1. KYBERNETICKÁ BEZPEČNOST

KYBERSPACE SECURITY

Jan Čapek

1.1. ÚVOD

Rozvojem informačních technologií, jimiž chápeme nástroje, prostředky a techniky, které si člověk vyvinul v oblasti výpočetní techniky, telekomunikací a zpracování informací, se vytvořil technologický potenciál, který svými důsledky a možnostmi začíná zasahovat do mnoha oborů lidské činnosti. Informační technologie jsou a vždy budou nástrojem, který lidé mohou používat k tomu, aby lépe a efektivněji vykonávali to, co považují za potřebné či vhodné vykonat. Kvalitativní změna je v tom, že možnosti tohoto nástroje radikálně mění naše dosavadní představy o tom, co je dosažitelné, možné a realizovatelné. Cesta k informační společnosti je podporována současnou technologickou revolucí, která je založena na vzájemném propojení informačních a komunikačních technologiích. Jejím výsledkem je dramatické snížení prostorového a časového omezení a zvýšení přístupu k množství veřejných informací. Oproti předchozím technologickým vlnám je vliv propojených informačních, komunikačních a mediálních technologií charakterizován širokou plošností a vysokou rychlostí pronikání do všech oblastí společnosti. Změny se ve velmi krátké době dotknou prakticky veškerého průmyslu i služeb, veřejného i soukromého sektoru. Vlastně celé společnosti v práci i mimo ni, vzdělávání i zábavy v každodenním životě. Informační společnost tak zásadně změní podnikání, veřejnou administrativu i život každého občana.

Informační společnost je možné chápat různým způsobem. Nejčastěji se můžeme setkat s vysvětlením sociálně ekonomickým; tedy že jde o společnost, která chápe informaci jako základní ekonomický statek a manipulace s ní přináší určitý profit. Mohli bychom samozřejmě sledovat více hledisek - třeba možnost volného přístupu k informacím a jejich zveřejňování nebo míru elektronické komunikace [4].

Nejvýznačnějším rysem informační společnosti je posun od závislosti na interních informačních systémech k systémům využívajících externí komunikace. Internet je konkrétním příkladem (prototypem) informační dálnice a důležitým nástrojem pro rozšíření nových služeb. Splývání informačních, komunikačních a mas-mediálních technologií vytvoří klíčový průmysl tohoto století.

Vidíme postupný nástup nové éry informační společnosti, jejímž základním rysem je vytvoření globální sítě umožňující nejen vzájemnou komunikaci, ale především poskytující velké množství dat. Povýšení infrastruktury z komunikační na informační úroveň je dalším důležitým krokem směrem k informační společnosti. Globální informační infrastruktura umožňující propojení koncových uživatelů bez zprostředkovatelů je klíčem k vytváření a přenosu znalostí. Nejvýznačnějším rysem informační společnosti je posun od závislosti na interních informačních systémech k systémům využívajících externí komunikace. Internet je konkrétním příkladem (prototypem) informační dálnice a důležitým nástrojem pro rozšíření nových služeb. Zavedením služeb cloud computingu mohou organizace mimo jiné zeštíhlit své IT

a také přesunout více energie ke svým hlavním cílům. Cloud computing je tak často k tomuto účelu využíván, přestože cena ve formě důvěry v nové technologie a částečná ztráta kontroly nad IT je zvláště pro evropské zákazníky určitou překážkou

1.2. INFORMAČNÍ BEZPEČNOST

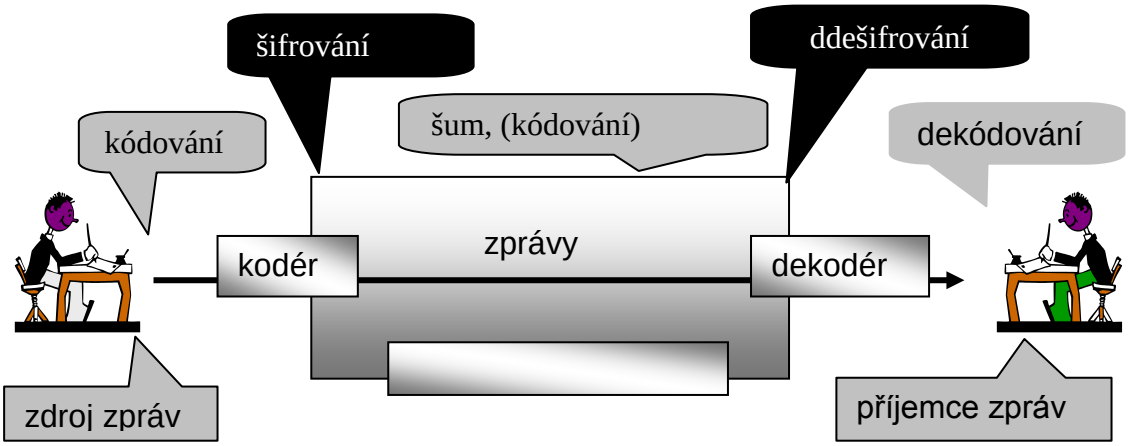
Informace má z pohledu bezpečnosti v zásadě tři hlavní charakteristiky (tzv. bezpečnostní triádu) – dostupnost, důvěrnost a integritu. Informace je dostupná tehdy, když „je pro oprávněné uživatele přístupná v okamžiku její potřeby“. Integrita znamená „zajištění správnosti a úplnosti informací“ – informace jsou tedy příjemci poskytnuty přesné a spolehlivé, a je zabráněno jejich neoprávněné modifikaci. Důvěrnost je chápána jako „zajištění toho, že informace je přístupná nebo sdělena pouze těm, kteří jsou k tomu oprávněni“. Lze ji tedy chápat i jako schopnost zabránit jejímu zneužití někým, komu nebyla určena.

Informační bezpečnosti a jejímu řízení se (podle [1], [2] [3] a [4]) věnuje řada norem. Přestože většina z nich obsahuje řadu různých charakteristik, podle kterých hodnotí míru zabezpečení informace. Normu lze chápat také jako souhrn zkušeností a dobrých praxí, přijatých širokou odbornou komunitou pro tu kterou oblast lidské činnosti. Normy pro bezpečnost informací jsou zaměřeny především na systémy řízení bezpečnosti informací, často označované jako ISMS (Information Safety Management System) [2]. Hlavním směrem v normativním zabezpečení informační bezpečnosti je série ISO (International Organization for Standardization). ISO 27000, která je přehledně uvedena níže.

- ISO/IEC 27000, principy a slovník;
- ISO/IEC 27001, požadavky na ISMS (resp. BS 7799-2:2004);
- ISO/IEC 27002, návody pro zavádění;
- ISO/IEC 27003, analýzy rizik (souvisí s ISO 13335-3);
- ISO/IEC 27004, metriky a měření;
- ISO/IEC 27005, řízení rizik;
- ISO/IEC 27006, kontinuita podnikání a obnova po havárii.

Informační a komunikační technologie se snaží přizpůsobit požadavkům dnes čím dál tím více „mobilních“ uživatelů. Lidé si zvykají pracovat nejen v místě svého zaměstnání, ale také jinde a díky novým zařízením a vyspělým komunikačním technologiím, je jim tento způsob činnosti umožněn. Rozvíjí se online webové aplikace, které díky jednoduchému zprovoznění a intuitivnímu rozhraní ze strany uživatele umožňují vysokou efektivitu práce a vysokou užitnou hodnotu. Jako jeden z příkladů můžeme uvést cloud computing. Zavedením služeb cloud computingu mohou organizace mimo jiné zeštíhlit své IT a také přesunout více energie ke svým hlavním cílům. Cloud computing je tak často k tomuto účelu využíván, přestože cena ve formě důvěry v nové technologie a částečná ztráta kontroly nad IT je zvláště pro evropské zákazníky určitou překážkou.

Spojení mezi jednotlivými informačními zdroji je prostřednictvím komunikačního kanálu, obr.1.



Obr. 1: Komunikační kanál

Zdroj: vlastní zpracování

1.3. INFORMAČNÍ AKTIVUM

Fyzická aktiva: počítačové vybavení, komunikační zařízení (kabeláž, aktivní prvky počítačové sítě, telefonní ústředny, faxy, záznamníky), úložná media (magnetické disky, pásky, CD/DVD nosiče), další technická zařízení (napájecí zdroje, klimatizační zařízení), nábytek, prostory.

Aplikační programová aktiva: aplikační a systémové programové vybavení, vývojové nástroje a utility.

Informační aktiva: databáze, datové soubory, systémová dokumentace, uživatelské manuály, školící materiály, provozní nebo podpůrné postupy, plány obnovy funkčnosti, dohody o zajištění záložního provozu, záznamy z auditů, archivované informace.

Služby: počítačové a komunikační služby, další technické služby (topení, osvětlení, napájení, klimatizace).

Lidé a jejich kvalifikace, dovednosti, zkušenosti, schopnosti řešit dosud neznámé problémy.

aktiva: pověst, image organizace.

1.4. KYBERNETICKÁ BEZPEČNOST

Kybernetická bezpečnost (CyberSecurity) je odvětví výpočetní techniky známé jako informační bezpečnost, uplatňované jak u počítačů tak i sítí. Cílem informační bezpečnosti je ochrana Informací a majetku před krádeží, korupcí, nebo přírodní katastrofou, přičemž informace a majetek musí zůstat přístupné a produktivní jeho předpokládaným uživatelům.

Kybernetickou bezpečnost představuje určitý soubor povinností, zásad a pravidel, jež by měla být závazná pro každého uživatele či provozovatele informačních technologií.

Životní cyklus kybernetické bezpečnosti je znázorněn na obr. 2.

Obr. 2: Životní cyklus kybernetické bezpečnosti.

Zdroj [4]

1.5. KYBERNETICKÁ BEZPEČNOST V ČR

Prezident republiky Miloš Zeman podepsal dne 13. srpna 2014 zákon o kybernetické bezpečnosti a o změně souvisejících zákonů.

V pátek 29. 8. 2014 byl ve Sbírce zákonů pod č. 181/2014 Sb. publikován zákon o kybernetické bezpečnosti.

Zákon o kybernetické bezpečnosti bude účinný od 1. ledna 2015.

Národní bezpečnostní úřad (NBÚ) se stal gestorem problematiky kybernetické bezpečnosti a národní autoritou pro tuto oblast (usnesením vlády č.781 ze dne 19. října 2011) vznik NCKB (Národní centrum kybernetické bezpečnosti) jako součást NBÚ, se sídlem v Brně.

NCKB uvádí, na jakých principech je zákon založen: Zákon je ‚postaven' na dvou zásadách a třech pilířích. První zásadou je minimalizace zásahu do práv soukromoprávních subjektů, druhou zásadou je individuální odpovědnost za bezpečnost vlastních informačních systémů. Tři pilíře tvoří: bezpečnostní opatření (standardizace), hlášení kybernetických bezpečnostních incidentů a protiopatření, tzn. reakce na incidenty. [5]

CERT (Computer Emergency Response Team) je v informatice skupina, která vznikla roku 1988 po aféře s jedním z prvních počítačových červů (Morrisův červ), který ke svému šíření využíval internet (v ČR GovCERT)

CSIRT (Computer Security Incident Respondent Team) je bezpečnostní tým pro koordinaci řešení bezpečnostních incidentů v počítačových sítích provozovaných v České republice.

CSIRT Bezpečnostní tým *CSIRT.CZ* provozuje sdružení CZ.NIC, správce české národní domény, a to na základě memoranda uzavřeného v roce 2012 s Národním bezpečnostním úřadem (NBÚ).

1.6. RIZIKA

Analýza rizik (AR) je klíčovým krokem ve výstavbě informačního bezpečnostního systémy. AR odpovídá na otázky:

- Co nastane, když nebudou informace chráněny?
- Jak může být bezpečnost informací porušena?
- Jaká je pravděpodobnost, že to nastane**?**

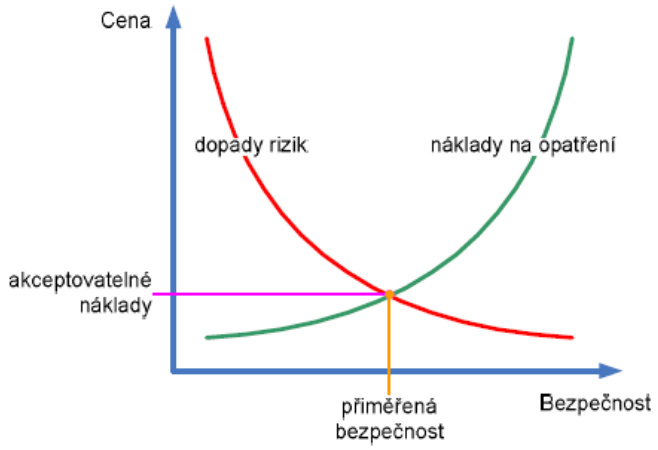
Termíny, s kterými se v kontextu s AR setkáme:
Bezpečnostní cíl, Zranitelné místo, Hrozba, Riziko, Útok, Dopad.
Hrozba – možnost využít zranitelné místo
Riziko – pravděpodobnost využití zranitelného místa (pravděpodobnost uskutečnění hrozby)
Útok – úmyslné (subjektivní útok) nebo neúmyslné (objektivní útok) využití zranitelného místa. Základní typy útoků:
přerušení

a) odposlech
b) změna
c) padělání - zfalšování

Rizika můžeme počítat například podle vztahu:

$$Riziko = \frac{Hrozba \times Zranitelnost \times Dopad}{Protiopatření} \qquad (1)$$

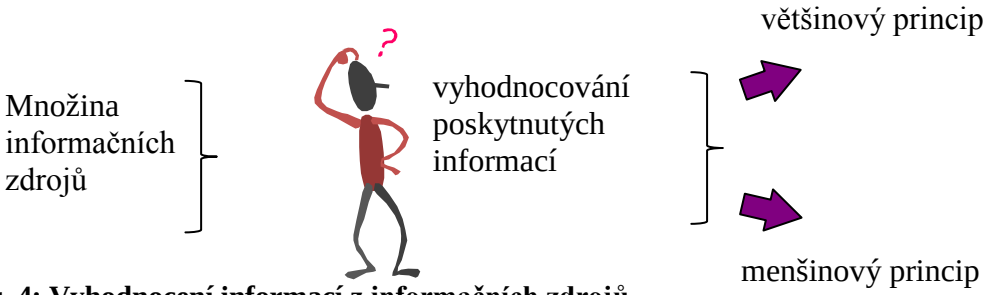
Přiměřené riziko vzhledem k přiměřené bezpečnosti dostaneme podle obr. 3



Obr. 3: Přiměřené riziko vzhledem k přiměřené bezpečnosti

Zdroj: upraveno podle [5]

Informace z množiny informačních zdrojů obvykle nedostaneme úplné tj. ne ze všech možných informačních zdrojů, vlivem informačního přesycení a tak k vyhodnocování použijeme většinový anebo menšinový princip podle obr. 4.



Obr. 4: Vyhodnocení informací z informačních zdrojů

Zdroj: vlastní zpracování

Příkladem menšinového principu je rozhodování za neurčitosti (příklad burzovního spekulanta).

1.7. ZÁVĚR

Kybernetická bezpečnost je neodmyslitelnou součástí dnešní doby, kdy se stále více organizací a podniků nevyhne integraci a závislosti na informačních a komunikačních technologií. Kybernetická bezpečnost se dostává čím dál tím více do popředí podnikových zájmů, důvodem je kyber-terorismus či zneužití informací konkurencí. Podniky si často uvědomují tuto skutečnost až, když přijde první vážný incident, který má za následek finanční ztrátu. V konkurenčním prostředí je nutno tyto hrozby predikovat, minimalizovat a životně důležitá data uchovávat v bezpečí. Bohužel závislost na informačních a komunikačních technologiích platí také pro jednotlivce, kdy se kyber-terorismus stává velkým problémem.

Literatura

[1] DOUCEK, P., NOVÁK, L., SVATÁ, V. *Řízení bezpečnosti informací*. Professional Publishing. Praha 2008. ISBN 978-80-86946-88-7

[2] DRTIL, Jan. Standardy bezpečnosti IS. Praha 4. 3. 2004. In: *Sborník prací účastníků vědeckého semináře doktorského studia FIS VŠE*. Praha: VŠE FIS, 2004, s. 43-51. ISBN 80-245-0706-4

[3] KOSTIHA, F. *Bezpečnost informací*. Ikaros [online]. 2006, roč. 10, č. 5 [cit. 2014-09-01]. Dostupný na World Wide Web: http://www.ikaros.cz/bezpecnost-informaci. ISSN 1212-5075

[4] https://www.kybez.cz/bezpecnost/pojmoslovi

[5] http://www.root.cz/clanky/zakon-o-kyberneticke-bezpecnosti-co-v-nem-stoji/

Kontakt:
Jan Čapek
Ústav systémového inženýrství a informatiky
Fakulta ekonomicko-správní, Univerzita Pardubice
Studentská 95, 53010 Pardubice
capek@upce.cz