Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 9, číslo 78/2007 **1. srpen 2007**

78/2007

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1183 registrovaných odběratelů)

Obsah : str.

Příloha: ne

A. Podzimní *Soutěž v luštění 2007*, úvodní informace

Pavel Vondruška (pavel.vondruska@crypto-world.info)

Vážení čtenáři, **15.9.2007** začne tradiční **podzimní soutěž v luštění jednoduchých šifrových textů o ceny – *Soutěž v luštění 2007***. Obdobné soutěže pořádal náš e-zin v letech 2000 až 2006. V roce 2000 byly úlohy zaměřeny na klasické šifrové systémy. V roce 2001 soutěž pokračovala řešením "moderních" systémů. Soutěže v roce 2003 až 2006 byly z hlediska předložených úloh zaměřeny na řešení úloh od hříček přes jednoduché šifry až po klasické šifrové systémy (jednoduchá záměna, transpozice, periodické heslo, Fleissnerova otočná mřížka, jedno-dvoumístná záměna a šifry prvé a druhé světové války …).

Předloni jsem začal doprovázet úkoly doprovodnými komentáři a nápovědami v NEWS, loni pak jsem přidal vymyšlený doprovodný příběh, který úlohy volně spojoval. Jednalo se o drobné epizody ze života detektiva kapitána Cardy. Příběh vyústil v lov na chameleóna rasy Cryptomelon Pragensis.

Loni se do soutěže zaregistrovalo přes 120 řešitelů, podmínku pro zařazení do losování o ceny (zisk 15-ti bodů) splnily dvě třetiny přihlášených soutěžících (83). Všech 31 předložených úloh vyřešili 4 soutěžící.

Podle e-mailů, které jsem během soutěže a po ní od vás obdržel, dělají doprovodné texty soutěž pro účastníky atraktivnější a mně zase umožňují publikovat texty, které díky této „nápovědě" mohou řešitelé rozluštit. Celá soutěž se tak místo pouhého luštění může stát téměř interaktivní hrou …

Letos bych proto chtěl na tento způsob komunikace s řešiteli soutěže navázat. Mottem bude tentokrát doprovodný fiktivní příběh z doby Marie Terezie. Bude to životní příběh matematika Štěpána Schmidta, který opravdu v osmnáctém století žil, ale ve skutečnosti nebyl kryptologem. Příběh bude využívat reálná data z jeho života a reálie tehdejší doby, ale bude zkombinován s fikcí, která popisuje jeho údajné působení v Černé komnatě – luštitelském pracovišti na tehdejším císařském dvoře.

S textem mi tentokrát pomohl můj bratr, spisovatel historických románů Vlastimil Vondruška (o jeho knížkách viz http://www.royal-glassworks.cz/vondruska/beletrie.php).

Chcete-li si připomenout starší úlohy a jejich řešení (což se vám může hodit i při hledání správného řešení v letošním roce), můžete je nalézt na domovské stránce našeho e-zinu v sekci věnované soutěžím: http://crypto-world.info/souteze.php .

Přesná pravidla soutěže, přehled cen a prvé úlohy najdete v příštím čísle našeho e-zinu Crypto-World 9/2007, který vyjde kolem 15.9.2007. Všechny informace budou dostupné i na našem webu v sekci věnované soutěžím http://crypto-world.info/souteze.php .

Soutěž je určena pouze registrovaným čtenářům našeho e-zinu, do soutěže bude nutné (tak jako v minulých ročnících) se zaregistrovat. Heslo k registraci bude rozesláno společně s kódy ke stažení e-zinu 9/2007.

Doporučená literatura

Vondruška, P: Toulky zajímavými zákoutími kryptologie - Luštitelé z dob Marie Terezie, Technet 7.10.2004 ,
http://technet.idnes.cz/tec_technika.asp?r=bezpecnost&c=A040929_5284148_bezpecnost

B. Štěpán Schmidt (prolog Soutěže 2007)

Pavel a Vlastimil Vondruškovi

Za oknem padal na brněnské ulice těžký vlhký sníh. Končil advent a blížily se Vánoce, ale toho roku léta Páně 1782 byly jiné, než dříve. První rok svobody. Císař Josef II. zrušil nevolnictví a také nenáviděný jezuitský řád. Štěpán Schmidt býval profesorem olomoucké univerzity, kterou spravovali jako jiné školy jezuité. Ještě na jaře přednášel, ale pak se vzdal místa profesora matematiky a odjel do Brna. Byl už stařec a netoužil po ničem jiném, než strávit pár měsíců ve společnosti svého přítele ze studií Josefa Steplinga. I když většina lidí jásala, že nastává nový věk, on sám raději vzpomínal na své mládí.

Nerozuměl už lidem, proč se pachtí za pomíjejícími zbytečnostmi. On sám zasvětil celý život něčemu, co je věčné. Od starověku byla matematika jedinou čistou vědou, na níž nemohla změnit nic církevní klatba ani císařský patent. Bůh mu dal schopnost chápat matematiku lépe než jeho současníci. Mnozí křesťané utráceli svůj talent zbůhdarma, ale on ne. Mohl být na sebe hrdý.

Seděl v křesle a vrásčitou rukou hladil hřbety knih, které věnoval základům matematiky. Ale mnohem větší proslulost mu přinesl útlý spisek, který kdysi sestavil pro stavovskou komisi. To bylo v době, kdy se podle nařízení císařovny Marie Terezie rušily staré české a moravské míry, které byly pro rychlý rozvoj hospodářství zcela nepřehledné a převáděly se na systém vídeňských mír. Šlo o čistě matematický problém, který mu nepřipadal složitý, ale jeho spisek pomohl tisícům lidí. Pokud budou na něho lidé vzpomínat, až zemře, pak určitě právě díky tomuto dílku. A přitom udělal spoustu jiných užitečných věcí. Až se bude psát o Učené společnosti, která byla založena před dvanácti lety v Olomouci, jen málokdo bude vědět, že byl jedním ze zakladatelů. A nejen to. Právě jejich Učená společnost začala vydávat první vědecký časopis v českých zemích.

Jistě, bylo toho hodně, na co mohl být jako učenec pyšný. Ale stejně jako většina jiných lidí vzpomínal nejraději na své mládí. Pocítil trochu nostalgie, neboť právě o téhle době nesměl nikomu vyprávět. A přitom toho tolik zažil! Od mládí byl vynikajícím matematikem. Měl štěstí, že si jeho schopností všiml baron Ignác von Koch, osobní sekretář císařovny Marie Terezie. To mu bylo jen dvacet let a snil o slávě a majetku. Prošel zkouškami a teprve pak se

dozvěděl, že bude pracovat na věcech neuvěřitelně vzrušujících, ale současně přísně tajných. Po krátkém váhání přijal. A tak se stal členem Černé komory, tajného císařského úřadu, který měl na starosti šifrování důležitých císařských dopisů a současně luštění šifer, které používaly jiné královské dvory. Málokdo si uměl představit, jak důležité zprávy procházely jeho rukama. Mohl by s hrdostí vyprávět, kolikrát pomohl válkami zmítané rakouské monarchii. Jenže nesměl. Když v roce 1757 odešel přednášet do Olomouce, musel podepsat slib věčného mlčení.

Odložil knihy na stolek a sepjal ruce. Unaveně zavřel oči a vzpomínal. Jistě, dal slib, že bude mlčet. Jenže copak měl právo pohřbít, co prožil? Ne, nešlo mu o to, aby se chlubil. Ale nikdo by neměl mít právo zatajovat výsledky vědy. A to, co v Černé komoře dělal, byla snad ta nejčistší matematika, jakou poznal. Kdyby tak směl svým žákům ukázat, k čemu se dá matematika použít. Nikdy se toho neodvážil. Ale teď, kdy už stál na prahu smrti, věděl, že nemůže odejít z tohoto podivného, někdy bolestného a přece tak vzrušujícího světa, aniž by nezapsal své vzpomínky.

Zvedl čistý list papíru, uchopil husí brk a seřízl jeho špičku. Namočil ji do inkoustu a chvíli uvažoval, čím vlastně začít. Kdy to vlastně začalo? V Černé komoře? Možná už dříve, během studií. Jeho ruka se váhavě rozběhla po papíru, ale postupně se začala zrychlovat.

- - -

Několik omšelých a zaprášených papírů jsem náhodou nalezl mezi jeho matematickými spisy, které se v olomoucké univerzitě dochovaly. Nejdříve jsem jim nevěnoval patřičnou pozornost, ale jednou večer jsem je otevřel a ihned se do nich začetl. Byl jsem jimi uchvácen. Štěpán Schmidt v nich popisuje své působení v Černé komoře. Kolik důvtipu při luštění tajné korespondence prokázal on a kryptologové dávné rakouské monarchie!

Napadlo mě, že by stálo za to změřit jeho um s umem dnešních zájemců o kryptologii.
Zkuste proto s nimi změřit svou sílu v letošní podzimní Soutěži 2007 i vy!

C. Z dějin československé kryptografie, část II. Československé šifrovací stroje z období 1930–1939 a 1945–1955

Mgr. Karel Šklíba (karel.skliba@crypto-world.info)

Šifrovací stroj ŠTOLBA

Šifrovací stroj ŠTOLBA představoval svou konstrukcí zcela ojedinělé řešení mechanického šifrátoru s vlastní tvorbou hesla. Princip šifrování textu byl sice analogický způsobu šifrování u německého šifrovacího stroje Enigma, ale přenos „signálu“ z klávesnice přes šifrová kola až po tiskový mechanismus byl řešen zcela specifickým způsobem pneumatickým převodem. Šifrátor byl navržen pravděpodobně okolo roku 1930 výborným odborníkem na mechanické konstrukce plk. Ing. Štolbou. Vývoj i výroba zařízení byla utajována, avšak stroj byl údajně patentově chráněn. Vyrobeno bylo asi 50 až 55 kusů, které byly pravděpodobně používány na ministerstvech a u vedení Československé armády. Jeden šifrátor byl údajně přidělen k osobnímu používání prezidentu Edvardu Benešovi. O využití tohoto stroje během 2. světové války není nic známo, v letech 1945 – 1955 byl používán v armádě k výrobě hesla aplikovaného potom v jiných šifrových systémech (na generálním štábu vyráběla na tomto stroji heslo Marie Voleská). V roce 1985 existovaly 2 kusy tohoto šifrovacího stroje, jeden funkční a jeden nefunkční.

Šifrovací stroj ŠTOLBA měl rozměry asi 50 x 30 cm, výška byla asi 25 cm. Vstup otevřeného nebo šifrového textu byl z klávesnice , která byla tvořena pneumatickými mosaznými písty a měla následující tvar:

W E R T Z U I O P
A S D F G H J K L
Y X C V B N M Q

Klávesnice byla umístěna v přední části stroje, písty byly dosti mohutné a při zadávání písmene je bylo nutno prstem silou zamáčknout. Vedle klávesnice se nacházel třípolohový přepínač režimů stroje, který mohl pracovat v režimech:

šifrování	označení přepínače	**Š**
dešifrace	označení přepínače	**D**
psaní otevřeného textu	označení přepínače	**N**

Výstup textu u tohoto šifrátoru byl tiskem na papírový pás, který byl umístěn na válci v horní zadní části stroje. Tisk byl realizován pomocí typů s malými a velkými písmeny latinské abecedy a typový koš se nacházel před válcem s papírem a byl označen REMINGTON.

Šifrátor ŠTOLBA měl celkem 9 kotoučů. Za klávesnicí bylo umístěno 6 hlavních šifrovacích kotoučů, které byly pravděpodobně všechny periody (čili velikosti) 26 a byly všechny označeny písmeny A B C D E F G H I J K L M N O P Q R S T U V W X Y Z. Na kotoučích byla u každé písmenem označené polohy na pravé i na levé straně z boku kotouče dírka. Každá dírka na právě straně kotouče byla uvnitř kotouče propojena kanálkem s právě jedinou dírkou na levé straně kotouče. Tento způsob propojení pravých a levých dírek každého kotouče a pořadí šesti hlavních šifrovacích kotoučů tvořilo dlouhodobé vnitřní nastavení šifrovacího stroje ŠTOLBA. Je pravděpodobné, že ke každému šifrátoru mohla být dodávána nějaká větší sada kotoučů, z níž se pak do šifrátoru vybíralo 6 funkčních kol. Rovněž je pravděpodobné, že kola měla ještě nějaké další značení, pomocí kterého bylo možné kotouče rozlišovat. O tomto značení však nejsou žádné informace. Vzadu za šesti šifrovacími koly byla ještě 3 kola pomocná, která ovlivňovala krokování šesti hlavních kol šifrovacích. Převod mezi třemi zadními a šesti hlavními koly byl pákový, neboť Ing. Štolba preferoval pákové převody před ozubenými koly, jejichž používání z nějakého důvodu neměl rád.

Šifrování u stroje ŠTOLBA bylo samozřejmě off-line a probíhalo následujícím způsobem: Nejprve se všech 6 hlavních šifrovacích kol nastavilo do počáteční polohy podle šestipísmenového hesla, které udávalo krátkodobé vnější nastavení šifrátoru. Pak po zmáčknutí pístu klávesnice označeného příslušným písmenem otevřeného textu se stlačený vzduch dostal odpovídající trubičkou k dírce na pravé straně určité polohy prvního kola, následně prošel určitými kanálkovými propojeními všech šesti hlavních šifrovacích kol a skončil u typového koše, kde uvedl do pohybu typovou páčku odpovídající příslušnému písmenu šifrového textu. Po zašifrování každého jednotlivého písmene se otočením kliky na pravé straně stroje posunula 3 zadní pomocná kola, která způsobila příslušné krokování šesti hlavních šifrovacích kol. Dešifrace se prováděla analogicky.

Myšlenka takovéto pneumatické konstrukce diskového komutátorového šifrovacího stroje byla sice velice pozoruhodná a mezi konstrukcemi šifrátorů pravděpodobně jediná, měla však i řadu úskalí. Stroj musel být konstruován velice precizně, aby v místech

pohyblivých spojů vzduch neunikal a došel pod dostatečným tlakem až ke svému cíli, tedy k příslušné typové páce. Stroj by se velice těžko udržoval v chodu za polních podmínek, neboť byl náročný na čistotu, zejména na čistotu vzduchových kanálků. Šifrátor bylo nutno navíc na mnoha místech pravidelně mazat. Zařízení však nebylo závislé na dodávání elektrické energie, což mohlo v krizových nebo válečných situacích představovat nespornou výhodu. V úvahu nepřipadalo samozřejmě ani žádné parazitní elektromagnetické vyzařování, které bylo značným bezpečnostním rizikem mnoha jiných šifrátorů.

Kromě šifrovacích strojů ŠTOLBA a MAGDA nebyl žádný jiný československý šifrátor v období 1930 až 1955 průmyslově vyráběn ve větší sérii. Všechny ostatní československé šifrátory z tohoto období byly zkonstruovány nejvýše v prototypech jednoho kusu nebo výjimečně nejvýše dvou kusů. V letech 1945 až 1955 se jednalo o zařízení, která představíme ve zbytku tohoto článku.

Šifrovací stroj ŠTOLBA-2

Toto zařízení existovalo pravděpodobně pouze ve výkresu a snad v jednom prototypu (Ing. Štolba měl prototypy svých návrhů šifrovacích strojů uzamčeny ve zvláštním cihlovém přístavku na pracovišti v 5. patře budovy generálního štábu v Dejvicích). Jednalo se asi o zcela mechanický off-line šifrátor, který měl konstrukci analogickou šifrátoru ŠTOLBA, avšak přenos „signálu“ nebyl pneumatický, ale byl mechanický. Každé kolo pravděpodobně o velikosti 26 poloh mělo kolíčky na pravé i levé straně a zasunutí kolíčku u určité polohy na pravé straně kola způsobilo vysunutí kolíčku v nějaké propojené poloze na levé straně kola, což způsobilo zasunutí kolíčku na pravé straně sousedního kola. Tímto způsobem „signál“ doputoval pomocí mechanických převodů až k typovému koši.

Šifrovací stroj KAREL

Šifrovací stroj KAREL byl plně mechanický komutátorový off-line šifrátor, který představoval dále zdokonalenou verzi šifrátoru ŠTOLBA-2. Název KAREL stanovil šéfkonstruktér Ing. Oldřich Hrudka podle jména konstruktéra Karla Bartáka, který na vývoji tohoto stroje pracoval. Šifrovací stroj KAREL byl zhotoven pouze v jediném prototypu, který se do současné doby pravděpodobně nezachoval. V roce 1985 již nebyl úplný a byl již nefunkční.

Šifrátor KAREL měl 6 hlavních šifrovacích kol o velikosti 26 poloh, která byla všechna označena A B C D E F G H I J K L M N O P Q R S T U V W X Y Z. Vzadu byla 4 pomocná kola rovněž velikosti 26 se stejným označením. Zadní pomocná kola ovlivňovala krokování šesti hlavních kol. Kolíčky na hlavních šifrovacích kolech, tj. komutátorech, měly údajně 3 polohy a zasunutím kolíčku na jedné straně došlo k vysunutí kolíčku na straně druhé v místě propojeném lamelou (úzkým páskem). Konstrukce komutátorů byla dosti složitá, neboť na obou stranách byly dvoje otvory pro kolíčky, které byly uspořádány do dvou soustředných kružnic, Vnější kružnici tvořily menší otvory (3mm) a vnitřní kružnici tvořily větší otvory (4mm). Do otvorů se pak osazovaly dvojice kolíčků, vždy jeden slabší a jeden silnější, které byly navzájem propojeny plíškovou pružnou lamelou. Detailní přesný princip pohybu kolíčků v komutátorech není znám.

Vstup textu do šifrátoru KAREL byl pravděpodobně klávesnicí klasického formátu QWERTZ. Výstup textu byl tiskem na pás papíru kde se tiskl najednou (ale odděleně) otevřený text i šifrový text do dvou sloupců širokých 4 pětimístné skupiny. Válec s papírem se pohyboval a narážel pravděpodobně na 2 otáčivá typová kolečka. Stejně jako ŠTOLBA měl i KAREL po straně kliku, kterou bylo nutno otočit po zašifrování každého písmene a která uváděla do chodu 4 zadní pomocná kola, jejichž pohyb pak způsoboval krokování šesti komutátorů.

Další skupinou šifrovacích strojů vyvíjených na generálním štábu Československé armády v letech 1945 – 1955 byly stroje na konstrukčním principu Borise Hagelina, z nichž do výroby byl doveden pouze šifrátor MAGDA. Jednalo se o stroje BOBA, ERA, ELA, VĚRA a HEDA.

Šifrovací stroj BOBA

Šifrovací stroj BOBA byl plně mechanický off-line šifrátor, který měl představovat zdokonalení stroje MAGDA. BOBA měla o jedno heslové kolo víc než MAGDA, měla tedy 6 kol. Na jejím vývoji pracoval konstruktér Zdeněk Pankrác a existovala pouze v jediném prototypu. V roce 1985 již nebyla k dispozici.

Šifrovací stroj ERA

Šifrovací stroj ERA byl dalším zdokonalením šifrátorů MAGDA a BOBA. Jednalo se o elektromechanický off-line šifrátor, který byl vyroben v jediném prototypu a který byl v roce 1985 ve funkčním stavu. Jeho vývoj probíhal v letech 1950 – 1955 a v závěrečné fázi se na něm podílel i Ing. Lubomír Odvárko, který přišel z Aritmy a později dělal šéfa konstrukční skupiny po jejím převedení na Zvláštní správu FMV.

Šifrátor ERA měl přibližně dvojnásobné rozměry než MAGDA. Měl 8 heslových kol s kolíčky. Všechna kola měla velikost 30 a jednotlivé polohy byly označeny

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 1 2 3 4

a vzhledem k nepravidelnému náhonu krokovala tato kola nepravidelně. Buben měl 26 lišt a na každé liště bylo umístěno 6 jezdců. Moleta byla pevná označená reciprokými abecedami

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A Z Y X W V U T S R Q P O N M L K J I H G F E D C B

(pokud byl šifrován text v azbuce, potom byla moleta tvořena reciproce seřazenými 26 znaky azbuky, přičemž měkký znak byl proti měkkému znaku). Pohyb při šifrování nebo dešifraci a při krokování kol byl poháněn elektromotorem s označením 220V / 100W. Vstup textu byl z klávesnice tvaru

Q W E R T Z U I O P
A S D F G H J K L
X Y C V B N M x x

kde x x byly dvě neoznačené klávesy. Pokud byla na klávesnici použita azbuka, tak měla rovněž 26 znaků a 2 klávesy zůstaly neoznačeny. Výstup textu byl tiskem na papírovou pásku. V případě použití azbukového tiskového kolečka byl výstupní text v azbuce.

Šifrátory ELA, VĚRA a HEDA byly zřejmě dalšími variacemi na oblíbenou konstrukci šifrátorů MAGDA, BOBA a ERA a pravděpodobně nebyly ani ve stavu prototypu, nýbrž jen ve výkresech. V roce 1985 žádné stroje s těmito názvy nebyly k dispozici. Zde bych chtěl poděkovat Ing. Zdeňku Křesinovi za cenné rady a poznámky při vzniku tohoto bohužel již jen informačně neúplného textu.

D. Matematizace komplexní bezpečnosti v ČR, část 2.

RNDr. Jaroslav Hrubý, CSc. (hruby.jar@centrum.cz)

4. Bezpečnostní procesy

Bezpečnostní procesy jsou klíčové pro KB a vycházejme z toho, že ve společnosti (ministerstvu, organizaci,firmě…) je velká pozornost věnována procesnímu řízení KB a celé společnosti, jehož závislost na IS/ICT je v současnosti neoddiskutovatelná.

Společnost by měla mít provedeno zmapování vybraných procesů např. dle COBIT a ostatních vnitřních bezpečnostních norem a směrnic, a následně pak je nezbytné zmapovat a zhodnotit (diky závislosti procesů na IS/ICT) v společnost i samotné bezpečnostní procesy IS/ICT dle ISO/IEC 17799, BS 7799-2 (v současnosti série norem ISO/IEC 27000), a to v návaznosti na provedené mapování dle COBITu a ITIL BS 15000.

Jedná se konkrétně o rozpracování v Delivery a Support v COBITu části DS5 a zavedení jejího monitoringu pomocí rozpracovaných dotazníků na bezpečnostní procesy a jejich uplatnění v společnost dle ISO/IEC 17799 (popřípadě aktualizované sérii norem ISO/IEC 27000).

Ve společnosti je KB řízena pomocí IS, a proto je nezbytné zavést ve společnosti systém řízení informační bezpečnosti ISMS (Information Security Management System). Základním smyslem zavedení ISMS ve společnosti, který však musí navazovat na systém nějakého bezpečnostního dohledu (BD) v IS je snížit a dlouhodobě zvládat rizika, vyplývající pro organizaci z provozu IS.

Předpokládáme, že společnost má uloženu a spravovánu značnou část svých aktiv ve formě informací v rámci IS, a proto je nutné zavést bezpečnostní procesy prokazatelně garantující snížení rizik pod hranicí přijatelné míry.

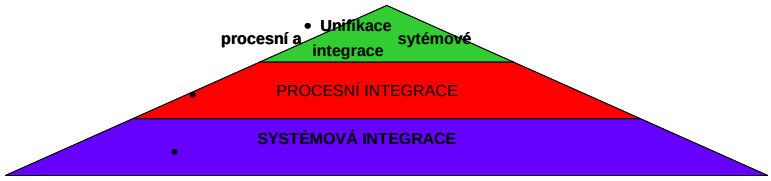
Měli bychom vycházet z toho, že zavedení ISMS v společnost musí být realizováno v propojení se systémem celkového BD v IS, dále se systémem řízení ostatních procesů ve společnosti, a vytvářet tak nedílnou součást KB ve společnost.

Bezpečnostní procesy, které jsou pro systém řízení KB klíčové, musí být provázány s ostatními řídícími procesy v společnost, a to se stává i základem koncepce přístupu pro bezpečnostní analýzu, a pak následnou realizaci projektu ISMS v společnosti.

Pro odůvodnění tohoto lze uvést následující:

V poslední době je možné ve světě zaznamenat zřetelný přechod /a to obzvláště v telekomunikačních službách, které klíčově využívají pro své vlastní řízení a řízení služeb pro telekomunikační společnosti, informační systémy a technologie (IS/IT), včetně jejich vzájemné komunikace (ICT), posun od systémové integrace k procesní integraci, a to na bázi systémově integrovaného IS/ICT.

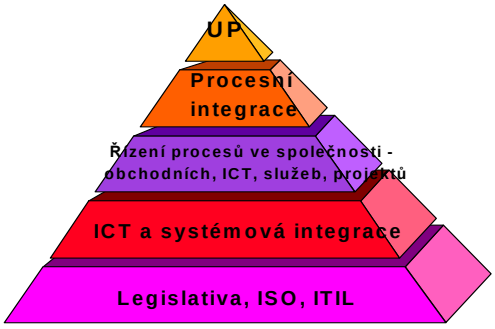
Lze hovořit o unifikaci procesní a systémové integrace:



Obrázek 4 – Procesní a systémová integrace

Špičkové společnosti ve světě se snaží o maximální unifikaci procesů (UP) na bázi platné legislativy s využitím platných norem pro ICT a posledních poznatků v oblasti bezpečnostních věd (např. kryptologie apod.), a to z důvodu konkurenceschopnosti. Struktura vedoucí k UP v organizaci, může být schématicky znázorněna následovně:

Hierarchie vedoucí k UP ve společnosti



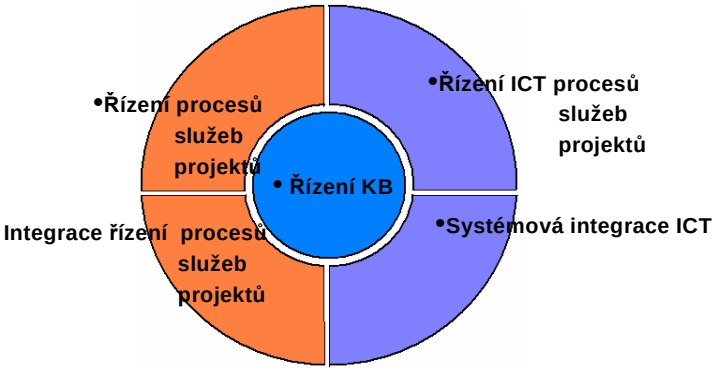
Obrázek 5 – Struktura vedoucí k procesní unifikaci

V současnosti je bezpečnost nedílnou součástí i samotného řízení a vnějších aktivit společnost, a proto řízení komplexní bezpečnosti je klíčové i pro společnost. Úspěšné řešení úkolů společnost musí vycházet z unifikovaných procesů, pro které je garantována komplexní bezpečností a její aktuální znalostí v společnost. To vše musí stát na základě platné legislativy ČR, vnitřních předpisů společnost, a také ISO norem popřípadě knihovny infrastruktury informačních technologií ITIL. Řízení komplexní bezpečnosti je jádrem procesní integrace i UP a provazuje procesní a systémovou integraci i řízení procesů v společnost (viz obr. 6).

Stanovení míry bezpečnosti a bezpečnostních rizik je nedílnou součástí informační, a tedy i KB ve společnost.

Opětovně zdůrazňujeme, že samotné stanovení KB je i každé moderní společnosti závislé na IS/ICT, a tedy není možné ji stanovit, bez znalosti bezpečnostních procesů a jejich provázanosti se všemi ostatními manažerskými procesy v společnost.

Unifikace procesů (UP)



Obrázek 6 – unifikace procesů a řízení komplexní bezpečnosti (KB)

Stanovení míry bezpečnosti a bezpečnostních rizik je nedílnou součástí informační, a tedy i KB ve společnost.

Opětovně zdůrazňujeme, že samotné stanovení KB je i každé moderní společnosti závislé na IS/ICT, a tedy není možné ji stanovit, bez znalosti bezpečnostních procesů a jejich provázanosti se všemi ostatními manažerskými procesy v společnost.

Pro aktuální znalost a řiditelnost procesů a realizaci ISMS v společnost, způsobem, který umožňuje řídit procesy (a veškeré aktivity s nimi související) v reálném čase, je zapotřebí stanovit měřitelnost, kvantifikaci a realizovat matematizaci komplexní bezpečnosti metodikami běžnými v EU i USA, a také v provázanosti s bezpečnostními procesy specifickými pro společnosti v ČR.

Dále je nutná její provázanost s ostatními řídícími procesy ve společnost, tak aby činnost této organizace mohla být efektivně řízena nástroji IS/ICT.

Proto je tedy zároveň nezbytné stanovit měřitelnost, kvantifikaci a realizovat matematizaci všech řídících procesů do jednoho provázaného celku s KB ve společnosti.

Kvantifikace je propojena s matematizací, kterou zde v první fázi např. rozumíme aplikaci statistických metod na soubory bezpečnostních dat a jejich vyhodnocení, výpočet metrik, zjištění korelací apod. (bezpečnostní data se získají v průběhu bezpečnostní analýzy společnosti) a v dalších fázích můžeme pokračovat v dalších metodách, jak je nastíněno ve 3.kapitole.

Tato vize je nezbytná pro realizaci e-managementu a e-administrativy ve společnosti, které by se měla v daném časovém horizontu blížit každá organizace v ČR, jenž chce obstát.Toto by mělo být cílem řízení bezpečnosti a přechodu k vytvoření e-bezpečnosti v celé ČR (v současnosti je to vize, i když řada projektů týkající se realizace elektronických pasů apod. se jí blíží).

Samotná realizace e-administrativy a e-managementu však vyžaduje od společnosti, aby zvolila specifickou optimální cestu pro dosažení tohoto cíle, a to z hlediska vyváženosti vynaložených nákladů na získání zvýšené kontroly, účinnějšího řízení a bezpečnosti ve společnosti.

Toho lze dosáhnout systémově integrovanými nástroji pro řízení všech procesů a nástroji pro BD.

Specifická optimální cesta k tomuto cíli musí právě začít analýzou KB ve společnosti a dopracováním úplné předpisové základny pro celou infrastrukturu této společnosti.

Dále je vždy nutné navázat s ní souvisejícím řízením bezpečnostních procesů a jejich provázaností na procesy ostatními, a to dle platných norem a právních předpisů v této oblasti v ČR i EU.

Je to nejenom proto, že tímto zmapováním společnost získá přehled o stavu bezpečného fungování všech ostatních procesů, ale především proto, že konsolidací KB v prvé řadě zabráníme ztrátám, které způsobuje realizace hrozeb na všechna aktiva společnosti.

Je zřejmé, že KB ve společnosti společnost se sama stává jedním z jejích nejvýznamnějších aktiv, a že informační bezpečnost je nedílnou součástí KB společnosti, a tedy je rovněž součástí všech jejich aktiv.

Lze tedy tvrdit, že dokonalou ochranu a řízení informační bezpečnosti (ve finálním stavu) lze dosáhnout ve společnosti pouze jejím nerozdělitelným vnořením do KB a provázáním všech řídících procesů ve společnost s bezpečnostními procesy a řízením ISMS.

Proto hovoříme o cíli unifikace procesů (UP) ve společnost, řízení informačních rizik a řízení bezpečnostních procesů ISMS, nutných k řízení KB.

Řízení bezpečnostních procesů a zabezpečení monitoringu bezpečnostních procesů musí být v souladu s legislativou ČR (která je v některých částech odlišná od legislativy v Německu – např. zákon o el.podpisu) a v případě bezpečnostních incidentů, umožňuje vrcholovému vedení společnosti prokázat, že ve společnost je prokazatelná bezpečnost a jakým způsobem je tato bezpečnost zajišťována.

Navíc bezpečnostní opatření mají přímé důsledky pro řízení rizik IS/ICT, která jsou provázána přes operační rizika s realizací vnitřních předpisů společnost a případně i bezpečnostní dokumentace organizace, týkající KB dle zákona č. 412/2005 Sb. a vyhlášek NBÚ k tomuto zákonu.

Hlavním cílem bezpečnostní analýzy je vždy navrhnout řešení, jak tedy optimálně řešit a vyřešit problém bezpečnosti provozování IS/ICT, včetně vytvoření a zavedení ITCP, v rámci KB a řízení procesů ve společnosti.

Bezpečnostní analýza má být koncipována tak, aby byla v souladu se stávajícími, ale i budoucími potřebami společnosti, a aby vždy byly její výsledky snadno integrovatelné s výstupy ostatních projektů zaměřených na zavádění procesního řízení organizace společnosti a KB v ní.

Výsledné řešení návrhu řízení bezpečnostních procesů ve společnosti, postavené na bezpečnostní analýze, má být proto maximálně flexibilní a otevřené, při současné minimalizaci nákladů na realizaci takového řešení, jeho budoucí údržbu a rozvoj, a to při současném využití všech existujících investic společnosti do IS/ICT.

Dovolme si pro lepší představu nezbytnosti bezpečnostní analýzy a matematizace KB nastínit dále nezbytnost řešení ITCP (Information Technology Contingency Planning) ve společnosti.

Řešení ITCP musí vycházet z analýzy rozpracování systému řízení informační bezpečnosti (ISMS) a musí dále navazovat na realizaci systému BD ve společnost, který by měl podporovat tento cíl následujícími funkčnostmi:

- zajišťuje sběr informací o bezpečnostně významných událostech,

- provádí průběžné vyhodnocení těchto informací a signalizuje výskyt událostí, které indikují možné překročení přijatelné míry rizika,
- analyzuje a popisuje stav a částečně řídí jednotlivé relevantní bezpečnostní procesy nad celým IS/ICT ve společnosti.

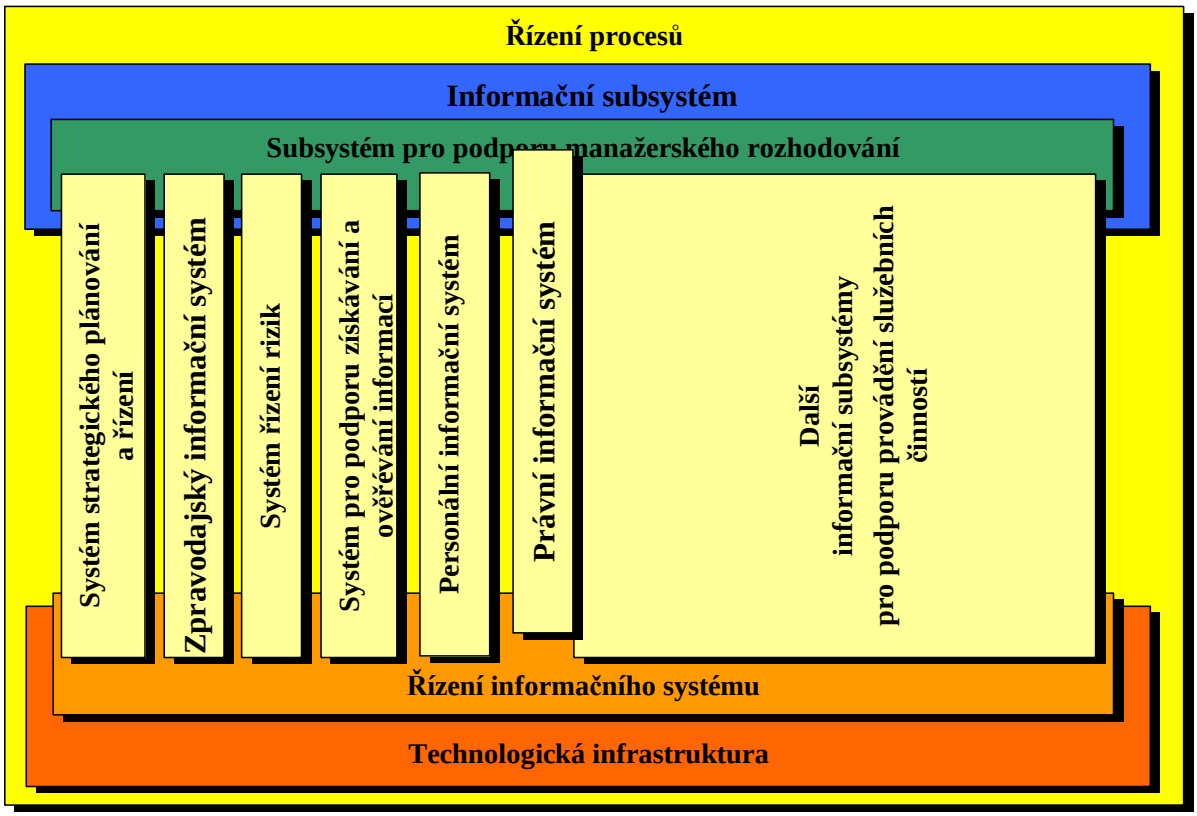
To vše ve smyslu normy ISO/IEC 17799, BS 7799-2:2002 (včetně ostatní legislativy vztahující se k této oblasti), a také pro průběžné zajištění jejího plnění a audit. Navazuje na rozpracování procesů dle COBIT a řídí se tzv. „best practices“ dle ITIL BS 15 000.

Takto bude garantováno dosažení prokazatelné úrovně bezpečnosti IS/ICT a její sledování a řízení ve společnosti, a to dynamicky v čase, a nikoliv pouze staticky.

Navrhované řešení ITCP pak bude jedním z nezbytných kroků společnosti pro řešení problematiky KB. Přitom zvolený způsob i forma jsou otevřené dalšímu vývoji pro naplnění celkové bezpečnostní vize společnost s přijatelným rizikem.

Po provedení bezpečnostní analýzy bude návrh ITCP vycházet z KB a řízení bezpečnostních procesů ve společnosti.

Základním smyslem řízení bezpečnostních procesů a zavedení ISMS v společnost, který musí navazovat na systém BD v IS, je tedy snížit a dlouhodobě zvládat rizika, vyplývající z provozování a organizaci IS/ICT ve společnosti.
ITCP musí vycházet nezbytně vycházet ze správné funkčnosti ISMS, na kterou navazuje.



Obrázek 7 – schématické zobrazení procesního řízení

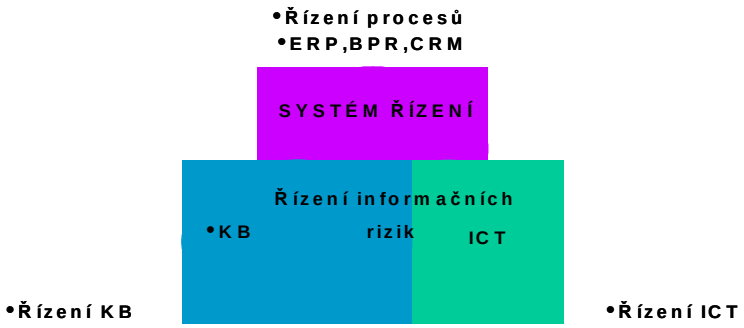
Bezpečnostní procesy, které jsou pro systém řízení KB klíčové, musí být provázány s ostatními manažerskými procesy společnosti. V současné době probíhá všeobecně přechod na procesní řízení ve společnostech, které je zaměřeno na provádění činností společnosti podle předem definovaných postupů. Zároveň je velmi diskutovaná otázka vztahu jednotlivých částí IS/ITC a metod, které slouží k jejich řízení i k řízení celé společnosti včetně procesního řízení.

Pro představu uvádíme v následujícím schématickém zobrazení (obr 7) model (který bude upřesněn dle konkrétních požadavků společnost) přehledu těchto jednotlivých oblastí a jejich základní vazby.

Z tohoto schématu je zřejmé, že procesní řízení ve společnosti je základem, do jehož rámce jsou zasazené a z něhož vycházejí ostatní uvedené oblasti - a to včetně KB, jejích procesů i řízení a funkčnosti organizace.

Je patrné, že při důsledné aplikaci procesního řízení dochází postupně k unifikaci procesů a v důsledku toho ke snižování nákladů na prováděné činnosti, zvýšení KB, fungování společnost a zrychlení činností společnosti tj. poskytovaných služeb, reakcí na události, apod.
Pro zavedení ITCP a jeho procesů v společnost je rovněž zapotřebí stanovit měřitelnost, kvantifikaci v provázanosti s bezpečnostními procesy, a to specifickým způsobem pro tuto organizaci. Dále je nutné zajistit její provázanost s ostatními procesy v společnost tak, aby společnost mohla být efektivně řízena nástroji IS/ICT, a to jako celek.

Proto je zároveň nezbytné stanovit měřitelnost, kvantifikaci a realizovat matematizaci všech řídících procesů společnosti jako provázaného celku s KB.
Kvantifikace je propojena s matematizací, kterou, jak bylo řečeno nejprve rozumíme aplikaci statistických metod na soubory bezpečnostních dat a jejich vyhodnocení, výpočet metrik, zjištění korelací apod. To předpokládá existenci digitalizované bezpečnostní databáze ve společnosti.



Obrázek 8 – Řízení informačních rizik v rámci unifikace procesů (v obr.společnost=komplexní bezpečnost, UP=unifikace procesů)

Vždy budeme vycházet z toho, že samotná realizace ISMS a návrh ITCP je jedním z nezbytných kroků k dokonalé ochraně informací ve společnosti. KB spojuje rovněž všechny

druhy bezpečnosti s informační bezpečností ve společnost a informační bezpečnost ve společnosti se s ostatními vzájemně prolíná v řadě oblastí.

KB ve společnosti musí být realizována bezpečnostními procesy, sjednocenými a provázanými se všemi ostatními procesy ve společnosti, bezpečnostní politikou a bezpečnostní strategií společnost, která musí být integrovaně řízena a ověřitelná auditem.
Proto je nutné pro ITCP vždy znát, jak procesy komplexní bezpečnosti analyzovat, kvantifikovat a řídit, a to skladbou špičkových dílčích SW a HW nástrojů přímo na míru současného stavu řízení procesů ve společnosti.

5. Závěr

V tomto článku jsme se snažili poukázat na potřebu komplexnosti pohledu na bezpečnost a potřebě její kvantitativního hodnocení a matematizaci.

Kvantitativní hodnocení bezpečnosti, matematizace procesu a manažérské bezpečnostní systémy řídící bezpečnost v reálném čase se jeví v současnosti jako jediný způsob, jak efektivně chránit s minimálními náklady toto klíčové aktivum organizace, či společnosti.

Tato tématika je vysoce aktuální v době existence reálných hrozeb v ČR. Problematika unifikovaného hodnocení je v současnosti také aktuální proto, že v ČR dochází k širšímu používání zákona o elektronickém podpisu a vyhlášky k tomuto zákonu (v platném znění).Dochází k realizaci zavádění infrastruktury s veřejnými klíči (PKI) a nejrůznějšími aplikacemi nad touto infrastrukturou a vizí budování e-všechno.

Jsme přesvědčeni, že v ČR je co zlepšovat v mnoha bezpečnostních aspektech z pohledu IS/ICT. Vzhledem k tomu, že při zavádění PKI, popřípadě aplikací nad PKI, se jedná vždy o vnoření IS/ICT podsystému do již existujícího IS/ICT systému, jsou otázky spojené s bezpečným vnořením tohoto podsystému základní.

Zde se hlavně projeví výhoda kvantitativního hodnocení bezpečnosti a její objektivní reálné měřitelnosti, tak jak je popsána v této práci.

Pro důvěryhodný e-stát a bezpečné zrychlení všech procesů v ČR (např. vytvořením e-soudnictví, e-notáře, e-archivnictví apod.) a realizace KB v celé ČR je její matematizace nezbytná.

Literatura:

[1] Hrubý, J.: O kvantifikaci a matematizaci bezpečnosti, Sborník konf.”Informačmí společnost”, prosinec 2001, ISBN 80-86433-07-2

[2] Suchý, O: Honeypot server zneužit k bankovním podvodům, část 1., Crypto-World 7-8/2005

Suchý, O: Honeypot server zneužit k bankovním podvodům, část 2., Crypto-World 9/2005

Honeynet Project: *Know Your Enemy: Phishing*

http://www.honeynet.org/papers/phishing/details/de-honeynet_files/phishing-snort.html

[3] ITSEC, Kritéria pro hodnocení bezpečnosti v informačních technologiích (1990)

[4] ITSEM, Příručka pro hodnocení IT bezpečnosti (1992)

[5] CRAMM Risk Analysis and Management Method, Security Service UK, verze 3.0 (1996)

[6] Hrubý, J.: Unifikace procesů a normy v EU, Crypto-World 11/2003

E. O čem jsme psali v létě 2000 – 2006

Crypto-World 78/2000

Příloha : 10000.txt , soubor obsahuje prvních 10 000 prvočísel (další informace viz závěr článku "Fermatův test primality, Carmichaelova čísla, bezčtvercová čísla" , str.9) .

Crypto-World 78/2001

Příloha : priloha78.zip (dopis pana Sůvy - detailní informace k horké sazbě, viz. článek Záhadná páska z Prahy, Crypto-World 6/2001)

Crypto-World 78/2002

Crypto-World 78/2003

Crypto-World 78/2004

Crypto-World 78/2005

Crypto-World 78/2006

F. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:
http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	Jaroslav.Pinkava@zoner.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info ,	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/