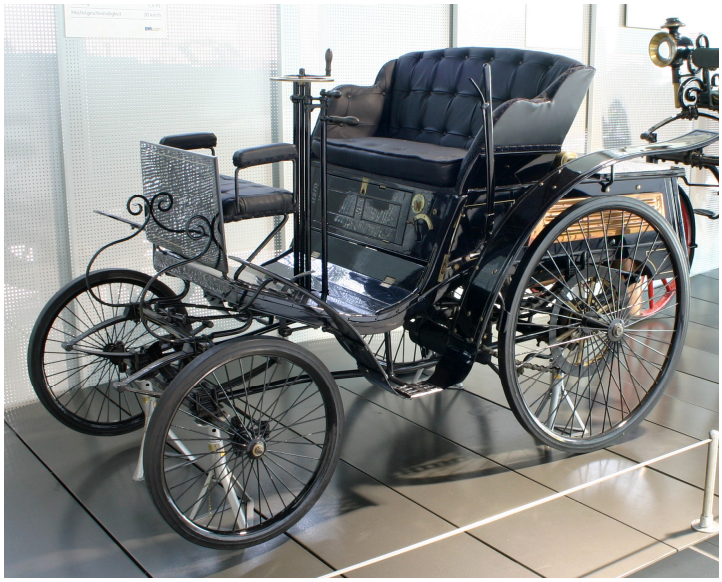
Motivační úvaha

1884 …



… a po necelých 140 letech.

Literatura

- http://www.obluda.cz/iprednasky/index.html
- ISO17799
- ITILv3
- ISO2700x
- PFLEEGER, "*Security in Computing*", Prentice-Hall, 1989 … ve znění následujících vydání
- 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
- 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*.

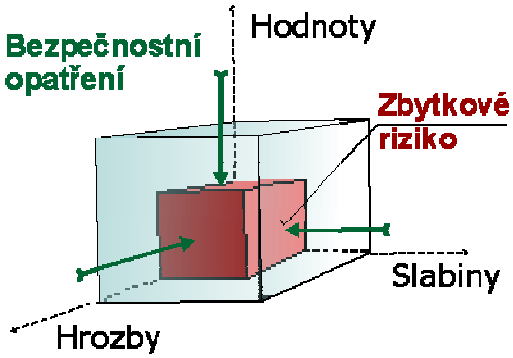
Cíl hry

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:

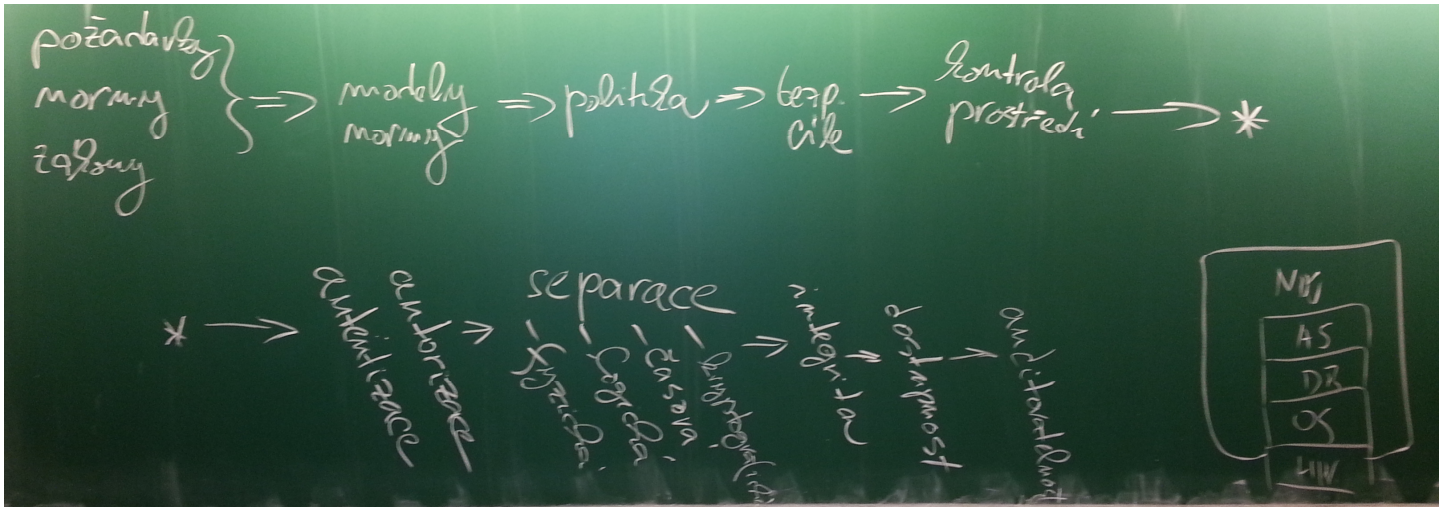
- **Investice**
- **Provozní náklady**
- **Očekávané ztráty**

… za sledované období.

Bezpečnost

Hlavní komponenty bezpečnosti lze rozdělit takto:

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



Jak na to

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

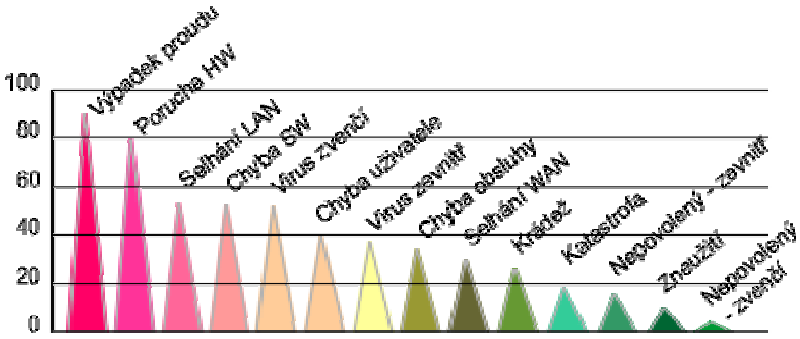
Potřebujete *bezpečnostní politiku*. – zde se naplánuje, jak budete řešit všechny oblasti bezpečnosti, kdo je za co zodpovědný a jak to budete implementovat a provozovat.

Realizace a provoz

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

Krok stranou

Bezpečnost je naprosto netriviální propletenec povětšinou velmi triviálních záležitostí. Obrázek je namalován před zhruba čtyřmi lety podle průzkumu který činil Národní Bezpečnostní Úřad ve spolupráci s časopisem DSM a společnosti PriceWaterhouseCoopers.



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