MASARYKOVA UNIVERZITA

IP firmy

7.12. 2012

Informační politika a firmy

- „Strategie vytváření podmínek, cílů a priorit v oblasti informačních procesů zejména zdokonalováním informačních technologií, kterou se má dosáhnout zlepšení kvality života občanů, úrovně státní správy a **podnikatelské sféry** na úrovni národní (státní), regionální nebo celosvětové.“ (VLASÁK, 2001:159-168)
- Zavádění ICT + politika sdělování a komunikování určitých konkrétních informací => i pro firmy

IS organizací

- Roste tlak na zpřístupnění dokumentů
- Potřeba přístupu bez ohledu na geografickou vzdálenost
- Zabezpečení nikdy 100% – viz „neprolomitelná“ šifra
- Riziko je pravděpodobnost, s jakou bude daná hodnota aktiva zničena či poškozena hrozbou ve formě konkrétního útoku, který zapůsobí přes zranitelnost systému. (volně dle Požár, s. 37-38)

Competitive Intelligence

- Podrobně v předmětu Informační průmysl

- Konkurenční zpravodajství
- Etické získávání informací o konkurenci a chránění o sobě
- Vyhledávání skrytých, ale dostupných informací, mnoho publikováno ze zákona (ochrana spotřebitele)
- Využití pro rozhodnutí o strategickém vývoji firmy s ohledem na prostředí (konkurence, státní regulace atp.)
- Více k CI v ČR – doporučuji článek T. Uhrína na Portálu CI o tom, jaké informace o firmách jsou cílem a jak se k nim dostat (legálně)

Základní postupy v CI

- Ofenzivní (aktivní) zpravodajství)
  - Odhalení strategie konkurence a využití ve prospěch vlastní organizace
  - Informace marketingové, o technologiích, o konkurenci atd.
- Obranné zpravodajství
  - Fyzickou bezpečnost
  - Personální bezpečnost
  - Bezpečnost HW i SW
  - Bezpečnost dat, Know How, technologických procesů
  - Bezpečnost komunikačních systémů a cest
  - Ochranu obchodních aktivit
  - Aktivní ochranu proti dezinformacím apod.

Informační audit

- „Je komunikace mezi pracovníky a pracovními týmy optimální?
- Jsou dostupné informační zdroje optimálně využity?
- Je firemní image (prezentace směrem navenek i dovnitř) v souladu s firemní identitou (zejména požadavky na prezentaci)?
- Je internetová prezentace optimální vzhledem k jejímu očekávanému přínosu?
  apod.“ (Dombrovská, Očko, Zeman)
- => hodnocení efektivity využití informací, informačních zdrojů a informačních technologií

Informační audit

- Často omezován na zhodnocení IS/IT => základ, ale nestačí
- Nutné řešit vnitřní i vnější informační procesy v celé organizaci
- Mnoho různých metodik, obvyklý postup: sběr dat => analýza => vyhodnocení
- Některé metodiky důraz na využití informačních zdrojů, jiné organizaci zpracování informací
- Na závěr nutné uvedení řešení nedostatků

Risk management

$$ALE = \sum_{|=|}^{n} P_i * c_i,$$

- Ocenění rizik (Risk Assessment) "*proces vyhodnocení hrozeb, které působí na informační systém s cílem definovat úroveň rizika, kterému je systém vystaven. Cílem je zjištění, jsou-li bezpečnostní opatření dostatečná, aby snížila pravděpodobnost vzniku škody na přijatelnou úroveň.*" (Požár, 2005, s. 37)
- Efektivita -> ALE (Annual Loss Expectancy)
  - p = pravděpodobnost, že během jednoho roku nastane ohrožení
  - C = ztráta, jestliže k ohrožení dojde
  - i = pořadí ohrožení
  - n = celkový počet ohrožení za rok
- Risk management součástí informačního auditu

Pomůcky zabezpečení

- ISO normy
  - ČSN ISO/IEC 27000 - 27002 - Systém řízení bezpečnosti informací,
  - ČSN ISO/IEC 15408 - Kritéria pro hodnocení bezpečnosti IT,
  - ČSN ISO/IEC TR 13335-1 - 13335-4 - Směrnice pro řízení bezpečnosti IT,
  - ISO/IEC TR 13335-5 - Guidelines for the management of IT Security, Management guidance on network security
- Hodnocení důvěryhodnosti systému
  - TCSEC - Trusted Computer System Evaluation Criteria, tzv. Orange Book
  - ITSEC - Information Technology Security Evaluation Criteria + evaluační manuál ITSEM
  - CTCPEC - Canadian Trusted Computer Product Evaluation Criteria
- Metodiky a softwarová řešení
  - CRAMM
  - Cobra
  - DRAMBORA

Kroky procesu řešení bezpečnosti

1. Cíle a strategie řešení informační bezpečnosti.
2. Analýza rizik informačního systému.
3. Bezpečnostní politika organizace.
4. Bezpečnostní standardy.
5. Implementace informační bezpečnosti.
6. Monitoring a audit.

- BS-7799 British Standard Institute a ISO/IEC 17799 pro řízení informační bezpečnosti a certifikace systému ISMS)

Bezpečnostní politika firmy

- Závazný písemný dokument schválený nejvyšším vedením pro celou organizaci a všem zaměstnancům známý
- Postupy pro předcházení a řešení bezpečnostních problémů – zaměstnanec má postupovat „podle příručky“ nejlepším možným řešením (nemělo by dojít k jeho chybě)
- Vznik dlouhý a složitý – obsah musí být dlouhodobě platný, tím obecný (např. neřeší postupný postup skartace, ale že proběhne a pro co)
- OECD vytvořila seznam doporučených principů Guidelines for the security of information systems

Pro zavedení musí být upraveno (Požár, s. 101)

- „Požadavky na bezpečnost počítačů (HW bezpečnost, zabezpečení přístupu, dostupnost dat a informací, jejich důvěrnost, viry, zásady pro uživatele).
- Správa dat (požadavky na správu dat, definice pojmů, zásady bezpečnosti dat neelektronické formě).
- Provoz s uvedením zásad, zodpovědnosti za provoz IS, zálohování a obnova SW, hodnocení rizik, vývoj aplikací a audit s pojištěním.
- Řízení přístupu s uvedením zásad, odpovědnost za řízení přístupu, fyzická a logická bezpečnost, problematika virů a červů.
- BP počítačové sítě zásady bezpečnosti a účelu sítě, pravidla provo-zu na síti.
- Bezpečnost datových přenosů odpovědnost za provoz sítí, logická bezpečnost.
- Osobní odpovědnost správců dat hardwarová a softwarová bez-pečnost, zneužití počítačových prostředků, hlášení bezpečnostních incidentů.
- Právní a etické otázky trestné činy, copyrighty, ochrana osobních dat, etické otázky aj.
- Vzory dokumentů.“

Zdroje

- DOMBROVSKÁ, Michaela, Petr OČKO a Petr ZEMAN. Informační audit – cesta k rozvoji znalostní organizace. *Ikaros* [online]. 2005, roč. 9, č. 9 [cit. 2012-12-04]. ISSN 1212-5075. Dostupné z: http://www.ikaros.cz/informacni-audit-%E2%80%93-cesta-k-rozvoji-znalostni-organizace
- POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, 309 s. Vysokoškolská učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-868-9838-5.
- SAPÍK, Milan. Konkurenční zpravodajství. *Internet Centrum* [online]. [cit. 2012-12-04]. Dostupné z: hujeri.ic.cz/4-INFM/IMG_Competitive_intelligence_v1.ppt
- UHRÍN, Tibor. Jak používat volně dostupné nástroje k základnímu sledování konkurenta: nástin problematiky (v ČR) a příklady. *Portál CI* [online]. 2011 [cit. 2012-12-04]. Dostupné z: http://www.portalci.cz/ci-v-praxi/jak-pouzivat-volne-dostupne-nastroje-k-zakladnimu-sledovani-konkurenta-nastin-problematiky-v-cr-a-priklady

MASARYKOVA UNIVERZITA

Děkuji za pozornost.