- **Záměry srategie informační bezpečnosti**
  - Cíl
  - Definice záměrů, obchdní závislosti
  - Požadovaný stav:
    - COBIT, COBIT 5 Process Assessment Model , Capability Maturity Model Integration, Balanced Scorecard, Architectural Approaches, ISO/IEC 27000 Series, jiné přístupy …
  - Záměry zvládání rizika
- **Stanovení aktuálního stavu bezpečnosti**
  - Aktuální riziko
  - Business Impact Analysis
- **Information Security Strategy Development**
  - Elements of a Strategy
  - Road Map
  - Strategy Resources and Constraints—Overview
- **Strategy Resources**
  - Policies and Standards
- **Politiky, standardy, postupy a pravidla**
  - Enterprise Information Security Architecture(s)
  - Controls
- **IT Controls, Non-IT Controls, Countermeasures, Layered Defenses**
  - Technologies
  - Personnel
  - Organizational Structure
- Centralized and Decentralized Approaches to Coordinating Information Security
  - Employee Roles and Responsibilities
  - Skills
  - Awareness and Education
  - Audits
  - Compliance Enforcement
  - Threat Assessment
  - Vulnerability Assessment
  - Hodnocení a řízení rizik
  - Pojištění

    - Analýza dopadu na obchod (Business Impact A.)
    - Resource Dependency Analysis
    - Outsourced Services
    - Other Organizational Support and Assurance Providers
- **Omezení strategie**
    - Právní a regulatorní požadavky
- **Požadavky na obsah a retenci obchodních záznamů**
- E-discovery
    - Physical
    - Ethics
    - Culture
    - Organizational Structure
    - Costs
    - Personnel
    - Resources
    - Capabilities
    - Time
    - Risk Acceptance and Tolerance
- **Action Plan to Implement Strategy**
    - Gap Analysis—Basis for an Action Plan
    - Policy Development
    - Standards Development
    - Training and Awareness
    - Action Plan Metrics
        - Key Goal Indicators, Critical Success Factors, Key Performance Indicators, General Metrics Considerations
    - Action Plan Intermediate Goals

- **Information Security Program Objectives**

No a $(ISC)^2$ metodika to vidí více v kontextu celého byznysu

- **Bezpečnost a řízení rizik**
    - Aplikace základních konceptů
    - Vyhodnocení a nasazení principů řízení bezpečnosti (procesy, role, odpovědnosti)
    - Due Care, Due Diligence
    - Určení shodu s požadavky (legislativní, smluvní, ochrana soukromí)
    - Právní a regulativní rámec bezpečnosti
    - Vyšetřování incidentů
    - Politika, standardy, procedury a pravidla
    - Identifikace, analýza a prioritizace požadavků na kontinuity business operací
    - Zajištění a podpora bezpečnosti osob
    - Aplikace konceptů řízení rizik (identifikace, hodnocení řízení, protiopatření, kontroly, monitoringzlepšování)

    - Aplikace konceptů modelování hrozeb
    - Řízení řízení rizik vdodavatelském řetězci
    - Vytváření a udržování informovanosti, vzdělávání a školení
- Bezpečnost aktiv
    - Identifikace a klasifikace aktiv
    - Stanovení požadavků na správu a použití oktiv
    - Bezpečné použití prostředků
    - Řízení životního cyklu
    - Zajištění dostatečného držení (retention) prostředků
    - Opatření pro zajištění bezpečnosti dat a shody s požadavky
- Architektura bezpečnosti
    - Implementace a řízení procesů v souladu s bezpečnostními principy (… keep it simple, zero trust, SOD, …)
    - Formální modely bezpečnosti a jejich aplikovatelnost
    - Aplikace bezpečnostních prvků informačních systémů
    - Hodnocení a minimalizace slabin
    - Volba kryptografických prostředků
    - Hodnocení potenciálních kryptografických útoků
    - Aplikace bezpečnostních principů při plánování
- Komunikační a síťová bezpečnost
    - Aplikace bezpečnostních principů do architektury sítí
    - Bezpečnostní koncepty aktivních komponent
    - Impelementace bezpečných kmunikačních kanálů
- Správa identit a řízení přístupu
    - Řízení fyzického a logického přístupu
    - Identifikace lidí, zařízení a služeb
    - Federace identit
    - Autorizační mechanismy
    - Životní cyklus identit, autorizací a jejich provisioning
    - Autentizační mechanismy
- Vyhodnocování bezpečnosti a testování
    - Návrh strategií hodnocení, testování a auditu bezpečnosti
    - Testování bezpečnostních protiopatření
    - Sběr dat bezpečnostních procesů
    - Analýza dat bezpečnostních procesů
    - Bezpečnostní audit
- Provoz bezpečnosti
    - Podpora vyšetřování
    - Logy a monitoring
    - Správa konfigurací
    - Aplikace základních konceptů bezpečnosti (need to know, need to retain, job rotation, …)
    - Ochrana zdrojů
    - Správa incidentů
    - Provoz preventivních a detektivních opatření
    - Správa patchů a slabin

    - Řízení změn
    - Strategie obnovy
    - Strategie obnovy po katastrofě
    - Testování plánů obnovy po katastrofě
    - Spolupráce na tvorbě a testování plánů kontinuity
    - Řízení fyzické bezpečnosti
    - Personální bezpečnsot
- Bezpečnost vývoje SW
    - Vývojové metodologie
    - Řízení bezpečnosti při vývoji SW
    - Hodnocení efektivity bezpečnostních opatření
    - Hodnocení bezpečnostního dopadu pořízeného SW
    - Pravidla a standardy bezpečného vývoje SW

Realizace a provoz

Praktické realizace, následně provoz, monitorování, aplikace změn, verifikace, auditu atd. atp.

Možné hrozby

1. *přerušení* - některá část systému je ztracena nebo nedosažitelná
2. *zachycení* - neautorizovaný subjekt získá přístup k nějakému objektu systému
3. *modifikace* - neautorizovaný subjekt získá možnost pozměňovat některé části systému
4. *fabrikace* - neautorizované vytvoření nového objektu
5. ...
6.

obecně narušení některé z požadovaných vlastností systému

Zdroje ohrožení

1. vyšší moc (požár, povodeň, zemětřesení, blesk, …)
2. závady technického zařízení
3. neúmyslné lidské chyby
4. záměrné útoky

Klasifikace možných útočníků

klasifikovat lze dle mnoha kriterií, zejména dle

I. způsobu, jak se projeví způsobená škoda

A. ztráta integrity
B. ztráta dosažitelnosti
C. ztráta autenticity …

II. druhu způsobené ztráty
A. neautorizované použití služeb
B. přímá finanční ztráta
C. fyzické poškození, vandalismus

III. role, kterou výpočetní technika hraje v tomto konání
A. objekt útoku
B. nástroj
C. prostředí
D. symbol

IV. použitých prostředků
A. opisování údajů
B. špionáž
C. vkládání falešných dat
D. krádež
E. odposlech
F. scanování, prohledávání - kupříkladu hledání hesel zkoušením, hledání tfn. linek, které vedou k počítači, …
G. piggybacking, tailgating - útočník se snaží projít vstupní kontrolou zároveň s autorizavanou osobou, nebo pokračovat v započaté session
H. trojské koně - programy, vykonávající skrytou funkci
I. viry
J. trapdoors - skryté vstupy do systému, utajené příkazy umožňující přeskočit některé části procesu
K. logické bomby - části kódu spouštěné výskytem určitých okolností - čas, dosažený obrat, stav systému
L. salami attack - využívání zaokrouhlovacích chyb, drobné úpravy na hranici přesnosti zpracovávaných dat
M. prosakování dat
N. pirátství