Úvod do problematiky informační bezpečnosti

Ing. Jan Bareš, CISA

CORPUS SOLUTIONS

Agenda

- Představení
- Information Security Management System
- Úvod do problematiky bezpečnosti
- Informace a systémy veřejné vs. privátní
- Pohled do praxe
- Funkčnost a bezpečnost
- Normy, standardy
- Nejen technika, ale i člověk

Ing. Jan Bareš, CISA

- 25 let praxe
- Začátky na socialistkém sálovém systému
- Absolvent ČVUT-FEL
- Osobní vývoj: technik, systémák, programátor, vedoucí provozu, konzultant, auditor, manažer

- Za poslední rok 5 auditů (zákaznicí se nezveřejňují)

Corpus Solutions

Řešení, která garantují bezpečnost, dostupnost a efektivitu business aplikací

- Společnost Corpus Solutions a.s. úspěšně působí na trhu informačních a komunikačních technologií již od roku 1992. Je stabilním partnerem pro dlouhodobou spolupráci založenou na porozumění potřeb zákazníků, pomáhá, aby jejich business aplikace pracovaly v infrastrukturním prostředí, tak, aby byla maximálním způsobem garantována jejich bezpečnost, výkonnost a efektivita provozu.
- Projekty jsou realizovány spolu s konzultačními službami, které je pomáhají zasadit do celkového systému procesů a řízení IT služeb v prostředí zákazníka. Tím je zajištěna cílovost projektů a sladění s obchodními a podnikatelskými záměry.
- Corpus Solutions a.s. poskytuje vysoce expertní služby v oblasti implementace nástrojů a řešení pro zvýšení efektivity, výkonnosti, spolehlivosti a bezpečnosti provozovaných aplikací a infrastruktury.
- Společnost disponuje nejvyššími certifikacemi v rámci vybraného produktového portfolia.

Agenda

- Představení
- Information Security Management System
- Úvod do problematiky bezpečnosti
- Informace a systémy veřejné vs. privátní
- Pohled do praxe
- Funkčnost a bezpečnost
- Normy, standardy
- Nejen technika, ale i člověk

ISMS

Information Security Management System

3 základní role

- **Rozhodování a řízení**
  - *Stanovuje CO se bude dělat*
  - *Soulad s potřebami celku*
- **Výkon**
  - *Nastavení technologie, školení uživatelů, dohled, řešení závad*
- **Kontrola**
  - *Audit: interní, externí, certifikovaný*

- **Proces se zpětnou vazbou**
- Pozor na konflikty rolí! Jsou neslučitelné!

Informace jako hodnota

- Většina dnešní civilizace je založena na informaci
  - Jak vyrobit
  - Jak navrhnout
  - Kde získat suroviny
  - Komu prodat, kde koupit
  - S kým a o čem jednat … atd.
- Informace je cenná
- Informace může ztratit hodnotu
  - Zánik
  - Vstoupení v obecnou známost
  - Ztráta důvěry v pravdivost

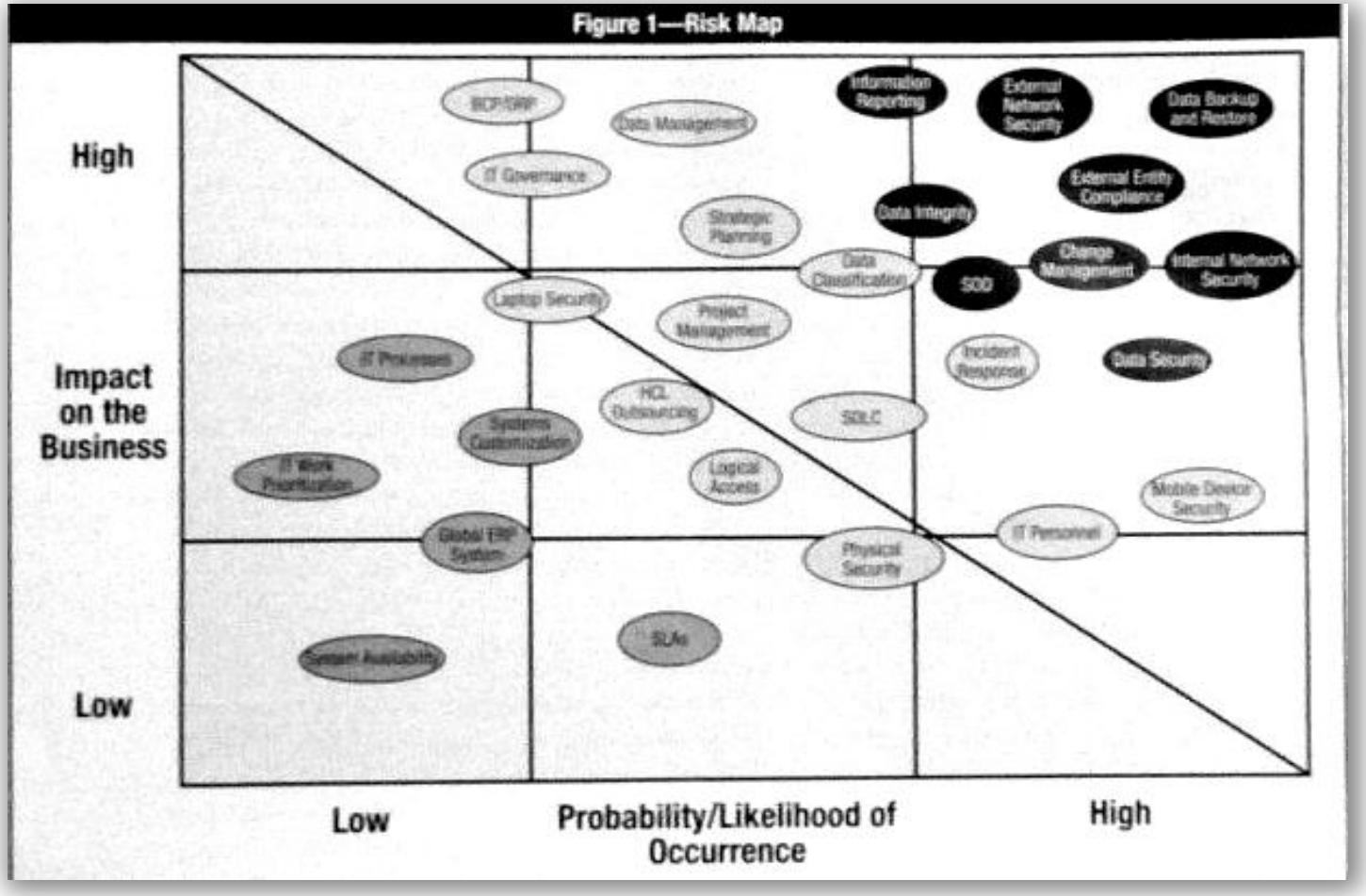
Agenda

- Představení
- Information Security Management System
- Úvod do problematiky bezpečnosti
- Informace a systémy veřejné vs. privátní
- Pohled do praxe
- Funkčnost a bezpečnost
- Normy, standardy
- Nejen technika, ale i člověk

Základní pojmy

- **Aktivum**
  - *„Něco“, co má pro držitele hodnotu*
- **Hrozba**
  - *Skutečnost nezávislá na vůli majitele aktiva*
- **Riziko**
  - *Výslednice působení hrozby na aktivum*

Odvození rizika



Praktické příklady

- Auto
- Dům
- Televizor

- Firma
- Stát

- Osoba

3 sudičky posuzování bezpečnosti informace

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

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

Agenda

- Představení
- Information Security Management System
- Úvod do problematiky bezpečnosti
- Informace a systémy veřejné vs. privátní
- Pohled do praxe
- Funkčnost a bezpečnost
- Normy, standardy
- Nejen technika, ale i člověk

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

Agenda

- Představení
- Information Security Management System
- Úvod do problematiky bezpečnosti
- Informace a systémy veřejné vs. privátní
- Pohled do praxe
- Funkčnost a bezpečnost
- Normy, standardy
- Nejen technika, ale i člověk

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

Kvíz osobní bezpečnosti

- Osobní počítač
- Soukromá data
- Sociální sítě
- Platební karta
- Internetbanking
- Nepočítačově předávané informace

- **Dostupnost, Důvěrnost, Integrita**

Agenda

- Představení
- Information Security Management System
- Úvod do problematiky bezpečnosti
- Informace a systémy veřejné vs. privátní
- Pohled do praxe
- Funkčnost a bezpečnost
- Normy, standardy
- Nejen technika, ale i člověk

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

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?*

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

Agenda

- Představení
- Information Security Management System
- Úvod do problematiky bezpečnosti
- Informace a systémy veřejné vs. privátní
- Pohled do praxe
- Funkčnost a bezpečnost
- Normy, standardy
- Nejen technika, ale i člověk

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)

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“

ITIL (2)

IT z pohledu uživatele - SLUŽBA

- ITIL (IT Infrastructure Library) - procesně orientované řízení služeb poskytovaných prostřednictvím ICT
- Co je služba?
- Technická nebo organizační kapacita, kterou IT poskytuje svým uživatelům (například e-mail, provoz a správa sítě, zálohování apod.)
- Každá služba má svůj životní cyklus, jenž reprezentuje „život“ služby od jejího vzniku, po její provoz a zánik
- Životní cyklus dle ITIL (5 fází): Service Strategy, Service Design, Service Transition, Service Operations, Continual Service Improvement

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

COBIT (2)

COBIT – vnitřní struktura

- COBIT (Control Objectives for Information and related Technology) - kontrola služeb poskytovaných IT a způsobu jejich řízení
- Pro manažery a auditory
- Aspekty managementu informatiky – například rozvoj lidských zdrojů, řízení majetku, řízení projektů apod.
- Jistota, že peníze investované do ICT jsou vynakládány efektivně
- Kontrola, že ICT plní role a funkce podpory obchodních procesů a poskytuje '*true-and-fair view*'

ITIL vs COBIT

- Každý z obou přístupů má jiné určení a použití:

- ITIL - každodenní řízení IT služeb a infrastruktury
- COBIT - nástroj auditu informatiky a strategického řízení

- Implementací některých procesů ITIL dojde automaticky ke splnění některých požadavků COBIT

Agenda

- Představení
- Information Security Management System
- Úvod do problematiky bezpečnosti
- Informace a systémy veřejné vs. privátní
- Pohled do praxe
- Funkčnost a bezpečnost
- Normy, standardy
- Nejen technika, ale i člověk

Trocha psychologie

- Homo Sapiens se vyvinul
  - Zvíře
  - Lovec a sběrač
  - Sociální tvor

- Informační bezpečnost je problém na společenské úrovni
- Instinkty zvířete stále máme v sobě
- Cizí bolest je vždy vzdálená
- Vzdálené dopady hrozeb podceňujeme

- **Je třeba hledat zástupné motivace na osobní úrovni**

Zájmy a motivace

- Košile bližší než kabát
- Nehas, co tě nepálí
- Proč stahovat kalhoty, když brod je ještě daleko

- Mně nemají co ukrást
- *časem* …Safra!!!

… **KDO za to může?**

- **Nutnost analogie**
  - *Nejdu v noci parkem před nádražím se svazkem bankovek v ruce (u dívek „ve vše odhalující minisukni“)*

Kvíz bezpečného hesla

- Heslo první: cVa-2h!u
- Heslo druhé: sKakaIpEspResoVes
- **Co je bezpečnější a PROČ?**

Dotazy a závěr

Kontakt

Ing. Jan Bareš

Jan.Bares@Corpus.cz