Kybernetická bezpečnost

Research · April 2015

DOI: 10.13140/RG.2.1.2435.0247

1 author:

Petr Hrůza
Univerzita Obrany
16 PUBLICATIONS **24** CITATIONS

SEE PROFILE

UNIVERZITA OBRANY
Fakulta ekonomiky a managementu

Kybernetická bezpečnost II

Petr HRŮZA a kolektiv

Brno, 2013

Kybernetická bezpečnost II

Ing. Petr HRŮZA, Ph.D. *(kapitola 1 a 2)*
Ing. Jaromír PITAŠ, Ph.D. *(kapitola 3)*
Ing. Jaroslav ŠANDA *(kapitola 4)*
doc. Ing. Bohumil BRECHTA, CSc. *(kapitola 5)*

Recenzenti:
doc. Ing. Vladimír VRÁB, CSc.
doc. Ing. Vlastimil MALÝ, CSc.

Tato odborná kniha byla vytvořena a financována z projektu „Vzdělávání pro bezpečnostní systém státu“ CZ.1.07/2.2.00/15.0070. Projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

Tato odborná kniha byla doporučena k publikaci vědeckou redakcí vydavatelství MONIKA Promotion s.r.o., Praha.

ISBN 978-80-7231-931-2

Obsah

Abstrakt

S nárůstem používání informačních technologií stoupá riziko jejich zneužití. Cílené útoky proti informačním technologiím jsou celosvětovým fenoménem a jejich dopad způsobuje rozsáhlé ekonomické škody ve veřejném i v soukromém sektoru. Co je kybernetická válka a jaké jsou její metody? V knize najdete odpovědi na tyto otázky. Důležitou součástí kybernetické bezpečnosti je řízení rizik. Kryptografické techniky jsou jediný způsob ochrany přenášené informace. Z kryptografie se postupně stává důležitý bezpečnostní nástroj. Fenoménem dnešní doby je používání mobilních zařízení.

Klíčová slova:

Kybernetická bezpečnost, kybernetická válka, kryptografie, riziko, proces hacker, botnet, komunikační systém.

Abstract

Together with the increase of using the IT we can mark an increased risk of misusing these technologies. Attacks aimed against the IT assets and networks are becoming a worldwide phenomenon and their impact result to extensive economic damage throughout both public as well we private sectors. What is the cyber war and what are their methods? Answers to all these questions are subject elaborated in book. The risk management is an important part of cyber security. Cryptographic techniques are the only way to protect the transmitted information. Cryptography is gradually becoming an important safety tool. The use of mobile devices is today phenomenon.

Key words:

Cyber Security, Cyber War, Risk, Process, Cryptography, Hacker, Botnet, Communication System

Úvod

Informační a komunikační technologie se staly nepostradatelnou součástí dnešního moderního životního stylu. Občané jsou denně závislí na informační a komunikační infrastruktuře při řízení společnosti, podnikání a výkonu svých práv a svobod, ale také v soukromém životě. Proto od informačních systémů očekáváme dostupnost, integritu a důvěrnost systému. V dnešní době platí, že klíčové informace mohou mít cenu zlata. Neexistuje organizace (komerční subjekt nebo orgán veřejné správy), která by nějakými důležitými informacemi nedisponovala.

Obecným trendem na celém světě je **kvalitní ochrana informačních technologií před útoky**, které by mohly ohrozit jejich fungování. Cílené útoky proti informačním technologiím jsou celosvětovým fenoménem a jejich dopad způsobuje rozsáhlé ekonomické škody ve veřejném i v soukromém sektoru, a to jak v národním tak v globálním měřítku. V případech, kdy je útok veden proti prvkům kritické infrastruktury, může být v konečném důsledku ohrožena bezpečnost nebo samotná existence státu. Zajištění kybernetické bezpečnosti jednotlivých států je jednou z klíčových výzev současné doby. Bezhraničnost a všudypřítomnost kybernetických hrozeb vyžaduje intenzivní mezinárodní spolupráci a také intenzivní úsilí při zajišťování kybernetické bezpečnosti jednotlivých států. Každý uživatel informačního systému (informační infrastruktury) ovlivňuje úroveň národní informační a komunikační infrastruktury proti kybernetickým hrozbám.

Oblast **kybernetické bezpečnosti** je a bude jedním z určujících aspektů bezpečnostního prostředí vyspělých zemí. Stále větší část ekonomických aktivit se přesouvá do prostředí Internetu - do kyberprostoru. Vznikem sociálních sítí se z nejznámější části kyberprostoru (Internetu) stává významný celospolečenský jev, jehož prostřednictvím lze společnost výrazně pozitivně nebo i negativně ovlivňovat. Kybernetická bezpečnost je mezinárodní problém, který vyžaduje mezinárodní spolupráci za účelem úspěšně dosáhnout přijatelné úrovně bezpečnosti na globální úrovni.

Důležitou součástí kybernetické bezpečnosti je **řízení rizik**. Cílem řízení kybernetických rizik je snížení pravděpodobnosti působení hrozeb, snížení

dopadů působení hrozeb, vyhnutí se rizikům nebo jejich přenesení (sdílení) spolu s efektivním využitím zdrojů pro jejich zvládnutí. Je však třeba si uvědomit, že veškerá **rizika kybernetické bezpečnosti** lze eliminovat pouze tak, že nebudeme využívat síťová připojení Intranetu i Internetu, přenášet data na discích a dalších paměťových médiích. Eliminaci veškerých rizik v době sdílení dat, on-line komunikaci, celkové závislosti soudobé moderní společnosti na výpočetní technice a všudy přítomnému Internetu nelze realizovat (stejně jako v dalších oblastech našeho života). Rizika tu byla již od prvopočátku, jsou a v budoucnu budou. Je třeba se pouze naučit je zvládat.

V přenosovém prostředí, které je z vzhledem ke své rozlehlosti a otevřenosti volně přístupné útočníkovi, představují **kryptografické techniky** jediný způsob ochrany přenášené informace. Z **kryptografie** se postupně stává bezpečnostní nástroj, který je neodmyslitelnou součástí veškerých informačních a komunikačních systémů. Šifrování již není doménou pouze utajovaných informací a umožňuje zamezit útokům i v Internetu. Pomocí šifrování lze data nejen ochránit před jejich únikem, ale též odhalit jejich modifikaci útočníkem.

Fenoménem dnešní doby je používání **mobilních zařízení**. Zdaleka nejde již pouze o telefonní přístroje. Používají se tzv. chytré telefony, smartphony, ultrabooky, netbooky, tablety a další technické vymoženosti. Jejich hardwarové vybavení je předurčuje pro činnost v bezdrátovém komunikačním prostředí. Využívají se nejen pro zábavu, ale i pro práci. Umí realizovat bankovní operace. Mnoho uživatelů si neuvědomuje, jak snadno jsou jejich osobní data zneužitelná.

Cílem této odborné publikace je poskytnout základní přehled o problematice kybernetické bezpečnosti. Publikace je především určena pro širokou odbornou veřejnost, která se chce o kybernetické bezpečnosti dozvědět základní a obecné informace. Může posloužit jako výchozí studijní materiál pro studenty na všech typech středních a vysokých škol v předmětech se zaměřením na informační a komunikační systémy a jejich bezpečnost. Kniha reaguje na fenomén dnešní doby, kterým kybernetická bezpečnost bezesporu je, a odráží aktuální aspekty této oblasti. Proto i platnost a aktuálnost informací v této publikaci je závislá na dalším vývoji popisované problematiky.

Publikace je rozdělena do pěti kapitol, které na sebe bezprostředně navazují.

První kapitola objasňuje vnímání kybernetického prostoru (kyberprostoru - Cyberspace). V kyberprostoru je ale několik nejasností. V této kapitole je možné se dočíst o definici, rozměrech, hranicích, pravomocích a odpovědnosti v kyberprostoru.

Druhá kapitola pojednává o kybernetických válkách. Dále se v kapitole dozvíte o doposud známých nebezpečných škodlivých počítačových programech využívaných pro špionáž, o plánech na kybernetické války, o metodách kybernetických válek a o možných budoucích kybernetických válkách.

Třetí kapitola se zabývá procesem řízení rizik s aplikací na řízení rizik kybernetické bezpečnosti s dodržením zásad řízení rizik a opatřeními na chyby současné praxe. Proces popsaný v ISO normách a dalších známých publikacích je v kapitole rozšířen o agregaci rizik do celkového rizikového profilu pro jasnější uchopení celého procesu manažery na všech úrovních.

Čtvrtá kapitola přináší stručný přehled vývoje kryptografických algoritmů a obecných principů jejich fungování. Smyslem uvedených informací je pochopení základů a pojmového aparátu pro možné další studium detailního principu fungování kryptografických algoritmů. Po seznámení s obsahem této kapitoly by čtenář měl získat jasnou představu o bezpečnostních službách, které lze s využitím kryptografie dodatečně realizovat v již provozovaných informačních systémech.

Pátá kapitola seznamuje čtenáře s možnostmi útoků kyberzločinců na mobilní zařízení včetně způsobů zneužití osobních dat pro přístup k jejich finančním zdrojům. Ukazuje na některá slabá místa volně přístupného komunikačního prostředí jako brány pro hackery.

1. Kyberprostor

Zformulovat jednoznačnou definici kybernetického prostoru není vůbec jednoduché. Ale začněme od začátku. Pojem **kyberprostor (*Cyberspace*)** se poprvé objevil v roce 1982. Tento termín vymyslel americko-kanadský spisovatel **William Gibson**, který ho následně použil ve své povídce s názvem „*Burning Chrome*". Termín kyberprostor pak začalo pro své myšlenky a díla používat mnoho dalších autorů.

Jako první, kdo tento termín použil v souvislosti s existujícími počítačovými sítěmi, byl **John Perry Barlow** (spoluzakladatel organizace Electronic Frontier Foundation). John Perry Barlow kyberprostor definoval jako symbolický prostor komunikace, kde komplexnost tohoto prostoru záleží na vyspělosti technologie.

Antropolog **David Hakken** (v devadesátých letech), v návaznosti na John Perry Barlowa, charakterizuje kyberprostor jako sociální arénu, do které vstupují všichni sociální aktéři, kteří používají ke vzájemné sociální interakci pokročilé technologie. Podle něj kyberprostor umožní vznik dalších sociálních forem a definuje jej jako distinktivní typ kultury.

Computer Science and Communications Dictionary (již v roce 2001) definuje kyberprostor jako nehmotný svět informací, který vzniká vzájemným propojením informačních a komunikačních systémů. Toto prostředí umožňuje vytvářet, uchovávat, využívat a vzájemně si vyměňovat informace. Zahrnuje počítače a databáze propojené komunikačními systémy, jako například celosvětovou síť Internet. [6] **Leo Troy** (v roce 2003) připisuje kyberprostoru nové možnosti komunikace, jako jsou například emaily, webové stránky, počítačové sítě, telefony, faxy a videokonference. [3] **Sofia Tzimopoulou** (v roce 2006) popisuje kyberprostor jako imaginární místo, na které se nevztahují omezení fyzického světa. To mimo jiné umožňuje vznik nových identit. Uživatel opouští své fyzické tělo a pobývá v tomto prostředí bez něj. [4]

Kyberprostor lze chápat jako metaforu vyjádření virtuálního (nefyzického) prostředí vytvořeného propojením počítačových systémů v síti. V kyberprostoru probíhá vzájemné působení mezi subjekty stejně jako v reálném světě, ovšem bez nutnosti fyzické aktivity. Informace jsou sdíleny v reálném čase či s určitým zpožděním, lidé mohou nakupovat

zboží, sdílet zkušenosti, prozkoumávat obsah, provádět výzkum, pracovat nebo si hrát. [1] Kyberprostor lze definovat také jako prostředí, v němž se informace vytvářejí, zpracovávají, ukládají a šíří pomocí elektromagnetického vlnění. Obecně si ho můžeme představit jako **virtuální svět vytvořený moderními technologickými prostředky**.

V současnosti bývá termín kyberprostor vykládán různými způsoby. V současné době nenajdeme žádnou stoprocentně platnou definici, která by zahrnovala vše a kterou by bylo možné jednotně a bez výjimek používat. I když se některé názory liší, většina definic se shoduje v tom, že **kyberprostor je nefyzickým místem, kde se nacházíme během komunikace zprostředkovanou moderními technologiemi** (např. počítačem).

Využívání kybernetického prostoru a souvisejících technologií v dnešní době ovlivňuje celou společnost. Význam sociálních síti pro sdílení informací a pro virtuální kontakt s přáteli představuje zcela nový rozměr. Z politologického hlediska představuje kybernetický prostor zcela nový koncept veřejného místa, kde lidé mohou sdílet své politické názory a být občansky aktivní.

1.1. Nejasnosti v kyberprostoru

Je v kyberprostoru vše jasné a přesně definované? Opak je pravdou, není jasného skoro nic. Jaké jsou tedy nejasnosti v kyberprostoru? Mezi hlavní nejasnosti lze zařadit:

- definici,
- rozměr (konečný, nekonečný),
- hranice (státy, organizace),
- pravomoc a odpovědnost.

1.1.1 Definice

První nejasností je **definice**. O nejasnosti definice jsem se již zmínil a mohli jste si o ní přečíst na předcházející stránce. Obecně si kyberprostor můžete představit jako **virtuální svět vytvořený moderními technologickými prostředky, v němž se informace vytvářejí, zpracovávají, ukládají a šíří pomocí elektromagnetického vlnění**.

1.1.2 Rozměr

Další diskutovanou nejasností je jeho **rozměr**. Má kyberprostor vůbec nějaký rozměr? Je jeho rozměr konečný nebo je nekonečný? Kde je začátek a kde konec? Kyberprostor stejně jako virtuální realita prezentují virtuální světy, ve kterých se mohou uživatelé či návštěvníci pohybovat a které mohou prozkoumávat. I když jsou si významy pojmů kyberprostor a virtuální realita podobné a místy velice blízké, ve skutečnosti se od sebe ale liší. Virtuální realita je softwarový program, který simuluje realistické prostředí, u kterého jsou hranice určeny programátorem. Na rozdíl od virtuální reality **kyberprostor nemá přesně určený rozměr**. Jedná se o síť navzájem propojených počítačů bez začátku a konce.

1.1.3 Hranice

Další diskutovanou nejasností jsou jeho **hranice**. Má kyberprostor vůbec nějaké hranice? Všichni známe slogan „*Internet nezná hranic*“. Jak je to ale s hranicemi kyberprostoru? Úplně stejné. **Kyberprostor také nemá ve skutečnosti žádné smysluplné geografické hranice**. To je a také bude problém při řešení právních sporů mezi státy či subjekty v různých zemích. Proto někteří právníci navrhují dodržovat i v kyberprostoru národní hranice jednotlivých států. Ve vznikající globální informační infrastruktuře se budou čím dál hůře řešit otázky kybernetické kriminality/kybernality (kybernalitu lze chápat jako kybernetickou kriminalitu, kriminalitu v kyberprostoru nebo jako narušení pokojného stavu v kyberprostoru). V dnešní době jsou patrné rozdíly v právních předpisech jednotlivých států a v jejich veřejné politice. V sociálních, kulturních a náboženských hodnotách jsou tyto rozdíly ještě větší. Ale kyberprostor tyto rozdíly nevnímá a neohraničuje. Internet umožňuje tok jakéhokoliv dat převoditelných do jedniček a nul nepozorovaně a téměř nekontrolovatelně přes hranice států. Některé státy se snaží omezovat či cenzurovat Internet. Zatím jsou v cenzuře docela úspěšné. Příklady několika států s přísnou cenzurou dále uvádím.

Například Čínská lidová republika důmyslným systémem blokuje přístup uživatelů na svém území k některým serverům. Fyzický přístup do Internetu je poskytován několika státem licencovanými a kontrolovanými

poskytovateli. Při pokusu o připojení k zakázané webové stránce se objeví uživateli neutrální chybová hláška, která mu oznámí, že z důvodu technické závady se k serveru nelze připojit.

Další zemí s přísnou cenzurou je Irán. Blokovány jsou například stránky Wikipedia, New York Times, YouTube, Facebook, Twitter, dále stránky obhajující ukončení praktik kamenování žen a jakékoliv stránky zabývající se propagací práv a rovnoprávnosti žen apod.

Většina těchto zemí používá k internetovému filtrování známý filtrovací programu SmartFilter. Pouze Čínská lidová republika k internetovému filtrování používá vlastní filtrovací program.

Například na Kubě a v Severní Koreji je systém cenzury Internetu podobný. Používání Internetu je zakázáno úplně. Jen prověřené osoby mohou získat povolení k používání Internetu, jako jsou například doktoři či státní úředníci.

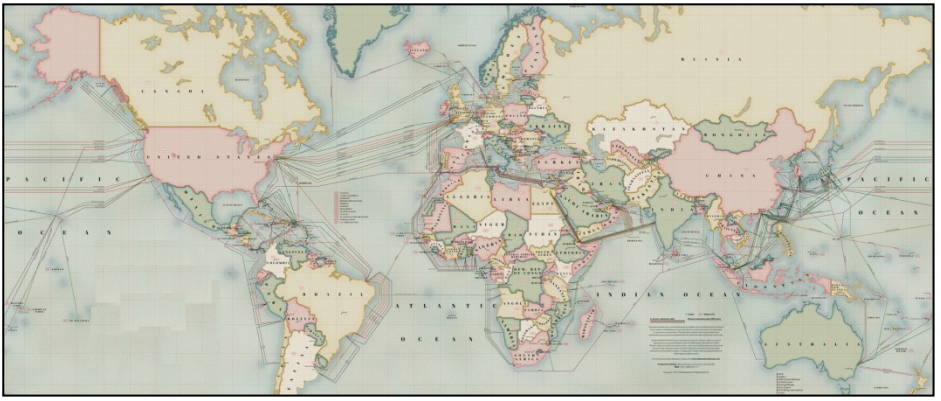
Takto bych mohl jmenovat i další státy, kde dochází k cenzuře Internetu, jako jsou například Spojené arabské emiráty, Saudská Arábie, Egypt, ale i Rusko či Austrálie.

Ale zpět k **hranicím** Internetu. Internet je celosvětový systém navzájem propojených počítačových sítí, ve kterých mezi sebou počítače komunikují. Internet s sebou přinesl mnoho nového do každodenního života lidí na celém světě. Z univerzitní sítě využívané k vědeckým a vojenským účelům se vyvinula síť celosvětová, která díky svým specifikům umožňuje spojení lidí bez ohledu na geografické vzdálenosti. Díky těmto charakteristikám přispěl Internet k nebývalému rozvoji přeshraničního styku. Pro běžného uživatele je téměř nemožné zjistit, v jakém státě se nachází server, na němž je prohlížená stránka uložena. Vzhledem k nestálosti a nejednoznačnosti tohoto umístění je vyvozování jakýchkoliv důsledků pro právo právě z umístění serveru nevhodné. Pozici běžného uživatele při určování geografického umístění provozovatele stránky či dokonce stránky samotné ztěžuje neexistence spolehlivého zeměpisného identifikátoru webové stránky či emailové adresy.

Komunikace na Internetu probíhá buď po kabelu, nebo se šíří vzduchem. Mezi kontinenty se data přenáší buď pomocí satelitního (prostřednictvím družic) spojení nebo tzv. podmořskými kabely. Družice jsou drahé, mají

velmi omezenou kapacitu, jejich životnost je přibližně 15 let a při jejich použití dochází ke zpoždění signálu vlivem překonávané vzdálenosti. Podmořské kabely jsou sice také drahé, ale ve všem ostatním družice předčí. Navíc oproti družicím mají tu výhodu, že je lze poměrně snadno a rychle opravit. Což je pro nepřetržitou funkčnost systému velice důležitý faktor.

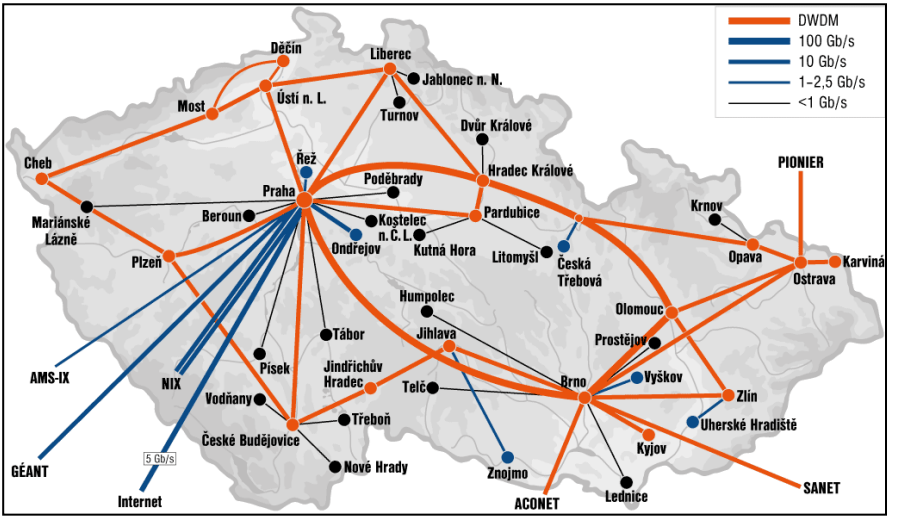
Na následujícím obrázku je vyobrazeno vzájemné propojení kontinentů pomocí podmořských kabelů. Jak je z obrázku patrné, není už dnes tak snadné odříznout část světa od Internetu pouhým přerušením kabelu. Těch obvykle na stejné trase vede více nebo vždy existuje přenos dat přes další kabel.



Obrázek 1- Mapa podmořských kabelů platná v lednu 2013
(Zdroj: http://submarine-cable-map-2013.telegeography.com/).

Jak je tomu ale na pevnině? Na pevnině je kabelů mnohem více. Na delší vzdálenosti se dnes obvykle používají optické kabely, které jsou tažené souběžně s jinými liniovými stavbami (dálnice, železnice, elektrická rozvodná síť, potrubní vedení apod.). Ve městě se většinou využívají kolektory, tunely metra apod. a vedení tvoří mnohem hustší síť. Jednou z provozovaných sítí v České republice je síť nazvaná CESNET2. CESNET2 je národní vysokorychlostní počítačová síť určená pro vědu, výzkum, vývoj a vzdělávání. Propojuje největší univerzitní města České republiky s vysokými přenosovými rychlostmi. Uživateli sítě jsou především vysoké školy, Akademie věd České republiky, ale i některé střední školy, nemocnice či knihovny. Na následujícím obrázku je

zobrazena topologie sítě CESNET2 (z konce roku 2012). CESNET2 má bohaté spojení také se zahraničím. Klíčové je napojení na evropskou síť GÉANT (kapacit 10 Gb/s). S běžným (komerčním) Internetem komunikuje síť CESNET2 prostřednictvím linky vedoucí přímo do USA, jejímž dodavatelem je společnost Telia. Její rychlost je 5 Gb/s a může být snadno podle potřeby navýšena. Dále je síť propojena se třemi sítěmi národního výzkumu a vzdělávání v sousedních státech. Jedná se o sítě SANET (Slovenská republika, 10 Gb/s), ACONET (Rakousko, 10 Gb/s) a PIONIER (Polsko, 10 Gb/s). [5]



Obrázek 2- Topologie sítě CESNET2 platná v lednu 2013
(Zdroj: https://www.cesnet.cz/wp-content/uploads/2012/10/cesnet2-topo1.gif).

1.1.4 Pravomoc a odpovědnost

Kdo má jakou **pravomoc** a kdo za co **odpovídá** v kyberprostoru? Toto jsou otázky velice diskutované na celém světě a hlavně ve vyspělých státech světa. Vlády jednotlivých států chtějí mít nad Internetem úplnou kontrolu, včetně odposlouchávání informací. Kdo má mít pravomoc „*vypnout*" nebo „*odposlouchávat*" Internet? Tuto rozhodovací pravomoc má mít prezident, představitel státu, vláda, ministerstvo nebo specifická společnost či firma? Vlády jednotlivých zemí požadují mít možnost změnit či zamezit přístupu k některým službám nebo webovým serverům. Kybernetickou bezpečnost pak vlády vyspělých států vnímají jako národní politickou záležitost,

protože nezákonné použití kyberprostoru může bránit rozvoji hospodářské, ekonomické a národní bezpečnostní činnosti. Proto občané od vládních institucí očekávají především udržování sociálního pořádku, ochranu životů a majetku. Z tohoto důvodu by vlády měli používat všechny nástroje národní moci ke snížení kybernetických rizik. Z toho vyplývá, že státní představitelé jsou zodpovědní i za kybernetickou bezpečnost.

Velký posun ve vnímání problému kyberkriminality je možné spatřit v posledních letech v koncipování nových organizací, které se aktivně zabývají ochranou kyberprostoru. V poslední době se stále častěji používá v politických diskusích pojem „státní příslušník kybernetické bezpečnosti". Stále více se s tímto pojmem setkáváme, ale zatím není přesně definován. Je to osoba nebo skupina osob zaměřená na národní kybernetickou bezpečnost? Jednou z těchto skupin osob jsou bezpečnostní týmy typu **CERT** (Computer Emergency Response Team) nebo **CSIRT** (Computer Security Incident Response Team). Obě zkratky možno chápat jako **tým, který je ve svém jasně definovaném poli působnosti zodpovědný za řešení bezpečnostních incidentů.** Z pohledu uživatelů nebo jiných týmů se tedy jedná o místo, na které je možno se obrátit se zjištěným bezpečnostním incidentem nebo jen s podezřením na bezpečnostní incident. **CSIRT týmy** vznikají na úrovni jednotlivých organizací, které zprostředkovávají chod Internetu (poskytovatelé služeb a obsahu), nebo které prostředí Internetu používají ke své hlavní činnosti (např. banky, e-shop, e-aukce). Základní povinností každého CSIRT týmu je spolupráce při řešení incidentů. Obvykle CSIRT tým řeší problém, který se vyskytne v okruhu jeho pole působnosti (např. vlastní síťové infrastruktury). Je to vždy v místě, kde má tento tým reálné možnosti k zásahu. [7]

Národní CSIRT tým plní funkci tzv. **poslední instance**, u které je možné žádat o **pomoc** a o **zásah**. Cílem národního CSIRT týmu je v rámci státu nebo oblasti působení zprostředkovat kontakt mezi napadeným a původcem problému. Národní týmy (většinou) nevlastní fyzickou infrastrukturu, takže nemají možnost přímého zásahu. Jejich role spočívá ve zprostředkování kontaktu, eventuálně v koordinaci (odtud taky název týmu ***koordinační***) postupu jednotlivých řešitelů v případě, že problém je

rozsáhlejší a jeho řešení vyžaduje spolupráci více složek daného státu či oblasti působení. [7]

Realizace, údržba a zlepšování **národní kybernetické bezpečnosti** se skládají z řady prvků, které by měly být součástí strategických dokumentů politické povahy, zákonů, předpisů, organizačních a administrativních opatření (jako jsou komunikace a postupy pro řešení krizí v rámci státu, ale i ryze technických ochranných opatření). Každý vyspělý stát vnímá rozdílně svoji národní kybernetickou bezpečnost s ohledem na svůj právní rámec, historické a politické kontexty, vládní strukturu, organizační struktury, procesy krizového řízení a mentalitu. Nejvíce se zapomíná na zvyšování povědomí, vzdělávání, výchovu, cvičení a mezinárodní spolupráci jako jeden z důležitých prvků národní kybernetické bezpečnosti. [2]

Při útocích na prvky kritické infrastruktury státu, by vláda postiženého státu měla vyhlásit stav nebezpečí. Pak by administrátoři serverů a správci sítí pravděpodobně převzali pravomoci, které má dnes jen policie. Poskytovatelům Internetu by pak pod hrozbou pokut mohli nařídit, aby problémy ve své síti vyřešili. Třeba i za cenu odpojení napadených počítačů. Za provoz Internetu odpovídají provozovatelé Internetu.

Při potížích s internetovým připojením se uživatel již nyní musí obrátit na poskytovatele internetového připojení a ten pak, pokud je jiný než provozovatel tohoto připojení, na provozovatele internetového připojení.

Bezpečnostní incidenty, kybernetické útoky a trestná činnost páchaná prostřednictvím informačních a komunikačních technologií v reálném i virtuálním světě nabývají na stále větší intenzitě a závažnosti. Výrazným odlišením této kyberkriminality od ostatních druhů kriminality je její vysoká latentnost, anonymita pachatele a jeho často obtížná identifikace, ale také značná míra tolerance společnosti. Vzrůstá tak potřeba tvořit, zformovat a zefektivnit obranu proti těmto útokům, zlepšit prostředí pro dohledání pachatelů a také vzdělávat uživatele. Hlavně uživatelé by měli být schopni rozpoznat hrozby a rizikové situace a vypořádat se s nimi. [2]

Každý uživatel informačního systému (informační infrastruktury) ovlivňuje úroveň národní informační a komunikační infrastruktury proti kybernetickým hrozbám. Ač si to běžní uživatelé nemusí ani uvědomovat,

jejich role při boji s kybernetickými útoky a obecně v oblasti bezpečného provozu sítí a služeb je nezanedbatelná. To oni jsou pověstným lidským faktorem, který často rozhoduje o účinnosti kybernetických útoků. Ne nadarmo se říká, že koncový uživatel je klíčem k bezpečnosti. Mnoho uživatelů bohužel přistupuje k otázkám bezpečnosti výpočetní techniky poměrně laxně, obvykle se slovy „Já nejsem pro nikoho zajímavý, tak co!“. Často to jsou právě špatně zabezpečené pracovní počítače koncových uživatelů, které umožňují útočníkům realizovat například masivní DDoS útoky pomocí zotročených počítačů (botů), nebo skrytí aktivit útočníka a jeho identity při provádění sofistikovanějších a přesně zacílených útoků s možným závažným dopadem.

Literatura

[1] McQUADE III., Samuel. *Encyclopedia of Cybercrime*. Westport: Greenwood. 2008.

[2] National Cyber Security Framework Manual. NATO CCD COE Publikace, Estonia: Tallinn, 2012, ISBN 978-9949-9211-2-6. [online] [cit. 2013-05-23]. Dostupné z <http://www.ccdcoe.org/369.html>.

[3] TROY, Leo. *Is the future of unionism in cyberspace?* Journal of Labor Research, 2003, Volume 24, Issue 2, pp 257-270. Springer New York, 2003, ISSN 1936-4768. [online] [cit. 2013-04-22]. Dostupné z: <http://www.springerlink.com/content/xqa1trp4djx053rm/fulltext.pdf>.

[4] TZIMOPOULOU, Sofia. *The virtuality of the digital*. Intelligent Environments, 2006. IE 06. 2nd IET International Conference on, Issue 1, pp. 75-79. IEEE, 2006, ISSN 0537-9989. [online] [cit. 2013-4-22]. Dostupné z: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4197757&isnumber=4197733>.

[5] Síť CESNET2. [online] [cit. 2013-04-18]. Dostupné z: <http://www.cesnet.cz/sluzby/pripojeni/sit-cesnet2/>.

[6] Computer Science and Communications Dictionary. Springer US, 2001, ISBN 978-1-4020-0613-5. [cit. 2013-04-22]. Dostupné z: <http://www.springerlink.com/content/m80g11848104t581/fulltext.html>.

[7] CERT/CSIRT týmy a jejich role. [online] [cit. 2013-05-12]. Dostupné z <http://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/>.

2. Kybernetická válka

Při myšlenkách na kybernetickou válku se musíme zamyslet, jestli se bavíme o virtuálním bojišti v prostředí Internetu nebo již o fyzickém bojišti. V poslední době dochází k militarizaci kyberprostoru. Znamená to, že se vyspělé státy bojí kybernetické války? Kybernetická válka by byla bez pěšáků, zbraní, tanků nebo raket. Místo toho by útoky zahájily skupiny počítačových bojovníků (nebo hackerů). Je ale kybernetická válka opravdu hrozbou? Může kybernetická válka skutečně ochromit svět nebo jen nějaký vybraný stát? V dnešní době si zatím asi nikdo nedokáže představit kybernetickou válku světového rozsahu. Pravděpodobně by se jednalo o celosvětovou válku nedozírných následků. Riziko kybernetické války je a bude jedním z nejzávažnějších témat v oblasti bezpečnosti informací v několika následujících letech. Například Spojené státy na začátku roku 2013 poprvé hrozbu kybernetické války označily za větší hrozbu než Al-Káida nebo terorismus. Na příkladu USA je vidět, že se kybernetické války vyspělé státy obávají a že se na ni snaží co nejlépe připravit. Armády různých zemí vytvářejí své vojenské kybernetické jednotky. Například v květnu 2010 Pentagon zřídil U.S. Army Cyber Command (USCYBERCOM - http://www.arcyber.army.mil/).

2.1. Dosud známé nebezpečné škodlivé počítačové programy

Malware – tak je označován škodlivý počítačový program, který je určený ke vniknutí nebo poškození počítačového systému. Nejznámější typy malware jsou viry a červi. Mezi nejznámější a nejnebezpečnější malware lze zařadit **Stuxnet, Duqu a Flame**. Malware Stuxnet a Duqu lze zařadit do stejné skupiny. Ale malware Flame je něco odlišného.

Malware **Stuxnet** představoval velmi nebezpečný druh hrozby. Předpokládá se, že útok byl spuštěn ke konci roku 2009. Zjištěn byl až v červnu 2010. Všechny odborníky v té době velice překvapil. Byl totiž poprvé objeven vir, který měl reálnou schopnost ohrozit průmyslové řídicí systémy SCADA a mohl ovlivnit procesy, které tyto systémy řídí. Systémy SCADA pracují především v elektrárnách, elektrických přenosových soustavách a v průmyslu. Stuxnet totiž nenapadal propojené počítače náhodně, ale cíleně si vybíral právě tyto řídicí systémy. Celková

sofistikovanost viru vede experty k domněnce, že se jedná o profesionální práci s největší pravděpodobností armádního původu.

V říjnu 2011 společnosti Symantec a McAfee informovaly, že objevily novou verzi viru podobnou Stuxnet, označovanou jako **DuQu** nebo také Stuxnet 2.0. Hlavní rozdíl mezi viry je v cílech útoků. Ve srovnání se Stuxnet není DuQu navržen za účelem sabotáže systémů řídících průmyslové procesy, ale především pro útoky na servery certifikačních autorit. Další cílem malware DuQu je špionáž, zejména krádeže duševního vlastnictví z informačních systémů velkých průmyslových podniků.

V květnu v roce 2012 byl objeven další malware pod názvem **Flame**. Je také nazýván jako sKyWIper nebo Skywiper. Jedná se o modulární počítačový malware, který napadá počítače s operačním systémem Microsoft Windows. Je využíván pro cílenou počítačovou špionáž v zemích Blízkého východu. Ohrozil především země na Blízkém východě jako jsou Írán, Izrael, Súdán, Sýrii, Libanon, Saúdskou Arábii a Egypt. Malware Flame se šíří přes Internet, LAN nebo přes USB. Na infikovaných počítačích nahrává zvuky, snímky obrazovky, činnost klávesnice a provoz v síti. Program také zaznamenává Skype konverzaci a přes Bluetooth rozhraní shromažďuje informace z okolních zařízení nacházejících se v dosahu napadených počítačů. Tyto údaje spolu s uloženými dokumenty následně posílá do jednoho z několika velících a řídících serverů, které jsou roztroušeny po celém světě. Program pak čeká na další instrukce z těchto serverů. Předpokládá se, že takto se nepozorovaně šířil a získával informace již od února 2010. Dne 19. června 2012 Washington Post publikoval článek, v němž se uvádí, že malware Flame byl vyvinutý společně U.S. National Security Agency, CIA a izraelskou armádou přibližně v roce 2007. Vývoj byl součástí utajovaného projektu nazvaného Olympic Games. Cílem projektu byl sběr zpravodajských informací v rámci přípravy na cyber-sabotážní kampaně zaměřené na zpomalení íránského jaderného úsilí. Tuto informaci žádná ze stran nikdy nepotvrdila. [1]

Nikdo na světě neví, kolik takových či podobných nebo dokonce úplně odlišných škodlivých počítačových programů zrovna je. Nemáte některý z nich na svém počítači či v chytrém telefonu nebo tabletu také?

2.2. Nová realita kybernetické války

O závislosti společnosti na kybernetickém prostoru se příliš často nemluví, ať už z obav možného zneužití nebo čistě z nepochopení podstaty problému. S rostoucí mírou využívání kybernetického prostoru se ale tato závislost stále zvyšuje. Může být zneužita v případě teroristického nebo kybernetického útoku. A právě v tomto prostoru je možné vést v budoucnu války.

Než začneme mluvit o nové realitě kybernetických válek, podívejme se do minulosti. O plánech kybernetické války mezi státy se potichu mluví již několik let. Nikdo o nich nechce mluvit a nikdo se tím ani nechlubí. Již v prvním dílu této knihy ve třetí kapitole jsem uváděl příklady dnes známých kybernetických útoků na několik států. Proto se nebudu opakovat. Ale zmíním se o jednom uvažovaném kybernetickém útoku, který měl být předvojem před přímým fyzickým útokem na jiný stát. Riziko vedlejších škod bylo tak velké, že k němu nakonec nedošlo.

Ještě před invazí Spojených států do Iráku začali v roce 2003 Pentagon a americké zpravodajské agentury dělal plány na provedení kybernetického útoku na zmrazení miliard dolarů na bankovních účtech Saddáma Husajna. Tím chtěli ochromit jeho vládu nad finančními prostředky. Uvažovali, že pokud nebude mít finanční prostředky, nebude mít peníze na zaplacení vojenských dodávek a ani na platy vojáků v jeho armádě. To mělo vést k destabilizaci armády a celé společnosti. Ale útok nikdy nedostal zelenou a nebyl proveden. Představitelé Bushovy administrativy měli obavy, že by tento útok mohl vyvolat celosvětovou finanční katastrofu, která by se šířila po celém Blízkém východě, po Evropě a možná by zasáhla i Spojené státy. Dále hrozilo velké riziko kybernetického protiútoku, který by mohl mít za následek újmu na civilních osobách nebo poškození kritické infrastruktury. Riziko vedlejších škod bylo velké. Neexistují žádná pravidla a ani dosud není známá taktika pro provádění útoků v kyberprostoru. [3]

Co si tedy pod pojmem kybernetická válka můžeme představit? Existuje nějaká definice pojmu kybernetická válka? **Kybernetickou válku** lze vnímat jako opatření ze strany jednoho státu proniknout do počítačů nebo počítačových sítí jiného státu za účelem jeho poškození nebo narušení jeho

celistvosti. Výkladový slovník kybernetické bezpečnosti kybernetickou válku definuje jako *„Použití počítačů a Internetu k vedení války v kybernetickém prostoru. Soubor rozsáhlých, často politicky či strategicky motivovaných, souvisejících a vzájemně vyvolaných organizovaných kybernetických útoků a protiútoků*“. [2, s. 58]

Kybernetickou válku lze chápat také jako využití počítačů a informačních technologií k provádění aktů války na úrovni vlád a velkých organizací. Spouštěčem kybernetické války může být jednotlivec, organizace anebo státní instituce. Je mnoho různých druhů kybernetické války, od specializovaných hackerských až k obecně zacíleným útokům na vyřazení určité služby nebo ochromení kritické infrastruktury napadeného státu. Nejvyšším stupněm kybernetické války je útok, který kompletně odstraní schopnost všech připojení k Internetu.

Dnešní kybernetické útoky jsou primárně prováděny k získávání informací o diplomatických, ekonomických a vojenských programech. Sekundárním cílem může být ochromení kritické infrastruktury daného státu.

Budoucí možné kybernetické války jsou důvodem k vážnému znepokojení nás všech. Na rozdíl od tradiční války, která vyžaduje obrovské množství zdrojů, jako jsou zbraně, personál a vybavení, kybernetické války potřebují jen někoho, kdo má správné znalosti, výpočetní techniku a chce způsobit zmatek. Nepřítel může být kdekoli, dokonce i vně vlastního národa či organizace. Silný útok může provést pouze několik hackerů za pomoci standardních počítačů.

Další děsivý aspekt kybernetické války je, že kybernetický útok může přijít jako součást koordinovaného útoku, nebo to může být jen výmysl zlomyslného hackera například s vtipnou myšlenkou. Bez ohledu na to, co je motivem útočníka, mohou kybernetické útoky způsobit velké finanční ztráty. A mnohé státy jsou žalostně nepřipraveny čelit těmto neočekávaným kybernetickým útokům.

Součástí plánování boje mohou být různé taktické propočty a kalkulace. Jedním z takovýchto propočtů je poměr sil a prostředků. Poměr sil a prostředků se zpracovává jako pomocný dokument, zejména k rozhodujícím fázím plnění úkolu (bojového úkolu). Poměr sil a prostředků může být zpracováván jako kvantitativní nebo jako

kvalitativní. Při kvantitativním poměru sil a prostředků zpracovatelé uvádějí počty nasazovaných (předpokládaných) sil a prostředků na straně nepřítele a vlastní po jednotlivých požadovaných kategoriích, při kvalitativním poměru sil a prostředků se zohledňuje kvalita nasazovaných sil a prostředků. Tato kvalita je do výsledného poměru sil a prostředků dané kategorie zohledněna tzv. bojovým potenciálem. Skutečností zůstává, že uvažované síly a prostředky na straně nepřítele (zejména co do kvantity, ale i co do kvality) jsou pravděpodobnostním odhadem. Matematicky vyjádřeno jde o souhrn kvalitativních a kvantitativních údajů o silách a prostředcích bojujících stran, pomocí jejichž porovnání lze získat představu o bojových možnostech stran a o možném výsledku boje.

Jak lze **vypočítat poměry sil kybernetických armád** stojících proti sobě ve válečném kybernetickém konfliktu? Je vůbec reálné takovýto výpočet provést? Ve skutečnosti je to skoro nemožné. V případě války v kybernetickém prostoru primárně nerozhoduje množství, ale kvalita. Stovka speciálně vycvičených vojáků kybernetických jednotek může selhat tváří v tvář jednomu nadanému protivníkovi. Lze sice hovořit o početní převaze, ale ta v kybernetickém prostoru nemusí být rozhodující. Je tedy 100 nebo 1.000 speciálně vycvičených vojáků hodně nebo málo?

Myslím si, že kybernetické vojenské jednotky lze porovnávat aspoň podle následujících třech kritérií:

- schopnost **podniknout útok** v kybernetickém prostoru (útočný potenciál),
- schopnost **útok odvrátit** (obranný potenciál),
- **závislost** na kybernetickém prostředí (závislost).

Za další aspekty pro podrobnější porovnání můžeme považovat schopnost obnovit klíčové systémy, existence náhradních či záložních systémů, krizové plány a další. V případě kybernetického boje hovoříme spíše o potenciálních možnostech výpočtu poměru sil kybernetických jednotek, protože konkrétnější informace nejsou nikde dostupné. Důvodem je skutečnost, že jakékoliv vyjádření budoucího útočníka může protivníka na potenciální slabiny připravit, může vyprovokovat zkušební akce nebo může narušit důvěru veřejnosti. Prohlášení budoucího útočníka o dokonalém zabezpečení vlastní sítě může vyprovokovat zkušební akce

jak ze strany potenciálních útočníků, tak i nahodilých nestátních aktérů (například hackerů) s cílem odhalit možné slabiny.

2.3. Metody kybernetické války

Významné možnosti využití kybernetického prostoru pro vojenské účely přineslo až masové rozšíření uživatelů v kybernetickém prostoru. Vzrůstající počet uživatelů způsobil, že šíření propagandy v kybernetickém prostoru je mnohem efektivnější než třeba vyhazování letáků z letadel. Šíření škodlivého počítačového programu (například malware) je se stoupajícím počtem uživatelů snadnější, dostupnější a rychlejší. Proto i hrozby kybernetických útoků jsou stále reálnější.

V kybernetickém prostoru existuje několik různých metod kybernetických útoků (od mírných až po ty nemilosrdné):

- **Vandalismus**: jedná se o běžné útoky na webové vládní stránky. Tyto útoky jsou obvykle prováděny rychle a nezpůsobí velké škody.
- **Propaganda**: jedná se o šíření politických zpráv zejména prostřednictvím Internetu.
- **Sběr dat**: jedná se o shromažďování důvěrných informací, které nejsou dostatečně chráněny.
- **Odepření přístupu**: jedná se o útoky například na ozbrojené síly, které používají počítače a satelity pro spojení. Rozkazy a zprávy mohou být zachyceny a pozměněny, což může pro armádu zapříčinit velmi nebezpečné situace.
- **Síťové útoky na infrastrukturu**: jedná se o útoky na přenosové soustavy společností podnikajících v energetice, plynárenství, teplárenství, ropného průmyslu a komunikační infrastruktury, kterou jsou citlivé na kybernetické útoky.
- **Nesíťové útoky na infrastrukturu**: jedná se o zneužití (nebo spíše využití) běžného hardware používaného v počítači a hardware používaného k provozu či k zabezpečení Internetu. Škodlivý program (vir) je ukrytý v samotném hardware, softwaru nebo snad dokonce v mikroprocesorech.

Kybernetickou válku můžeme dále dělit stejně jako konvenční válku na obrannou a útočnou kybernetickou válku.

Obranná kybernetická válka

V případě obranné kybernetické války jako takové bude důležité stanovit strategicky důležité objekty. V dnešní době jsou těmito objekty stavby a rozhodujícími kritérii je jejich geografická poloha, vybavení těchto objektů atd. V případě kybernetické války mohou být tyto objekty také virtuální. K odvrácení útoku či zmírnění ztrát a škod je potřeba ještě před samotným útokem minimalizovat počet vstupních přístupových míst, zavést vícečetné softwarové zabezpečení, hardwarové zabezpečení a řádně prověřit a proškolit personál s povolením vstupu na síť. Obrana v budoucí kybernetické válce nebude nikdy snadná.

Kybernetičtí útočníci mají jasný cíl s jednoduchým plánem. Klíčem k jejich úspěchu je využít moment překvapení při útoku. Čím dříve bude obránce na útok reagovat, tím snazší může být zastavení nebo odražení útoku. Pokud k útoku s momentem překvapení dojde, je potřeba se nejdříve vypořádat s tímto překvapením stabilizací celého systému. Následně je potřeba detekovat útok a snažit se pochopit útočníkovi plány a záměry. Pak může dojít k odražení útoku. Nesmí se ale zapomenout, že vždy musí následovat analýza celého útoku. Na základě zjištěných informací musí dojít k posílení ochrany kritické infrastruktury (hardware a software), aby se zabránilo následným možným kybernetickým útokům.

Útočná kybernetická válka

V první řadě je třeba si uvědomit aspekty útočné kybernetické války a jejich srovnání s aspekty tradičními (konvenčními válečnými, diplomacií, atd.). Takový druh války může být akceptovatelnější pro veřejnost než použití konvenčních válečných prostředků. Přestože je možné vyhnout se pomocí kybernetické války přímým obětem na životech a majetku, jsou stále přítomna nepřímá nebezpečí. Na pomezí mezi státním a soukromým sektorem je kritická infrastruktura. Hovoříme například o distribuční síti vody, elektrické energie, o řízení letového provozu a o dalších systémech, které jsou kritické pro chod dané země. Právě útok na kritickou infrastrukturu může vést k vyřazení sítí, které dále slouží ve prospěch zdravotnictví, vodohospodářství a dalších životně důležitých prvků státu.

Závislost na kybernetickém prostoru může být využita nepřítelem k získání strategické výhody při případném konfliktu. Předpokládá se, že kybernetická válka bude předcházet před konvenční válkou.

Literatura

[1] *Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk*. The New York Times, USA, 2009. [online] [cit. 2013-05-28]. Dostupné z <http://www.nytimes.com/2009/08/02/us/politics/02cyber.html?ref=cyberwar&_r=0l>.

[2] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti. 2.* aktualizované vyd. Praha: Policejní akademie ČR v Praze, 2013, 200 s. ISBN 978-80-7251-397-0.

[3] Richard A. CLARKE , Robert K. KNAKE. *Cyber War - The Next Threat to National Security and What to Do about It.* USA: Ecco Press, 2010, 290 s. ISBN 9780061962233

3. Řízení rizik v prostředí kybernetické bezpečnosti

Pod pojmem **řízení rizik** rozumíme koordinované aktivity, pomocí kterých řídíme a ovládáme organizaci vzhledem na rizika. [2; 4]

Řízení rizik je procesem, který napomáhá organizaci vytvářet hodnoty pro její zainteresované strany s optimálním využitím zdrojů organizace, a tím optimalizovat náklady vzhledem k dosahované hodnotě.

Cílem řízení rizik je pro organizaci zvýšit pravděpodobnosti dosažení cílů organizace (operativních, taktických a strategických) spolu s optimálním vynaložením nákladů pro jejich dosažení a dodržením zákonných a regulačních požadavků a mezinárodních norem.

Hlavní přínosy řízení rizik pro organizaci lze spatřovat v:

- včasné a správné identifikace příležitostí (využití pozitivního účinku nejistoty na dosažení cílů) a hrozeb (zvládnutí, spolu s minimalizací možných ztrát, negativního účinku nejistoty na dosažení cílů organizace),
- spolehlivosti a důvěře u zainteresovaných stran,
- prevenci ztrát a v úspěšném řízení incidentů (zejména předcházení incidentům),
- efektivnosti a účinnosti používání zdrojů organizace (pracovníci, stroje, software, data, finance atd.) [2]

Teorie řízení rizik nahlíží na řízení rizik jako na řízení příležitostí (pozitivní účinek nejistoty na dosažení cíle) a hrozeb (negativní účinek nejistoty na dosažení cíle). V prostředí kybernetické bezpečnosti se však zaobíráme riziky pouze z pohledu hrozeb (viz ČSN ISO / IEC 27005).

3.1. Chyby řízení rizik

Současná praxe ukazuje na 4 základní chyby, ke kterým dochází při řízení rizik v organizaci a kterým je třeba se vyvarovat:

a) identifikace nerelevantních rizik (rizik, která nejsou navázány na cíle organizace),
b) absence víceúrovňového řízení rizik (manažeři rizika ze své úrovně),
c) absence agregace rizik (chybí celkový rizikový profil),

d) přílišná orientace na proces a nikoli na efekt řízení (neefektivní vynakládání nákladů na řízení a využívání lidských zdrojů). [4]

Identifikace nerelevantních rizik – rizika nejsou vztažena k rizikovým faktorům, konkrétní zranitelnosti kritický aktiv, potřebných k dosažení cílů organizace, vůči působení hrozby. Přestože na první pohled se jeví, že vše je v pořádku a rizika popsaná v Registru rizik jsou zvládána, tak při podrobnější analýze zjistíme, že obsah rizik končí u obecného popisu hrozby a definovaná opatření na zvládnutí rizika nejsou ničím podložena. Důsledkem chybné identifikace rizik jsou tak zbytečně vynakládány finanční prostředky na zvládání rizik, která nepřispívají k splnění stanovených cílů. Případně opatření ke zvládnutí rizika se míjí účinkem, čímž finanční prostředky nejsou vynakládány účelně a dopady rizika se mohou projevit v plné míře.

Rozhodující roli zde sehrává analýza definovaných cílů organizace, strategie jejich dosažení a aktiv potřebných k realizaci strategie. Manažeři organizace proto nemohou identifikovat relevantní rizika bez znalosti kontextu prostředí, aby mohli odpovědět na otázku: „Co může ohrozit splnění cílů v mé odpovědnosti?“

Absence víceúrovňového řízení rizik – je charakterizována nejasnostmi týkající se kompetencí k řízení rizika včetně schopnosti zvládat riziko z potřebné úrovně řízení organizace (manažeři 3. až 1. úrovně řízení). Zejména může docházet k vypuštění vrcholového řízení rizik (management 1. úrovně) a spolu s tím i nejasnost kdo za jaká rizika nese odpovědnost. Nedochází k přenášení (eskalace) rizik na manažery vyšší úrovně, kteří mají kompetence zvládat tato rizika. Dále není zřejmé, jak velké riziko je přijatelné (akceptovatelné) – není nastaven tzv. rizikový apetit. Důsledkem je ztráta celistvého pohledu na rizika v organizaci. Každá část organizace nebo úroveň řízení vnímá jinak chuť riskovat. Proces řízení rizik nesplní očekávané cíle a selže.

Je třeba si uvědomit, že např. manažer 3. úrovně nemůže zvládat rizika vztahující se ke strategickým cílům organizace, za které je odpovědný manažer 1. úrovně (vliv nastavení / nenastavení přenesení – eskalace rizik). Nelze také pouze vycházet z domněnky, že manažer vyšší úrovně

řízení o rizicích ví a sám vyvine přiměřenou odezvu na tato rizika (vliv funkčního / nefunkčního reportingu).

Absence agregace rizik – do rizikového profilu jednotlivých součástí organizace a organizace jako takové. Izolovaný přístup ke zvládání rizik je v praxi průvodním jevem chybějící agregace rizik, který způsobuje ztrátu kontroly nad celkovým rizikovým profilem té či oné části organizace nebo i celé organizace, aniž to manažeři tuši. Další možnou variantou je prováděná agregace rizik z jednotlivých částí organizace, která je zúžena na referování bez vyjádření spolupůsobení a vazeb mezi riziky (např. z hlediska času a jejich společného dopadu).

Chybějící agregace rizik do celkového rizikového profilu neumožňuje hledat vzájemné vazby mezi riziky a následně identifikovat dopad jejich vzájemného spolupůsobeni. Důsledkem jsou dopady, jež nebyly identifikovány a které byly způsobeny například řetězením nevýznamných rizik. Dopady takových to řetězení rizik, mohou být pro organizaci velmi zásadní – vyvolání krize (finanční ztráty nebude moci organizace zvládnout).

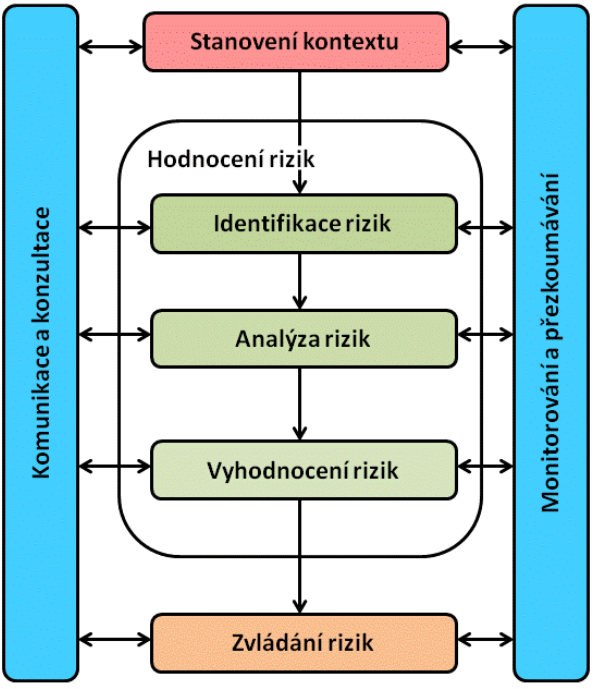
Přílišná orientace na proces a nikoli na efekt řízení – také dělat nesprávné věci správně. Účelem řízení rizik je napomoci organizaci dělat správné věci správně. Různé standardy pro řízení rizik (projektových rizik, rizik organizace) hledají odpověď na to, co jsou „správné věci". Hledají tedy odpověď na otázky: „K čemu vztahovat rizika?" a „Od čeho v organizaci rizika odvozovat?" Standardy, zabývající se řízením rizik, se shodují, že základem jsou cíle, kterých má být v organizaci a jejich částí dosaženo.

Důsledkem přílišné orientace na proces řízení rizik je pouze slib (přání), že bude dosaženo i správného efektu z řízení rizik směřující k dosažení cílů organizace. Jedná se o zavádějící slib (nesplněné přání), protože selhává smysl řízení rizik, přičemž náklady na řízení rizik zůstávají místo toho aby byly sníženy.

3.1.1 Proces řízení rizik

Proces řízení rizik je naplňován stanovením kontextu, hodnocením rizik, zvládáním rizik (sekvenční subprocesy), komunikací a konzultací rizik,

monitorováním a přezkoumáváním rizik (paralelní subprocesy). Hodnocení rizik sestává z kroků identifikace rizik, analýza rizik a vyhodnocení rizik (viz Obrázek 3).



Obrázek 3- Proces řízení rizik (zdroj ISO ČNS / IEC 31000)

Proces řízení rizik, jak ukazuje Obrázek 3, je cyklickým procesem. Jakákoli změna na úrovni kontextu (realizací přezkoumávání je identifikována změna) se projeví v možnosti vzniku nových (doposud neidentifikovaných) rizik, která je potřeba hodnotit i zvládnout. Monitorování a přezkoumávání hodnocení rizik může při každém opakování rozsah a detail hodnocení zvyšovat. Obdobně to platí také u zvládání rizik, neboť je třeba neustále monitorovat a přezkoumávat účinnost provedených opatření (nejsou k dispozici účinnější možnosti, není třeba nahradit již nevyhovující opatření). Přístup s využitím monitorování a přezkoumávání zajišťuje správnou rovnováhu mezi minimalizací času, vynaloženého úsilí a nákladů potřebného k účinnému zvládnutí rizik.

Subproces komunikace a konzultace zabezpečuje v procesu řízení rizik tok informací v procesu. Správné nastavení tohoto subprocesu je základem informovanosti manažerů a jejich podřízených pro úspěšné zvládání incidentů a snížení potenciální škody.

Proces řízení rizik zahrnuje následující rozhodovací body:

- výběr kritérií pro proces řízení rizik (stanovení kontextu),
- výběr kritických aktiv (stanovení kontextu),
- akceptace rizik s nízkou hodnotou nebo postoupení rizik ke zvládání (vyhodnocení rizik),
- rozhodnutí, že definovaná opatření / úkoly jsou dostatečné vzhledem k nově provedenému odhadu hodnoty rizika (zvládání rizik),
- rozhodnutí o přenesení (eskalace) rizika na nadřízeného (zvládání rizik)
- určení vlastníka rizika a delegování pravomoci k přípravě /realizaci opatření ke zvládnutí rizika (zvládání rizik),
- rozhodnutí o realizaci opatření ke zvládnutí rizika (zvládání rizik).

Řízení rizik je směřováno do bodu akceptace (akceptace opatření na zvládání rizik, akceptace zbytkového rizika tzv. míra rizikového apetitu), kdy manažeři jednotlivých úrovní rizika přijmou. To je důležité zejména ve vztahu k potřebným nákladům na zvládnutí rizik. Od bodu akceptace se řízení rizik zaměřuje na jejich zvládání s podporou monitorování a přezkoumávání, komunikace a konzultace.

Proces řízení rizik může být aplikován na proces řízení bezpečnosti informací (ISMS), který je navázán na model "Plánuj-Dělej-Kontroluj-Jednej" (Plan-Do-Check-Act nebo PDCA).[1] Tabulka 1 názorně ukazuje tuto aplikaci. Dále se proto v procesu řízení rizik detailněji zaměříme na rizika řízení bezpečnosti informací, jejichž součástí je kybernetická bezpečnost. Proces řízení rizik je však shodný ať se jedná o rizika v kybernetickém prostředí, bezpečnosti práce ve stavebnictví, marketingu nebo kdekoli jinde. [1; 3]

[1] Součástí procesu řízení bezpečnosti informací (systému bezpečnosti informací) je řízení kybernetické bezpečnosti, jako specifická oblast.

Tabulka 1 – Řízení rizik a fáze procesu ISMS (zdroj ISO ČNS / IEC 27005)

Proces ISMS	Proces řízení rizik
Plánuj	Stanovení kontextu Hodnocení rizik Zvládání rizik (plán zvládání *akceptovaných* rizik)
Dělej	Implementace plánu zvládání akceptovaných rizik Kontinuální komunikace a konzultace
Kontroluj	Kontinuální monitorování a přezkoumávání rizik
Jednej	Udržování a zlepšování procesu řízení rizik bezpečnosti informací

3.2. Stanovení kontextu řízení rizik kybernetické bezpečnosti

Stanovení kontextu pro řízení rizik kybernetické bezpečnosti zahrnuje určení základních kritérií pro řízení rizik kybernetické bezpečnosti, definování rozsahu a hranic, a stanovení příslušné organizační struktury pro řízení rizik kybernetické bezpečnosti.

Základem řízení rizik kybernetické bezpečnosti je určení cílů organizace (zejména ve vztahu k bezpečnosti informací), neboť tyto cíle ovlivňují celý proces a zejména stanovení kontextu. Cílem může být:

- efektivně využít finanční zdroje (finanční aktiva) pro minimalizaci dopadů hrozeb na systém řízení bezpečnosti informací,
- dodržet právní a další regulatorní požadavky na správu bezpečnosti informací.

Výstupem stanovení kontextu je specifikace základních kritérií, rozsahu, hranic, organizační struktury a kritických aktiv pro proces řízení rizik bezpečnosti informací. [1; 3]

3.2.1 Základní kritéria řízení rizik kybernetické bezpečnosti

V závislosti na rozsahu a cílech řízení rizik by měla být organizací definována kritéria vyhodnocení rizik, dopadu a akceptace rizik (tzv. kritéria rizikového apetitu).

Kritéria jsou nastavována na stupnici měřitelnosti (kvalitativní, semikvantitativní nebo kvantitativní).

Kritéria vyhodnocení rizik kybernetické bezpečnosti [1]
Měla by být vytvořena kritéria vyhodnocení rizik kybernetické bezpečnosti zohledňující:

- strategické hodnoty procesu informací o činnostech organizace (proces – aktivum2),
- legislativní a regulační požadavky, smluvní povinnosti (smlouvy – aktiva),
- dostupnost, důvěrnost a integrita provozu a obchodních činností (aktiva),
- cíle a očekávání zainteresovaných stran (aktiva), negativní následky ztráty důvěryhodnosti (aktivum) a pověsti (aktivum),
- kritičnost aktiv (např. z pohledu dostupnosti, důvěrnosti a integrity aktiv).

Definovaná kritéria vyhodnocení rizik je vhodné následně použít k určení priorit pro zvládání rizik (např. kvalitativně – priorita vysoká – nutnost zvládnout okamžitě, priorita střední – připravit opatření, priorita nízká – opatření budou připravována v případě dostatku finančních prostředků).

Kritéria dopadu na aktiva kybernetické bezpečnosti [1]
Kritéria dopadu by měla být specifikována na základě stupně škod nebo ztrát organizace (např. finanční, dostupnosti, důvěrnosti a integrity), které byly způsobeny bezpečnostní událostí, s ohledem na:

- úroveň klasifikace ovlivněného aktiva (např. kvalitativní úroveň – vysoká, střední, nízká, semikvantitativní úroveň – 1 až 5),
- narušení systému bezpečnosti informací (např. ztráta důvěrnosti, integrity a dostupnosti informací),
- poškozené provozy (vlastní nebo třetích stran),
- ztrátu činností organizace (např. organizace není schopna nebo částečně schopna realizovat své činnosti) a finanční hodnoty (např. ztráta hodnoty akcií na trhu),

[2] Aktivum – vše co má pro organizaci hodnotu. Ve vztahu k riziku jsou brány v úvahu aktiva používaná k dosažení cílů organizace.

- přerušení plánů a nedodržení konečných termínů (např. projekty musí být pozastaveny a jednotlivé produkty jsou dodány se zpožděním),
- poškození pověsti (např. nezískání pozitivních referencí, negativní informace zapříčiní odstoupení zákazníka od jednání),
- porušení právních, regulatorních nebo smluvních požadavků (např. nedodržení kritérií dle normy xy a následná ztráta certifikátu).

Kritéria akceptace rizik kybernetické bezpečnosti [1]

Kritéria akceptace rizik jsou přímo závislé na rizikovém apetitu organizace. [3] Další závislost je dána politikami, záměry a cíli organizace a stupněm zájmů vzhledem síle vlivu zainteresovaných stran (zejména klíčových zainteresovaných stran).

Kritéria akceptace rizik se nejčastěji vyjadřují jako poměr odhadnutého zisku (nebo jiného obchodního přínosu) k odhadnutému riziku[4] (ztrátě). Dalším zásadním kritériem akceptace rizik je nesoulad s předpisy nebo zákony (POZOR – tato rizika nelze akceptovat vzhledem ke vzniklé ztrátě).

Kritéria akceptace rizik (úroveň rizikového apetitu) jsou ovlivňována:

- obchodními kritérii, právními a regulačními aspekty (zákony a normy, požadavky zákazníka),
- vlastním provozem a technologiemi organizace, včetně financí (např. cash flow organizace),
- sociálními a humanitárními faktory.

3.2.2 Rozsah a hranice bezpečnosti informací

Rozsah procesu řízení rizik kybernetické bezpečnosti je třeba vnímat v kontextu systému bezpečnosti informací. Proto musí být rozsah definován tak, aby bylo zajištěno, že jsou při hodnocení rizik brána

[3] Rizikový apatit je schopnost absorbovat ztrátu akceptované míry rizik. [4]

[4] Odhadnuté riziko (hodnota rizika) je dána součinem hodnotou pravděpodobnosti působení hrozby (vyvolané aktérem) na zranitelnost aktiva a hodnotou dopadu jeho působení na aktivum (cíl).

v úvahu všechna příslušná aktiva (kritická aktiva, která mají pro organizaci vysokou hodnotu a je třeba je chránit) systému bezpečnosti informací. Kromě toho je nutno identifikovat hranice k zvládnutí těch rizik v závislosti na kritická aktiva, cíle organizace a kompetence manažerů jednotlivých úrovní. [1; 4]

Při definování rozsahu a hranic kybernetické bezpečnosti je nutno aby organizace zohlednila následující informace:

- strategické obchodní cíle, strategie (způsob dosažení strategických cílů) a politiky organizace (včetně politiky bezpečnosti informací, jehož součástí je kybernetická bezpečnost),
- funkce, struktura a procesy organizace (včetně procesu řízení rizik v organizaci a přístupu organizace k němu),
- právní, regulatorní normy a smluvní požadavky platné pro organizaci,
- aktiva kybernetické bezpečnosti, případně celého systému bezpečnosti informací,
- očekávání podílníků (jako klíčových zainteresovaných stran organizace),
- sociálně kulturní prostředí organizace a místa činnosti,
- rozhraní styku uvnitř organizace a organizace s okolím (např. výměna informací s vnějším prostředím),
- další omezení ovlivňující organizaci.

3.2.3 Organizační struktura pro řízení rizik systému bezpečnosti informací

Organizační struktura a odpovědnosti systému bezpečnosti informací (v dílčím pojetí pro proces řízení kybernetické bezpečnosti) je strukturou realizující tento proces a nesoucí plnou odpovědnost za jeho efektivitu (efektivní použití zdrojů a dosažení cílů organizace). Hlavní role a odpovědnosti procesu řízení rizik kybernetické bezpečnosti v rámci systému bezpečnosti informací jsou:

- údržba procesu řízení rizik kybernetické bezpečnosti se zaměřením na splnění požadavků organizace (cílů organizace),

- řízení zainteresovaných stran v organizaci i vně organizace (proces řízení zainteresovaných stran – aktérů vyvolávajících hrozby, lidských zdrojů organizace jako kritických aktiv atd.) se zaměřením na řízení rizik kybernetické bezpečnosti,
- definování rolí a odpovědností pracovníků a manažerů jednotlivých úrovní (interní) všech částí organizace, tak i dodavatelů, subdodavatelů, zákazníků (externích) ve vztahu k systému řízení rizik informací,
- stanovení požadovaných vztahů mezi organizací a zainteresovanými stranami (vnitřními a vnějšími), jakož i rozhraní k funkcím řízení rizik bezpečnosti informací a rizik organizace na vyšší úrovni (např. zvládání rizik s využitím eskalace rizik a agregace závislých a nezávislých rizik), jakož i rozhraní k projektům (projektovým programům, portfoliu) nebo činnostem organizace,
- stanovení procesu eskalace rozhodnutí (např. eskalace rizika k jeho zvládnutí na vyšší úroveň)
- specifikace záznamů (proces reportingu organizace a obsah reportů), které musí být uchovávány (včetně způsobu uchovávání a jejich dostupnosti). [4]

3.2.4 Identifikace kritických aktiv organizace

Cíl: Aktiva jsou identifikována v rámci stanoveného rozsahu pro řízení rizik bezpečnosti informací.

Aktivem rozumíme cokoli, co má pro organizaci významnou hodnotu a z toho důvodu vyžaduje také ochranu proti působení hrozby. [1; 3; 4]

U aktiva je třeba identifikovat vlastníka aktiva k zajištění záruky a odpovědnosti za aktivum. Vlastník aktiva nemusí toto aktivum fyzicky vlastnit, ale má stanovenu odpovědnost za jeho produkci, vývoj a používání v souladu s pravidly používání. Pro určení hodnoty aktiva je vhodné využít znalostí vlastníka aktiva pro organizaci. Přesto že vlastník aktiva může jeho hodnotu přecenit nebo nedocenit, tak poskytne potřebné informace o tomto aktivu pro stanovení jeho hodnoty pro organizaci.

Identifikace aktiv (rozsah) je definována okruhem aktiv organizace, který má být zvládán procesem řízení rizik kybernetické bezpečnosti. Aktiva, která jsou mimo proces řízení rizik kybernetické bezpečnosti, nejsou brána v úvahu.

Výstupem může být seznam aktiv, u kterých by využití zranitelnosti hrozbou mělo dopady nad rámec rizikového apetitu a jejich důležitost.

Příklad

Organizace identifikovala na základě analýzy kontextu procesu řízení rizik kybernetické bezpečnosti následující rizika (výpis):[5]

- *intranetový server umístěný v budově A na 1. podlaží, místnost Ax, pro chod intranetové sítě a archivaci dat, vlastník aktiva správce serveru,*
- *54 ks pracovních stanic PC umístěných v budově A a B v kancelářích zaměstnanců organizace, pro tvorbu dat a jejich přenos na úložiště na serveru, vlastník aktiva – pracovníci, jimž je pracovní stanice přidělena k výkonu činnosti,*
- *serverový software umístěný na intranetovém serveru v budově A na 1. podlaží, místnost Ax, pro chod intranetové sítě a archivaci dat, vlastník aktiva správce serveru,*
- *54 ks MS Office 2013 CZ Professional umístěných na 54 ks pracovních stanic PC v budově A a B v kancelářích zaměstnanců organizace, pro tvorbu dat a jejich přenos na úložiště na serveru, vlastník aktiva – pracovníci, jimž je pracovní stanice přidělena k výkonu činnosti,*
- *1000 ks disketa 3.5"/1.44MB uložených v budově B, suterénní místnosti Sx pro zálohování a přenos dat, vlastník aktiva – správce materiálu.*

Hodnota aktiv (viz Tabulka 2) je dána nejvyšší hodnotou hodnocených kritérií. Aktiva hodnocená níže jak 3 nejsou pro organizaci kritická a proto je nebude ani chránit (řídit hrozby, které by mohli způsobit ztrátu).

V tomto případě organizace již nepočítá s použitím disket (v nejbližší době budou zničeny pod dozorem správce materiálu – rozdrceny v drtičce).

[5] Vhodná metoda pro identifikaci aktiv je brainstorming.

Tabulka 2 – Semikvantitativní analýza aktiv a jejich hodnocení[6] (zdroj vlastní)

P. č.	*aktivum*	*dostupnost*	*důvěrnost*	*integrita*	*hodnota*
1.	*server*	*3*	*4*	*5*	*5*
2.	*54 ks PC*	*2*	*3*	*3*	*3*
3.	*Server SW*	*3*	*5*	*5*	*5*
4.	*MSO 2013*	*2*	*1*	*3*	*3*
5.	*disketa*	*1*	*1*	*1*	*1*

3.3. Hodnocení rizik kybernetické bezpečnosti

Hodnocení rizik je subprocesem zahajovaným po realizaci subprocesu stanovení kontextu, kdy byla stanovena kritéria řízení rizik kybernetické bezpečnosti, analyzováno vnitřní a vnější prostředí organizace. Nejdůležitějším vstupem do hodnocení rizik jsou identifikovaná kritická aktiva (která je třeba chránit) a kritéria hodnocení rizik. [1; 2]

Rizika jsou v subprocesu hodnocení identifikována, kvantifikována nebo kvalitativně popsána a prioritizována v souladu s kritérii a cíli hodnocení rizik vztaženými ke kritickým aktivům (a tím i cílům) organizace.

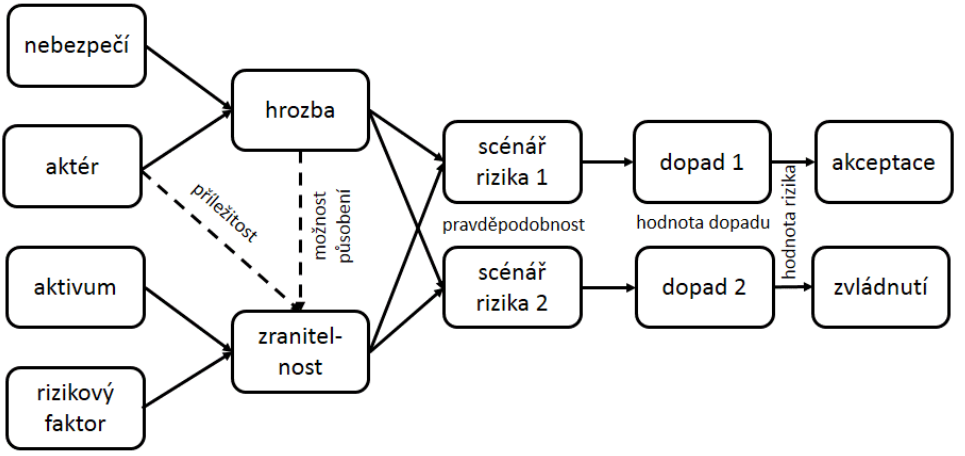
Hodnocení rizik rizika kvantifikuje nebo kvalitativně popisuje, čímž umožňuje manažerům určit prioritu rizik podle jejich důležitosti ve vazbě na první agregaci závislých rizik.

Hodnocení rizik sestává z těchto činností:

- identifikace rizika (obsahuje také identifikaci aktérů generujících hrozbu, hrozeb, kritických faktorů a zranitelnosti aktiv),
- analýza rizik zahrnuje:
  - analýzu kritických faktorů (výstupem jsou zranitelnosti aktiv),
  - analýzu působení hrozeb na zranitelnosti aktiv (jaká hrozba může využít zranitelnosti – možné scénáře působení hrozby),

[6] Analýzu lze provést skórovací metodou na hodnotící stupnici např. 1 – 5 (např. 1 – aktivum snadno dostupné, 5 – aktivum velmi těžko nahraditelné / nedostupné).

- odhad rizik (záměr působení na zranitelnost – pravděpodobnost působení hrozby a kvantifikovaný dopad scénáře na aktivum nebo cíl),
- vyhodnocení rizik (vyhodnocení dopadu a stanovení hodnoty rizika, agregace závislých rizik, akceptace rizik v souladu s rizikovým apetitem a posunutí neakceptovaných rizik ke zvládnutí). [1]



Obrázek 4 - Model formulace rizika v subprocesu hodnocení rizik (zdroj vlastní)

Hodnocení rizik je navázáno na hodnotu aktiv systému bezpečnosti informací. Součástí je také identifikace stávající opatření a jejich účinek na identifikované riziko. Hodnocení rizik zahrnuje analýzu potenciálních dopadů a stanovení priorit rizik. Prioritizovaná rizika jsou vyhodnocena vzhledem ke kritériím vyhodnocení rizik, určenými v subprocesu stanovení kontextu. Obrázek 4 názorně ukazuje vývoj formulace rizika zakončeného rozhodnutím o akceptaci (podstoupení rizika) nebo jeho posunutí ke zvládnutí.

Výstupem subprocesu je seznam rizik (hodnocených rizik akceptovaných a rizik posouvaných do zvládnutí). Rizika mají přiřazenu prioritu na základě kritérií hodnocení rizik.

Příklad dle modelu na Obrázek 4

Nebezpeční *kybernetického útoku na smartphone.*
Aktivum *– smartphone s operačním systémem.*
Rizikový faktor *– antivirová ochrana.*
Hrozba *– vir ovlivňuje funkčnost operačního systému.*
Aktér *– hacker.*
Zranitelnost *– antivirová ochrana není nainstalována.*
Příležitost *– hacker využije* ***příležitost*** *nechráněného smartphone antivirovým programem.*
Rizikový scénář *– při prohlížení emailu na internetu dojde k aktivaci viru zaslaného v infikovaném e-mailu a dojde k trvalému poškození operačního systému.*
Dopad *– telefon nelze používat pro komunikaci, je nefunkční.*

3.3.1 Identifikace rizik kybernetické bezpečnosti

Cíl: Určit, co by se mohlo stát, aby byla způsobena potenciální ztráta, a porozumět tomu jak, kde a proč ke ztrátě (dopadu) může dojít.

Identifikace hrozeb kybernetické bezpečnosti [1; 4]
Cíl: Identifikovat možné hrozby, které mají potenciál poškodit aktiva a jejich aktéry, kteří mohou vyvolat hrozby.

Vstupem do toho to kroku jsou informace o hrozbách získaných z přezkoumání již nastalých incidentů, od vlastníků aktiv, manažerů a z jiných zdrojů, včetně registru rizik (plánu protirizikových opatření, seznamu rizik).

Hrozby je vhodné identifikovat obecně podle typu (např. technické, manažerské atd.), přičemž některé z nich mohou působit na více aktiv. Velký počet identifikovaných hrozeb neznamená, že všechny bude třeba zvládnout, neboť zdroje na jejich zvládnutí jsou omezené, a to včetně finančních prostředků.

Výstupem kroku je seznam hrozeb (viz Tabulka 3) s identifikací typu a aktéra (zdroje) hrozby (seznam rizik).

Příklad

Tabulka 3 – Výpis ze seznamu identifikovaných hrozeb (Zdroj vlastní)

P. č.	*Typ hrozby*	*Hrozba*	*Aktér / zdroj*
1.	*Kybernetická*	*Virus ALFA ničí data na serverech*	*Hacker skupina „NOTE“ k šíření využívá soubory, které infikuje*
2.		*Červ Dixie zablokuje PC (server)*	*Hacker „DUCK“, k šíření využívá e-mailovou poštu*

Identifikace stávajících opatření na zvládání rizik kybernetické bezpečnosti [1; 4]

Cíl: Identifikovat stávající, plánovaná opatření zvládání rizik a tím předejít neefektivnímu použití zdrojů a vynakládání finančních prostředků (duplikace opatření).

Vstupem jsou dokumenty stávajících opatření na zvládání rizik a implementační plány zvládání rizik, zprávy z auditu.

Kromě identifikaci stávajících opatření je vhodné provést kontrolu odpovídající funkčnosti realizovaných opatření. Opatření, která neplní požadovanou funkci (účinnost není odpovídající), s velkou pravděpodobností zvyšují dopad (ztrátu) nad akceptovatelnou hodnotu (stávají se zranitelností aktiva). Realizovaná opatření nemusí být účinná k nově identifikovaným rizikům, proto bude nutno přijmout doplňková opatření.

Existující nebo plánované opatření, které je identifikováno jako neúčinné, nedostačující nebo neoprávněné je třeba zkontrolovat a určit způsob odstranění opatření nebo způsob nahrazení odpovídajícím opatřením. Lze také rozhodnout o ponechání opatření například z finančních důvodů.

Výstupem je seznam existujících a plánovaných opatření (viz *Tabulka 4*), jejich zavedení a stav užívání (plán protirizikových opatření).

Příklad

Tabulka 4 - Výpis ze seznamu existujících opatření s hodnocením účinnosti (Zdroj vlastní)

P. č.	*Opatření a zavedení*	*Účinnost*
1.	*Antivirový program Q2naistalovaný do pracovních stanic organizace od roku 2006*	*Neúčinný – podpora ukončena před 3 měsíci*
2.	*Síť WIFI je chráněna proti zneužití heslem o délce 5 znaků od jejího zprovoznění (5/5/2009), heslo se skládá z 5-ti znaků abecedy bez použití velkých písmen*	*Neúčinný – heslo lze prolomit do 6 min.*

Identifikace zranitelností aktiv [1; 4]

Cíl: Identifikovat zranitelnosti aktiv, které mohou být zneužity hrozbami na základě identifikace rizikových faktorů.

Vstupní dokumenty jsou seznamy rizik, seznam aktiv, existujících a plánovaných opatření.

Zranitelnosti aktiv nejsou ztrátou pro organizaci, ale slabými stránkami aktiv, které lze opatřeními zvládat. Neexistuje-li zranitelnost, kterou může využít hrozba, tak není ani riziko (není třeba je zvládat), což platí i naopak jestliže neexistuje hrozba. Existuje-li zranitelnost, která nemá identifikovanou možnou hrozbu, je třeba tuto monitorovat, zda nebyla identifikována hrozba, která ji může využít.

Zranitelnosti mohou souviset s vlastnostmi aktiva, které lze použít způsobem nebo pro účel, který je jiný, než bylo zamýšleno, když bylo aktivum zakoupeno nebo zhotoveno. Je nutno posuzovat zranitelnosti vyplývající z různých zdrojů, například ty, které jsou pro aktivum podstatné nebo vedlejší.

Výstupem je seznam zranitelností ve vztahu k aktivům, hrozbám a opatřením (viz Tabulka 5) a seznam zranitelností, které se nevztahují

k žádné identifikované hrozbě pro realizaci subprocesu monitorování a přezkoumání.

Příklad

Tabulka 5 - Výpis ze seznamu zranitelností s uvedením možné hrozby a identifikovaným stávajícím opatřením (zdroj vlastní)

P. č.	*Aktivum*	*Zranitelnost*	*Hrozba*	*Opatření*
1.	*Data v uložišti na serveru*	*Není požadováno heslo pro vstup na uložiště v délce min. 10 znaků obsahující …*	*Hacker pronikne do uložiště*	*Požadováno heslo o min. délce 5 znaků od roku 2004*
2.	…..	…..	…..	…….

3.3.2 Analýza rizik kybernetické bezpečnosti

Identifikace a hodnocení následků [1; 4]

Cíle: Identifikovat následky, které mohou znamenat pro aktivum ztrátu důvěrnosti, dostupnosti a integrity. Stanovit hodnotu obchodního dopadu na organizaci (dosažení cíle).

Vstupní dokumenty jsou seznam aktiv, seznam rizik a zranitelností, vztahujících ke kritickým aktivům.

Následek je ztráta účinnosti, nepříznivé provozní podmínky, ztráta obchodu, pověsti, škoda na majetku atd. (následky stálé, dočasné) dle scénáře incidentu. Kritéria dopadu jsou definována v subprocesu stanovení kontextu. Následek zpravidla ovlivňuje jedno nebo více aktiv. Pozor - ovlivněno ale může být jen část aktiva.

Scénář incidentu (rizikový scénář) je scénářem působení hrozby využívající určitou zranitelnost nebo soubor zranitelností. Hrozba může různě využívat zranitelnosti a tak působení jedné hrozby na jedno riziko

může být popsána více scénáři s různými dopady (čas, intenzita působení hrozby).

Hodnota dopadu na organizaci se vyjadřuje v kvalitativně (např. nízká, střední, vysoká), kvantitativně (např. v Kč) nebo semikvantitativně (např. na stupnici hodnot 1-5). Kvantitativní vyjádření dopadu je náročné na množství dat a vyžaduje zkušeného risk manažera. Další vyjádření jsou méně náročné na data, ale jsou také méně přesná pro rozhodování.

Příklad

Rozpracováním dat z

Tabulka 5 jsou identifikovány scénář následující scénáře incidentu:

a) Hacker v časovém intervalu mezi 1,00 až 3,30 hod. ranní s využitím software identifikuje přístupové heslo v délce 5 znaků číselné řady na uložiště serveru. Identifikace hesla trvá max. 6 minut. Po identifikaci vstoupí do uložiště a zkopíruje uložená data v průběhu 2 hodin.

b) Hacker v časovém intervalu mezi 1,00 až 3,30 hod. ranní s využitím software identifikuje přístupové heslo v délce 5 znaků číselné řady na uložiště serveru. Identifikace hesla trvá max. 6 minut. Po identifikaci vstoupí do uložiště, kde nejprve zkopíruje uložená data v průběhu 2 hodin a poté data vymaže.

Dopad scénáře incidentu a jeho hodnota:

Ad a) Zkopírovaná data získá konkurence a použije je pro rozvoj vlastního know-how, čímž zvýší svoji konkurence schopnost na trhu vzhledem k poškozené organizaci. Organizace ztratí první pozici na trhu a obrat se sníží o 33 %. Dopad vysoký (kvalitativní) nebo 5 (semikvantitativní), ztráta 20 mil. Kč (kvantitativní).

Ad b) Zkopírovaná data získá konkurence a použije je pro rozvoj vlastního know-how, čímž zvýší svoji konkurence schopnost na trhu vzhledem k poškozené organizaci. Organizace neztratí první pozici na trhu (vzhledem k nízké důvěrnosti dat na uložišti) a obrat se sníží max. o 1 %. Data jsou vyzálohována a lze je rychle opět umístit na server (do 2 hodin). Dopad nízký (kvalitativní) nebo 2 (semikvantitativní), ztráta 50 tis. Kč (kvantitativní).

Určení pravděpodobnosti scénářů incidentu [1]

Cíl: Určit pravděpodobnosti scénářů incidentů (rizikových scénářů).

Vstupy - seznam identifikovaných scénářů incidentů, seznam rizik, kritických aktiv, využitých zranitelností a dopadů, seznam všech existujících a plánovaných opatření, jejich účinnost, uplatnění a stav použití.

Po vytvoření scénářů incidentů je nutné určit i pravděpodobnost každého scénáře a výskytu dopadu (kvalitativní, semikvantitativní nebo kvantitativní hodnocení). Důležité jsou informace o četnosti výskytu hrozeb a snadnost využití zranitelnosti, které je třeba vzít v úvahu. Stanovení pravděpodobnosti je ovlivněno:

- zkušenostmi a statistikami o pravděpodobnosti vzniku hrozeb,
- u aktérů (zdrojů) úmyslných hrozeb: jejich motivací a schopnostmi (časem se mění), dostupnými zdroji, vnímáním atraktivity a zranitelnosti aktiv,
- u aktérů (zdrojů) náhodných hrozeb: geografickými faktory, možností extrémních atmosférických podmínek a faktory, které by mohly mít vliv na lidská selhání a funkční poruchy zařízení,
- zranitelnostmi, jak jednotlivě, tak v souvislostech (agregace závislých rizik),
- již existujícími opatřeními a jejich účinností na snížení zranitelnosti.

V závislosti na potřebné přesnosti určení pravděpodobnosti se aktiva spojují do skupin (podle typu aktiv, působení stejné hrozby atd. – hledání závislostí pro agregaci závislých rizik) nebo rozdělují aktiva na jejich prvky a přiřazují se scénáře k daným prvkům.

Výstupem je definovaná pravděpodobnost scénáře incidentů (rizikových scénářů – kvantitativně, semikvantitativně nebo kvalitativně).

Příklad

Odhad pravděpodobnosti scénáře incidentu a) (viz bod 0.) – V minulosti již byly zaznamenány pokusy o proniknutí na uložiště, vzhledem k zvýšení kvality software k prolomení hesel je velká pravděpodobnost (70 % nebo 5) hraničící s jistotou, že dojde k prolomení hesla, získání dat a jejich využití konkurencí.

Objasnění použití ohodnocení pravděpodobnosti (kvalitativně, semikvantitativně, kvantitativně) – převod:

- *Nízká pravděpodobnost = 1-11 % = 1-2,*
- *Střední pravděpodobnost = 12-32 % = 3,*
- *Vysoká pravděpodobnost = více jak 32 % = 4-5.*

Určení hodnoty rizik a úroveň odhadu rizik [1; 2]

Cíl: Určit kvalitativní, semikvantitativní nebo kvantitativní hodnotu rizika.

Vstupem je seznam scénářů incidentů s jejich následky (ohodnoceny kvalitativně, semikvantitativně nebo kvantitativně).

Jestliže v předchozích krocích byla pravděpodobnost a dopad ohodnoceny kvantitativně a některé kvalitativně, tak je třeba všechny hodnoty převést na jednotné hodnoty. V současné praxi se nejčastěji využívá semikvantitativní hodnocení (bodová stupnice), která se následně využívá pro vytvoření mapy rizik.

Hodnota rizika je dána součinem pravděpodobnosti scénáře incidentu (rizikového scénáře) a dopadu tohoto scénáře na činnost organizace (dosažení cílů). Kromě toho může brát při výpočtu v úvahu i poměr přínosů (podstoupení rizika) a nákladů (ztráty), zájmy klíčových zainteresovaných stran a další kritéria pro hodnocení rizik.

Výstup – seznam rizik s přiřazenými úrovněmi hodnot.

Příklad

Hodnota rizika a) (viz bod 0.) je dána součinem pravděpodobnosti scénáře incidentu a hodnoty dopadu:

- *70 % * 20 mil. Kč = 14 mil. Kč (kvantitativní)*
- *nebo 5 * 5 = 25 (semikvantitativní).*

3.3.3 Vyhodnocení rizik kybernetické bezpečnosti

Cíl: Porovnat hodnoty a úrovně rizik s kritérii vyhodnocení a akceptace rizik.

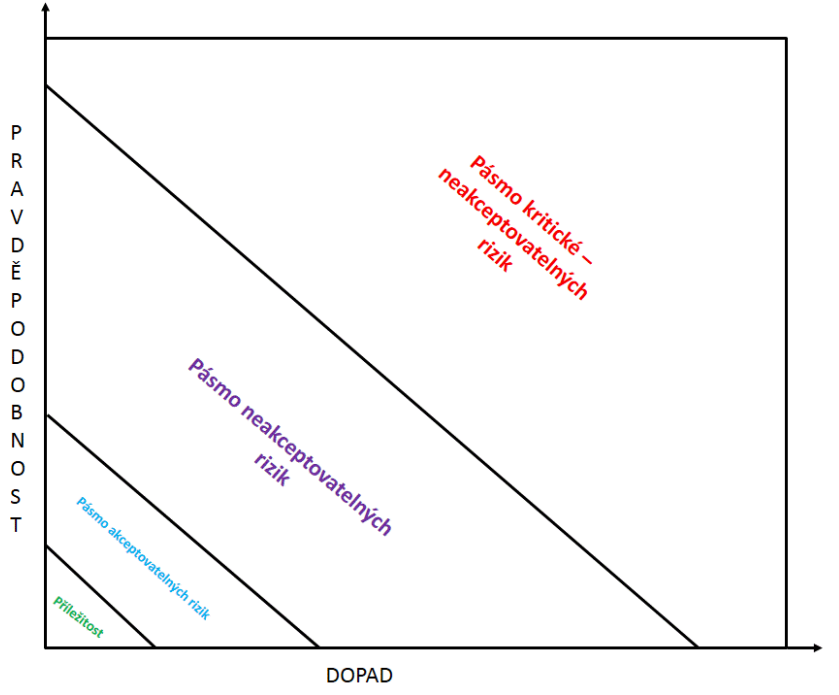
Vstup – seznam rizik s přiřazenými úrovněmi hodnot a kritéria pro vyhodnocení rizik.

Kritéria vyhodnocení rizik, používaná k rozhodování akceptace (viz Obrázek 5) nebo posunutí rizik ke zvládnutí, musí být v souladu

se stanoveným kontextem řízení rizik kybernetické bezpečnosti. Rozhodnutí o akceptaci rizik učiněná v rámci kroku vyhodnocení rizik vychází z definovaného rizikového apetitu. [1; 4]

Získané informace při analýze rizik je při vyhodnocování rizik využito k rozhodnutí o budoucích krocích (opatřeních na snížení zranitelnosti).

Nezbytnou součástí vyhodnocení rizik je první agregace závislých rizik (rozlišení závislých a nezávislých rizik). Pro určení závislých rizik je třeba identifikovat kritéria závislosti na základě popisu aktiv a jejich zranitelností, hrozeb a scénářů působení hrozeb. Dalším východiskem pro definování kritéria závislosti může také být pravděpodobnost řetězení rizik se střední až vysokou pravděpodobností vzniku a nízkým dopadem, které následně mohou vytvořit riziko s vysokým dopadem. Taktéž nahromadění většího množství nízkých nebo středních rizik může vyústit agregací rizik do vyšších celkových rizik a potřebu tuto situaci podle toho řešit (tzn. neakceptovat rizika, ale posunout ke zvládnutí). [1; 4]



Obrázek 5 – Pásma rizik v závislosti na pravděpodobnosti vzniku rizikového scénáře a velikosti dopadu na činnost organizace (zdroj vlastní)

Po vyhodnocení rizik jsou rizikům přiřazeny hodnoty priority (např. 1 – řešit okamžitě, 2 – připravit opatření, 3 – intenzivně monitorovat, 4 – monitorovat průběžně).

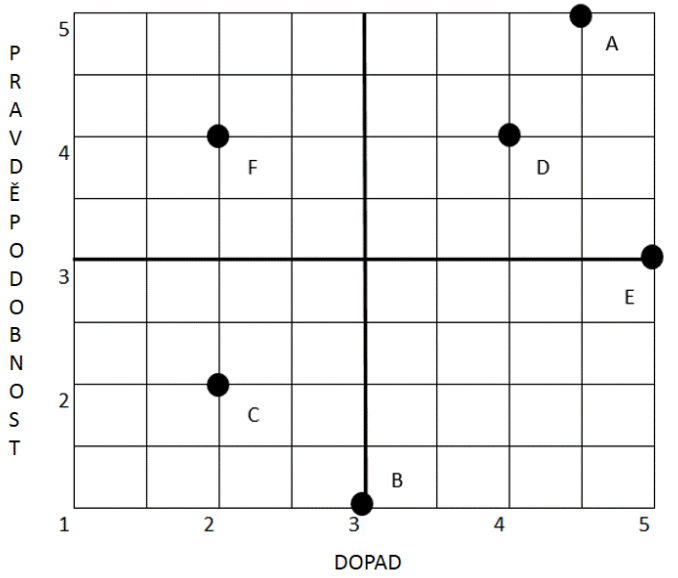
Výstupem jsou seznam rizik s přiřazenou prioritou, mapa rizik (viz Obrázek 6).

Příklad

Úroveň rizika a) (viz bod 0.) je 1 (priorita 1) na stupnici 1-4.

Objasnění prioritizace rizik:

- *1 – riziko nejvyšší úrovně (nepřijatelné, okamžitě nalézt a realizovat opatření),*
- *2 – riziko vysoké úrovně (neakceptovatelné, nalézt, připravit a případně realizovat opatření),*
- *3 – riziko střední úrovně (akceptovatelné, pouze monitorovat a přezkoumávat),*
- *4 – riziko nízké úrovně (příležitost prakticky nic nekonat, monitorovat a přezkoumávat nahodile).*



Obrázek 6 - Možná varianta mapy rizik (zdroj vlastní)

3.4. Zvládání rizik kybernetické bezpečnosti

Cíl: Identifikovat, připravit a případně realizovat potřebná opatření na úspěšné zvládnutí rizik vlastníky rizik s efektivním využitím zdrojů organizace pro dosažení cílů organizace.

Vstupem jsou seznamy rizik, kterým byla udělena priorita podle kritérií vyhodnocení rizik, aktiv a zranitelností, realizovaných a plánovaných opatření.

Zvládání rizik je rozděleno do sedmi kroků:

1. vyhnutí se riziku,
2. přenesení rizika (někdy také nazýváno sdílení rizika),
3. snížení rizika,
4. posunutí rizika,
5. agregace rizika,
6. akceptace rizika,
7. řízení akceptovaných rizik (příprava, včasná realizace opatření).

První tři kroky jsou standardní přístupy, které vyúsťují v definovaná opatření, které mají vliv na pravděpodobnost vzniku rizikového scénáře, nebo velikost dopadu působení hrozby na aktivum (aktiva), případně ovlivňují jak pravděpodobnost, tak i dopad současně.

Přístup ke zvládání rizik se realizuje postupně naplňovanými kroky 1 až 3. Nejprve se hledají opatření k vyhnutí se riziku, nelze-li se riziku vyhnout je nutno posoudit zda není možno riziko přenést (dodavatele, zákazníka, pojišťovnu atd.). Snížení rizika zvažuje manažer až v kroku 3. Při hledání vhodných opatření se manažer opírá o výstupy z hodnocení rizik, analýzy očekávaných nákladů, potřebu zdrojů na implementaci opatření a možných přínosů.

Jestliže jsou nalezena opatření, analyzovány náklady a potřeba zdrojů na zvládnutí, je třeba určit novou hodnotu sníženého rizika, vlastníky rizik odpovědných za přípravu a včasnou realizaci definovaných opatření. Každé navrhované opatření musí být také analyzováno z pohledu jeho dopadů a účinnosti, neboť může pokrýt i další riziko (rizika) k němuž opatření ještě nebylo stanoveno (agregace opatření). [1]

V případě, že manažer odpovědný za řízení rizik své úrovně nenalezne efektivní opatření v krocích 1 až 3, tak musí zvládnutí těchto rizik posunout na nadřízeného manažera. Subproces zvládání se tím vrací na počátek, ke kroku 1.

Rizika se stanovenými opatřeními a vlastníky rizik je třeba předložit nadřízenému manažeru ke schválení. Nadřízený manažer posoudí úroveň akceptace zbytkového rizika, opatření, výše nákladů na zvládání a potřebu zdrojů, včetně vlastníků rizik. Agreguje rizika (závislá i nezávislá) od podřízených manažerů do svého rizikového profilu a rozhodne:

- o ponechání předložených návrhů v nezměněné podobě,
- o převzetí některých rizik do své kompetence (definuje nová opatření a jmenuje vlastníky rizik),
- o případném posunutí vybraných rizik ke zvládání nadřízenému,
- o akceptaci zbytkového rizika (v souladu se stanoveným rizikovým apetitem organizace).

Při analýze opatření ke zvládání rizik je třeba přihlédnout:

- k tomu, jak riziko vnímají klíčové zainteresované strany,
- ke strategii přístupu k zainteresovaným stranám (jak s nimi komunikovat.

V subprocesu zvládání rizik je nutno vzít v úvahu všechna omezení, která byla identifikována v subprocesu stanovení kontextu.

Výstupem je plán zvládání rizik a zbytková rizika (plán protirizikových opatření).

3.4.1 Vyhnutí se riziku

Cíl: Vyhnout se činnosti nebo podmínce, která umožňuje vznik rizika.

Zpravidla se vyhnutí riziku přistupuje za následujících podmínek:

- identifikovaná rizika považována za příliš vysoká (priorita 1),
- náklady na jiné způsoby zvládání rizik (přenesení, snížení) převyšují přínosy (zpravidla analyzováno před posunutím nadřízenému).

Rozhodnutí o vyhnutí se riziku znamená, že organizace upustí od plánované nebo existující činnosti (souboru činností), nebo změní podmínky, za nichž činnost (vyvolávající riziko) provozuje. [1; 2]

Příklad
Data podléhající utajení nebudou již uložena na sdíleném uložišti (přístup z intranetu), ale bude s nimi pracováno na vyčleněných PC v zabezpečených místnostech se stanoveným režimem vstupu a oprávněním seznamování se s těmi to daty., které nejsou připojeny do sítě intranetu. Data na nosičích budou uložena v zabezpečené místnosti s definovaným režimem vstupu a oprávněním manipulace s těmi to daty.

3.4.2 Přenesení rizika

Cíl: Přenést riziko na jinou zainteresovanou stranu nebo s ní riziko sdílet a přenést nebo sdílet možnou ztrátu s touto zainteresovanou stranou, jestliže má schopnosti toto riziko efektivněji zvládnout.

Přenesení rizika může vyvolat nová rizika nebo měnit stávající již hodnocená rizika. Tato skutečnost může vyvolat nové hodnocení rizik. [1; 2]

Přenos lze provést:

- pojištěním (pokrytí negativních dopadů – ztrát),
- uzavřením smlouvy s dodavatelem nebo i zákazníkem.

Příklad
Uzavřená smlouva mezi organizací a dodavatelem služby (virtuální server). Tento dodavatel je pak plně zodpovědný za technický provoz toho serveru, zabezpečení dat a přístup k nim.

3.4.3 Snížení rizika

Cíl: Snížit pravděpodobnost vzniku rizikového scénáře nebo snížení negativního dopadu na činnost organizace (ztráty) na úroveň akceptace.

Opatření ke snížení rizik musí vycházet z kritérií akceptace rizik (např. rizikového apetitu, nákladů na snížení, časového rámce atd.), jakož i z dalších požadavků identifikovaných v subprocesu stanovení kontextu. Důležitým kritériem jsou taktéž celkové náklady na zvládnutí rizik ve vztahu k hodnotě chráněných aktiv. [1; 2]

Opatření ke snížení rizik lze provést s využitím těchto typů ochrany:

- náprava zjištěných nedostatků (kontrolní zjištění, audit atd.),
- prevence minimalizaci dopadu (ztráty),
- odstrašování aktéra od úmyslu zámyslu vzniku a působení hrozby,
- odhalení zdroje hrozby nebo aktéra,
- obnovení účinnosti realizovaných, plánovaných opatření,
- monitorování zvýšení pravděpodobnosti vzniku rizikového scénáře,
- zvýšení povědomí zaměstnanců a snížení pravděpodobnosti neúmyslného (nechtěného) vzniku rizikového scénáře (aktivum se stává aktérem).

Příklad

Kontrolou bylo zjištěno, že stávající antivirový software není dostatečně účinný, neboť jeho podpora dodavatelem není na odpovídající úrovni – opatření na snížení rizika: Nákup nového antivirového software splňující požadavky na úroveň zabezpečení.

Tento týden bylo oznámeno, že k 1. následujícího měsíce do organizace nastoupí 5 nových zaměstnanců, kteří mají odpovídající schopnosti práce se software a hardware. Noví zaměstnanci neznají pravidla přenosu, sdílení a archivace dat v organizaci – opatření na snížení rizika: V následujícím měsíci bud provedeno školení nových zaměstnanců se zaměřením na přenos dat, jejich sdílení a archivaci.

3.4.4 Posunutí a agregace rizik

Cíle: Zvládnout odpovídajícím způsobem rizika z vyšší úrovně řízení, není-li toho schopna daná úroveň řízení. Agregace závislých i nezávislých rizik do jednotného rizikového profilu. [1; 4]

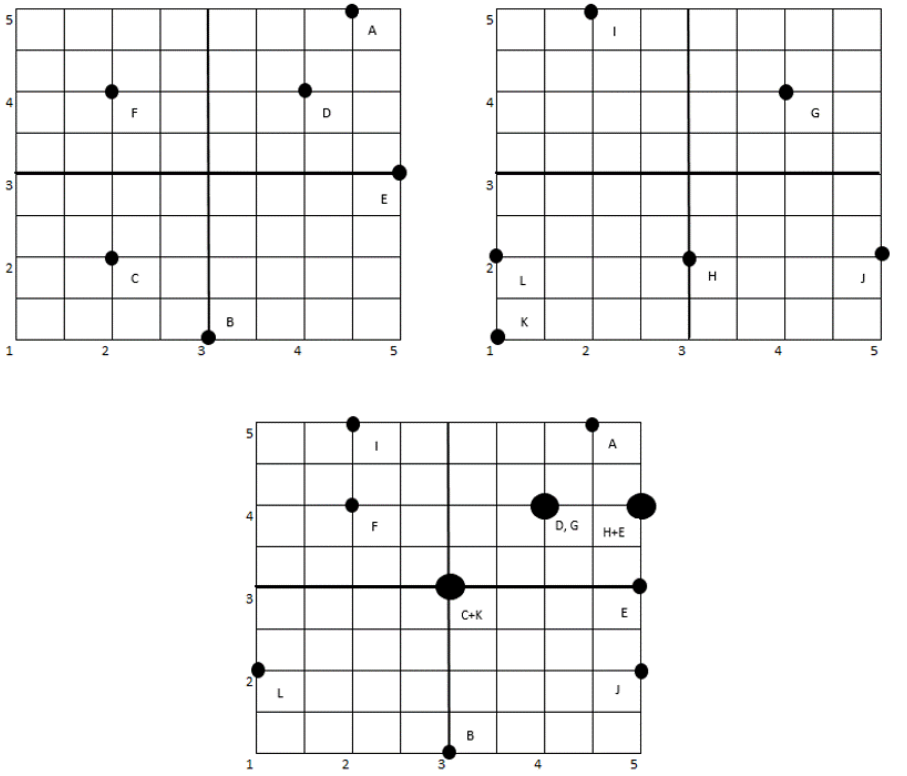
Příklad

Zvládané neúmyslné riziko – zaměstnanec otevře nevyžádanou e-mailovou poštu s infikovaným souborem (virem), který napadne intranetovou síť organizace (vyřadí z činnosti server a zničí uložená data).

Manažer není schopen ze své úrovně účinně a efektivně přijmout a realizovat potřebné opatření (např. poučení zaměstnanců organizace o práci s e-mailovou

poštou). Z tohoto důvodu posune toto riziko ke zvládnutí nadřízenému, který má odpovídající kompetence.

Nadřízený manažer obdrží od podřízených seznamy rizik a plány řízení rizik. Dokumenty analyzuje a vyhodnocuje (hledá závislosti mezi riziky ze seznamů). Výstupem je jednotný rizikový profil v jeho organizační působnosti (viz Obrázek 7) a nově definovaná opatření pro závislá rizika.



Obrázek 7 - Agregace rizik do jediného rizikového profilu (zdroj vlastní)

3.4.5 Akceptace rizik

Cíl: Rozhodnout o podstoupení rizika bez opatření ke zvládání rizika (na základě vyhodnocení rizika) nebo podstoupení rizika s odsouhlasenými opatřeními a akceptovatelnou zbytkovou hodnotou.

V souladu s definovanými kritérii akceptace rizik v subprocesu stanovení kontextu manažer akceptuje rizika po hodnocení rizik. Akceptace rizik je

završením kroku agregace rizik a schválení opatření ke zvládnutí rizik. [1; 2]

Příklad

Manažer 2. úrovně akceptoval sníženou hodnotu rizik (zbytkové riziko) po rozhodnutí o opatření ke zvládnutí.

Původní hodnota rizika – 5.

Opatření – nákup a instalace nového antivirového software, náklady 150 000,- Kč. Realizovat do 30. dne příštího měsíce.

Nová hodnota rizika – 2.

Nadřízení manažer 1. úrovně odsouhlasí navržené opatření a náklady.

3.4.6 Řízení akceptovaných rizik

Cíl: Včas a správně realizovat schválená opatření s minimalizací nákladů a potřebných zdrojů.

Řízení akceptovaných rizik spočívá v realizaci schválených opatření s naplánovanými zdroji a náklady. Důležitou složkou jsou vazby na subprocesy monitorování a přezkoumávání, komunikace a konzultace. Tyto subprocesy umožňují získávat informace o účinnosti realizovaných opatření, čase zahájení realizace opatření včetně dopadů na činnosti organizace a dosažených přínosech (vzhledem k dosahování cílů organizace). [1]

Příklad

Vlastník rizika má schválenými opatřeními delegovány kompetence k realizaci opatření:

- *výběr a nákup antivirového software,*
- *instalace antivirového software do pracovních stanic a serveru,*
- *proškolení uživatelů software k používání a zabránění infikování pracovních stanic a serveru.*

Další kompetence, které má delegovány:

- *finanční prostředky ve výši 150 000,- Kč,*
- *2 pracovníky IT k instalaci software a přípravu podkladů pro proškolení uživatelů (zaměstnanců organizace).*

Pro realizaci opatření jsou stanoveny následující milníky:

- *nákup a instalace antivirového software do 30. dne následujícího měsíce,*
- *proškolení uživatelů (zaměstnanců do 30. dne následujícího měsíce.*

Realizované kroky ke splnění opatření:

- *sběr informací o možnostech softwarových antivirových produktů dostupných na trhu a jejich cena (5 pracovních dní),*
- *výběr antivirového software a odsouhlasení výběru (2 pracovní dny),*
- *dodání a instalace softwarového produktu a jeho postupná instalace (10 pracovních dní),*
- *příprava proškolení a jeho realizace (2 pracovní dny),*
- *monitorování účinnosti realizovaného opatření.*

3.5. Komunikace a konzultace rizik kybernetické bezpečnosti

Cíl: Předávat, získávat a sdílet relevantní informace v dostatečném množství, kvalitě a potřebném čase z realizace sekvenčních subprocesů pro rozhodování v průběhu řízení rizik.

Vstup – informace z jednotlivých subprocesů řízení rizik kybernetické bezpečnosti.

Komunikace a konzultace rizik je subproces zaměřený k dohodě o tom, jak řídit rizika předáváním, výměnou a/nebo sdílením informací o rizicích mezi rozhodovateli a ostatními klíčovými zainteresovanými stranami. Obsah jednotlivých informací vychází z realizace jednotlivých sekvenčních subprocesů řízení rizik. [1; 2]

Efektivní komunikace mezi všemi klíčovými zainteresovanými stranami je základním kritériem pro zvládnutí relevantních rizik a rozhodování o nich. Komunikace zajistí, že odpovědní pracovníci za realizaci řízení rizik, a zainteresované strany, které mají na tomto procesu velký zájem, rozumějí podkladům, na jejichž podkladě rozhodují, a nutnosti realizace navrhovaných (přijatých) opatření. Komunikace musí být vždy obousměrná a otevřená.

Komunikace a konzultace umožňuje vnímat změny související s riziky, ať to jsou změny vyvolané zvenčí nebo zevnitř organizace. Vnímání změn vytváří potřebné předpoklady pro realizaci změn definice kritérií kontextu řízení rizik, což má následně dopad i do hodnocení rizik a přístupu ke zvládání rizik. Subproces komunikace a konzultace tak umožňuje

předcházet konfliktům mezi manažery a podřízenými, manažery klíčovými zainteresovanými stranami mimo organizaci. [1; 2]

Účelem komunikace a konzultace rizik je:

- shromažďování, sdílení a předávání informací o rizicích,
- jednotné vnímání obsahu rizik a jejich zvládání,
- snížení pravděpodobnosti výskytu narušení kybernetické bezpečnosti v důsledku nedostatku vzájemného porozumění mezi rozhodovateli a klíčovými zainteresovanými stranami, včetně snížení dopadů nedorozumění,
- podpora rozhodování,
- rozšíření znalostní databáze o kybernetické bezpečnosti,
- poskytnutí (vytvoření) pocitu odpovědnosti za rizika u rozhodovatelů a klíčových zainteresovaných stran.

Tak jak organizace tvoří plány komunikace pro řízení projektů, řízení rutinních činností a řízení krizových situací, tak je nutné sestavit plán komunikace rizik.

Organizace by měla pro řízení rizik jmenovat manažera rizik, který koordinuje řízení rizik napříč organizací s využitím komunikace a konzultace.

Výstup – jednotné vnímání procesu řízení rizik kybernetické bezpečnosti organizace a výsledků tohoto procesu.

3.6. Monitorování a přezkoumávání rizik kybernetické bezpečnosti

Cíle: Včas zjistit změny vstupů, výstupů jednotlivých sekvenčních subprocesů řízení rizik informací a včasná, efektivní realizace reakce na identifikované změny. Identifikovat příznaky blížící hrozby (realizace scénáře působení hrozby na zranitelnost aktiva) pro realizaci připravených opatření. Zkvalitňovat proces řízení rizik.

Změny, které je třeba zachytit, vyhodnotit a zrealizovat [1; 2]:

- kontextové změny ve specifikaci základních kritériích, rozsahu, hranic, organizační struktury a kritických aktiv procesu řízení rizik kybernetické bezpečnosti,

- kontextové změny v seznamech rizik, kterým byla udělena priorita podle kritérií vyhodnocení rizik, včetně rizikových faktorů, aktiv a zranitelností, realizovaných a plánovaných opatření, aktérů a zdrojů hrozeb,
- kontextové změny plánu zvládání rizik a zbytkových rizik (plánu protirizikových opatření), včetně účinnosti opatření.

Monitorování a přezkoumávání rizika umožňuje udržet komplexní přehled o rizikovém profilu organizace a tak zvýšit pravděpodobnost dosažení úspěchu (velikosti přínosů zainteresovaným stranám).

Je třeba si uvědomit, že rizika kybernetické bezpečnosti nejsou stálá, ale vysoce turbulentní, čehož jsem dnes svědky. Hrozby, zranitelnosti, pravděpodobnost nebo následky (velikost ztráty) se mohou náhle změnit, aniž by se objevilo nějaké varování či náznak toho co nastane. V prostředí kybernetické bezpečnosti to způsobují zdroje, které se rychle vyvíjejí a účinně používány aktéry (hackery). Tyto skutečnosti zdůrazňují nutnost neustálého monitorování a přezkoumávání.

Pozor - nové hrozby a zranitelnosti, změny pravděpodobností vzniku působení hrozby na zranitelnost mhou způsobit zvýšení rizik, která byla dříve hodnocena jako nízká (agregace závislých rizik).

Obecně platí, že výstup monitorování rizik vstupem pro přezkoumávání rizik, které vyúsťuje v nápravnou akci nebo do monitorování rizik. Nápravná akce je realizována při zjištění odchylek od již definovaného stavu, a to ať se jedná o odchylku pozitivní nebo negativní. Jestliže nejsou zjištěny žádné odchylky od definovaného stavu, tak se nápravná akce není vyvolána a může se přejít opat k monitorování. Tento stav lze přirovnat k pohybu po dvou kružnicích:

- monitorování, přezkoumávání, nápravná akce, a opět monitorování,
- monitorování, přezkoumávání, a opět monitorování.

Monitorování řízení rizik ve vztahu ke zkvalitňování celého procesu může vyústit ve změnu nebo doplnění pozměnění nebo doplnění metodiky řízení rizik v organizaci, včetně používaných nástrojů a technik nebo softwarové podpory v závislosti na:

- identifikovaných změnách obsahu jednotlivých kroků,

- četnosti opakování hodnocení rizik a detailu tohoto hodnocení,
- definovaných cílech procesu řízení rizik kybernetické bezpečnosti,
- předmětu procesu řízení rizik kybernetické bezpečnosti (například informačním procesu, jeho technickém zavedení a aplikaci, typu připojení k internetu).

Příklad:

Nová aktiva v rozsahu řízení rizik

Organizace přijala 2 nové programátory a správce intranetové sítě. Noví zaměstnanci představují zpravidla nové zranitelnosti (neznalost interních procesů, realizovaných a plánovaných opatření zvládaných rizik atd.), hrozby i rizikové scénáře. Případně zvýšení pravděpodobnosti stávajících rizikových scénářů (na stupnici 1-5 z 1 na 4), a tím i hodnot rizik (na stupnici 1-25, z 4 na 16), již akceptovaných rizik (je třeba rizika posunout ke zvládnutí). Na straně druhé noví programátoři mohou snížit pravděpodobnost rizikového scénáře (na stupnici 1-5 z 4 na 1) a hodnoty rizika (na stupnici 1-25, z 16 na 4). U takového to rizika mohou být ušetřeny zdroje používané na realizaci opatření (zrušení opatření) a riziko je dále pouze monitorováno.

Doporučení – při zařazení nových aktiv je třeba realizovat celý proces řízení rizik od počátku, neboť došlo ke změně kontextu řízení rizik.[7]

Nové hrozby

Organizace získala informace o nové hrozbě (bezpečnostním incident zaznamenaný mimo organizaci) – kybernetický útok prostřednictvím viru „Xb", který je zaměřen na získání dat. Hrozba není uvedena v seznamu rizik a z tohoto důvodu je třeba realizovat proces řízení rizik minimálně od subprocesu hodnocení rizik.

Doporučení - realizace celého procesu, z důvodu ujasnění si kontextu řízení rizik, vzhledem k nové hrozbě, a tím např. ušetření nákladů a zdrojů na případné zvládání rizika neboť jsou již připravena nebo realizována účinná opatření.

[7] *Týká se také změněny hodnot aktiv (nová kritická aktiva, která je třeba chránit).*

Literatura

[1] ČSN ISO/IEC 27005 - Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací.

[2] ČSN ISO/IEC 31000 - Management rizik – Principy a směrnice.

[3] HRŮZA, Petr. *Kybernetická bezpečnost.* 1. vydání. Brno: Univerzita obrany. 2012. ISBN 978-8-7231-914-5.

[4] HUJŇÁK, Petr, HUJŇÁK, Jaroslav. *Řízení rizik a příležitostí – metodické přístupy & praxe na projektech a v organizacích.* [online] [cit. 2013-05-15]. Dostupné z WWW: http://www.perpartes.cz/publikace/Nez%C3%A1visl%C3%A9+studie

4. Role kryptografie v kybernetické bezpečnosti

Kryptografie představuje souhrn matematických metod, které umožňují na logické úrovni ochránit informaci před jejím přečtením nebo modifikací. Při přenosu informace v otevřené čitelné podobě hrozí v přenosovém prostředí riziko jejího zachycení útočníkem. V prostředí Internetu tato nechráněná přenosová cesta začíná síťovým rozhraním odesílatele a končí síťovým rozhraním příjemce. Bez šifrování je informace kdekoliv na této trase útočníkovi přímo přístupná v otevřené podobě. Protože nelze fyzicky zabránit přístupu k přenosovému prostředí, musíme přítomnost útočníka brát v úvahu a informace během jejich přenosu chránit.

Krajním řešením by bylo nepřenášet elektronickou cestou žádné informace, které představují hodnotu pro jejich vlastníka. Takové řešení je zcela protichůdné k představě o výměně informací v informační společnosti, která je na výměně a sdílení informací v reálném čase přímo závislá a pro kterou informace představují hlavní nástroj činnosti.

Dalším protiopatřením by bylo přenášet cenné informace pouze fyzicky s vyloučením jejich výskytu ve veřejně přístupném přenosovém prostředí. Ruční distribuce informací by však znamenala značné zpoždění, nemožnost komunikace v reálném čase a materiální náročnost distribuce.

Z výše uvedených důvodů je kryptografie jediným v současné době dostupným způsobem, jak logicky ochránit informace během jejich přenosu nebo uložení. Přenos informací v šifrované podobě znemožňuje především jejich přečtení a úmyslnou modifikaci ze strany útočníka. Zajištění důvěrnosti bylo původně jediným smyslem kryptografie v počátcích jejího vzniku. Moderní kryptografické algoritmy však umožňují další bezpečnostní služby. Tyto kromě samotného utajení obsahu zprávy zajišťují bezpečnostní funkce zvyšující bezpečnost, důvěrnost a průkaznost ukládaných, sdílených a přenášených informací.

Běžně jsou dnes elektronickou cestou přenášeny informace, jejichž výskyt v jiné než písemné podobě byl dříve z bezpečnostních důvodů nepřípustný. Důvěra v komunikační prostředí vzrostla a pravděpodobně souvisí spíše se zevšedněním informačních technologií v našem životě, než s nárůstem bezpečnosti komunikace. K pasivním útokům na přenášené

informace v podobě jejich odposlechů přibývají také útoky aktivní. Ty jsou zaměřeny především na průnik do informačních systémů, zahlcení systémů a modifikace ukládaných a přenášených informací. Vzhledem k požadavku na dostupnost těchto systémů prostřednictvím veřejného přenosového prostředí vyvstává problém s jejich zabezpečením proti kybernetickým útokům. Pomocí kryptografie lze realizovat řadu bezpečnostních služeb, které mohou kybernetickou odolnost zvýšit.

V minulosti byla kryptografie převážně doménou diplomacie, tajných služeb a ozbrojených složek. Teprve v sedmdesátých letech 20. století byly veřejně publikovány první kryptografické algoritmy pro civilní a komerční využití.

V první dekádě 21. století došlo vlivem rozšíření Internetu a elektronických transakcí k masovému zasazení kryptografických algoritmů do nejrůznějších komerčních koncových zařízení a komunikačních protokolů a šifrování se tak stalo běžnou součástí každodenního života.

4.1. Bezpečnostní služby realizovatelné pomocí kryptografie

Kryptografické algoritmy vznikaly primárně za účelem utajení obsahu zprávy, tedy k zajištění důvěrnosti přenášené informace. Až s nástupem moderních kryptografických algoritmů se možnosti využití šifrovacích algoritmů rozšiřují na autentizaci odesílatele, ověření nepozměněnosti obsahu zprávy a možnost elektronickou cestou podepsat dokumenty v jejich datové podobě. Současná kryptografie poskytuje kromě důvěrnosti a řízení přístupu také zajištění integrity a autentizace obsahu zprávy, autentizaci původce zprávy a nepopíratelnost manipulace s ní.

Jednotlivé bezpečnostní funkce realizovatelné pomocí kryptografie lze definovat jako:

Důvěrnost (***confidentiality***) – zajištěním důvěrnosti rozumíme takovou vlastnost zprávy, že její obsah je nečitelný pro jakoukoliv neoprávněnou osobu. Při přenosu zprávy rozumíme oprávněnými osobami odesílatele a příjemce zprávy. Při uložení zprávy může být odesílatel totožný s příjemcem zprávy (vlastník souboru). Neschopnost útočníka přečíst kryptogram je dána neznalostí dešifrovacího klíče.

Integrita (*integrity*) – zajištěním integrity rozumíme možnost prokázat celistvost a neporušenost přenesené zprávy. Odesílatel a příjemce chtějí mít možnost prokázat, že přijatá zpráva je totožná s odeslanou. Pomocí kryptografických technik lze odhalit pokus útočníka o vymazání části přenášené zprávy nebo modifikaci některých znaků zprávy. Lze také odhalit pokus o zpřeházení bloků zprávy nebo pokus o doplnění obsahu.

Autentizace (*authentication*) **–** výhradní vlastnictví šifrovacího klíče pro tvorbu elektronického podpisu slouží k jednoznačnému prokázání identity osoby, vlastnictví dat, autorství dokumentu nebo oprávnění k určitému úkonu. Na rozdíl od autentizace pomocí uživatelského hesla je při kryptografických autentizačních technikách znám pouze výsledek operace závislé na klíči. Prokázáním schopnosti šifrovat tímto klíčem je dokázáno jeho vlastnictví bez nutnosti zveřejnění nebo přenášení tohoto klíče.

Dostupnost (*availability*) – dostupnost dat nebo systémových služeb lze zajistit pomocí autentizace uživatele informačního nebo komunikačního systému kryptografickými technikami. Pro útočníka bez znalosti kryptografického klíče je služba nedostupná z toho důvodu, že neprokáže svoje oprávnění. Díky tomu systém obsluhuje pouze osoby, které jednoznačně autentizoval a nemůže být zahlcen neoprávněnými požadavky. Řízení přístupu k službám je v současnosti typické pouze u uzavřených systémů korporací nebo státu.

Nepopíratelnost (*non-repudiation*) – nemožnost popřít zpětně autorství zprávy nebo odpovědnost za její odeslání, přijetí či seznámení se s jejím obsahem. Nepopíratelnost je dána tím, že manipulace se zprávou je podmíněna použitím kryptografického klíče drženého ve výhradním vlastnictví konkrétní osoby. Ve vztahu odesílatel-příjemce zprávy je tak možné zajistit vzájemnou nepopíratelnost na obou stranách komunikace.

4.2. Základní principy a pojmy v kryptografii

Svým historickým vývojem se kryptografie jako obor lidské činnosti nachází na pomezí matematiky a informatiky. Zahrnuje mechanismy a postupy spočívající v utajení obsahu zprávy a další bezpečnostní funkce. **Kryptografie** je spolu se **steganografií** a **kryptoanalýzou** součástí samostatného vědního oboru, nazývaného **kryptologie**.

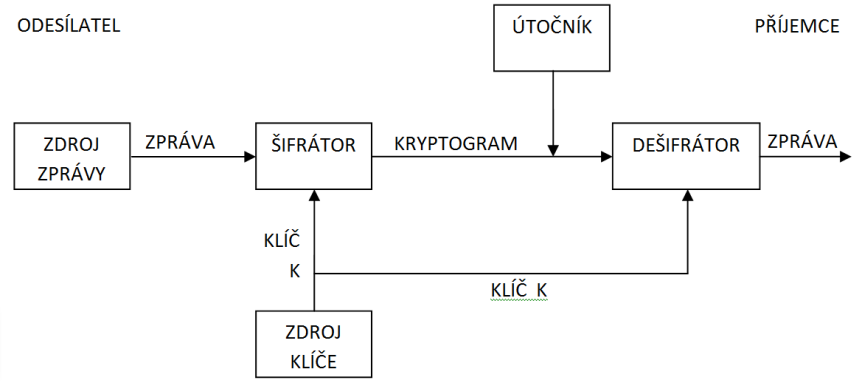
Zatímco kryptografie se zabývá znečitelněním obsahu zprávy, steganografie se zabývá utajením samotné existence zprávy.

Kryptografie zprávu pozmění na základě matematických postupů do podoby nečitelné bez znalosti dešifrovacího postupu a především bez znalosti dešifrovacího klíče.

Steganografie na rozdíl od kryptografie způsobí ukrytí samotné zprávy v prostředí, kterým je zpráva přenášena nebo v kterém je uložena. Steganografie používá takové principy a techniky, které umožní uložit nebo přenášet zprávu na pozadí jiné zprávy tak, aby utajená zpráva nebyla zjistitelná útočníkem. Obsahově nesouvisející zpráva poslouží pouze jako nosič steganograficky utajeného textu.

Jiné steganografické postupy zahrnují ukrytí zprávy na prázdném přenosovém médiu. Informace je zaznamenána nebo přenášena pod rozlišovací schopností útočníka. V takovém případě má útočník dojem, že přenosové prostředí nebo paměťové médium neobsahuje žádnou informaci.

Kryptografický systém se skládá z šifrovacího a dešifrovacího zařízení, z šifrovacího a dešifrovacího klíče, zprávy v otevřeném textu a kryptogramu. Lidský faktor je v schématu zastoupen prvky odesílatel, příjemce a útočník. **Odesílatel** a **příjemce** jsou uživateli kryptografického systému a jejich cílem je zabezpečené přenesení zprávy. **Útočník** vstupuje do přenosového prostředí s cílem přečíst zprávu, modifikovat její obsah nebo se vydávat za jednu z komunikujících stran. Přenosové prostředí představuje jakékoliv komunikační prostředí, kterým je zpráva po zašifrování přenášena. Příkladem takového prostředí je Internet.



Obrázek 8 - obecné schéma kryptografického systému podle [8].

Transformace otevřeného textu zprávy do podoby kryptogramu se nazývá **šifrování**. **Dešifrování** je operací inverzní k šifrování a dochází při něm k transformaci kryptogramu do podoby zprávy ve formě otevřeného textu. Šifrování a dešifrování je závislé na hodnotě klíče.

Šifrovací klíč je jedinečná informace o pevně definované délce, která je parametrem šifrovacího algoritmu a má zásadní vliv na podobu výstupu šifrování. Při každém použití stejného šifrovacího klíče a stejného algoritmu k zašifrování stejné zprávy je výsledkem šifrování vždy shodný kryptogram. Změna klíče znamená změnu podoby kryptogramu pro dvě stejné zprávy při jejich šifrování. Klíč může mít podoby písmen, číselné sekvence nebo u moderních šifrovacích algoritmů je vyjádřen pomocí řetězce bitů.

Kryptografický algoritmus jsou matematické operace pro šifrování a dešifrování, popsané v pevně definovaném sledu s přesně definovanou formou vstupních hodnot, výstupních hodnot a proměnného klíčového parametru. Smyslem ustálení postupu do formy algoritmu je jednoznačnost při postupu šifrování a dešifrování odesílatelem a příjemcem. Algoritmus je popsatelný sadou matematických vztahů.

Konkrétní způsob, jak jsou tyto vztahy vyjádřeny v programovacím jazyce nebo zapojeny pomocí logických obvodů se nazývá **implementace** kryptografického algoritmu. Chyby v implementaci mohou představovat výrazné bezpečnostní riziko pro jinak kvalitní a odolný kryptografický

algoritmus. Záleží tedy na přesném pochopení funkce a smyslu jednotlivých bloků šifrování a dešifrování.

Šifrátor představuje finální podobu implementace kryptografického algoritmu. Z hlediska formy provedení lze rozdělit šifrátory na softwarové a hardwarové.

Softwarový šifrátor může být proveden jako samostatný program s grafickým uživatelským rozhraním, zdrojový kód ve skriptovacím jazyce (např. PHP), utilita spustitelná v konzolovém režimu nebo zásuvný plugin modul. Pomocí pluginu lze například rozšířit funkcionalitu webového prohlížeče nebo e-mailového klienta. Softwarové šifrátory jsou pro nízkou finanční nákladnost jejich pořízení a distribuce typické pro použití v komerční sféře a u koncových uživatelů. Typickým prostředím pro jejich využití je Internet.

Hardwarový šifrátor je jednoúčelové zařízení, v němž je kryptografický algoritmus realizován pomocí speciálně navržených obvodů a firmware. Mezi hlavní výhody hardwarových šifrátorů patří několikanásobně vyšší rychlost šifrování v porovnání se softwarovými. Důvodem jsou optimalizované obvody, navržené přesně k tomuto účelu. Hardwarové šifrátory jsou určeny k šifrování ve státní správě, telekomunikacích, bankách, silových složkách a k ochraně utajovaných informací. Mohou šifrovat velmi velké objemy dat a lze je použít k zabezpečení celého přenosového kanálu mezi pobočkami organizace.

Veškeré kryptografické algoritmy do druhé poloviny sedmdesátých let používaly shodný klíč pro šifrování a dešifrování. Právě pro symetričnost použití klíče na straně odesílatele i příjemce byly tyto později nazývány jako **symetrická kryptografie**. Klíč je používán oběma stranami komunikace pro šifrování i dešifrování. Tyto postupy jsou vzájemně inverzní a pracují se shodnou vstupní podobou klíče. Odesílatel s příjemcem proto musí klíč společně sdílet, distribuovat a utajit jeho podobu před útočníkem. V opačném případě by totiž byl schopen kryptogramy nejen číst a modifikovat, ale i vydávat se podvržením kryptogramu za libovolnou z komunikujících stran. Z důvodu nutnosti utajení symetrického klíče bývají tyto systémy nazývány jako kryptografické **kryptografie s tajným klíčem**.

Mezi největší problémy spojené s používáním symetrických systémů patří obrovský nárok na počet klíčů při rostoucím počtu šifrujících účastníků. Pro splnění podmínky důvěrnosti mezi každou z možných komunikujících dvojic je zapotřebí počet unikátních klíčů odpovídající počtu možných propojení mezi uživateli. Tento problém není zřetelný pro pouhé dva uživatele, kteří využívají jediný klíč. Naopak markantní je pro 10 uživatelů, mezi kterými existuje 45 možných vzájemných propojení. Počet klíčů k potřebných pro n uživatelů se dá vyjádřit vztahem $k=(n^2-n)/2$

V druhé polovině sedmdesátých let 20. století došlo k významným změnám ve vývoji kryptografie. Nedostatky symetrických systémů byly již dobře známy a očekávanou náhradou měla být **asymetrická kryptografie.** Asymetričnost spočívá v použití dvojice klíčů vztahující se přímo k jejich vlastníkovi a nikoliv ke komunikujícím stranám vzájemně, jako tomu je u symetrických systémů. Asymetrická kryptografie pracuje s veřejným tajným klíčem uživatele. Podle vlastnosti, která umožňuje šířit veřejně šifrovací klíč při utajení tajného klíče se pro asymetrické kryptosystémy vžil také pojem **kryptografie s veřejným klíčem**. Asymetrická kryptografie však symetrické šifrování díky své výpočetní náročnosti oproti očekávání nenahradila. Symetrické šifry jsou nezastupitelné pro šifrování dat, zatímco asymetrické šifry jsou masivně použity v systémech elektronického podpisu. Pro aplikace, v kterých jsou oba systémy účelově kombinovány, se vžil pojem **hybridní kryptosystémy.** Toto označení znamená, že daný kryptosystém používá pro určité operace symetrických algoritmů a pro jiné asymetrických.

Kryptoanalýza se zabývá získáním otevřeného textu původní zprávy z kryptogramu bez znalosti dešifrovacího klíče. Výsledkem kryptoanalýzy je získání čitelné zprávy, obsažené v kryptogramu. Nalezení konkrétního klíče z množiny všech možných klíčů použitelných k dešifrování můžeme, nazýváme jako **prolomení klíče**. V okamžiku nalezení konkrétního klíče je útočník schopen dešifrovat nejen tuto zprávu, ale i všechny předchozí a následující zprávy šifrované stejným klíčem. Nalezení konkrétního klíče **nemá vliv na bezpečnost použitého algoritmu**. Uhodnutí klíče protivníkem představuje stejné bezpečnostní riziko, jako vyzrazení klíče. Kompromitovaný klíč je nutné přestat používat a neprodleně jej změnit.

Změna klíče totiž znamená pro útočníka vždy nový proces hledání mezi všemi klíči dané délky, které připadají v úvahu.

Dalším předmětem kryptoanalýzy je nalezení postupu k dešifrování libovolné zprávy zašifrované **jakýmkoliv klíčem** pomocí konkrétního algoritmu. Nalezení takového postupu nazýváme jako **prolomení algoritmu**. Motivem kryptoanalýzy je v tomto případě snaha o nalezení univerzálního postupu, který by útočníkovi výrazně zkrátil dobu potřebnou k dešifrování bez znalosti klíče. Po prolomení algoritmu nehraje kryptografický klíč pro útočníka zásadní roli. Doba dešifrování je výrazně kratší, než zkoušení veškerých možných klíčů. Změna klíče mezi odesílatelem a příjemcem neznamená pro útočníka vážný problém, dešifrování všech kryptogramů po prolomení algoritmu trvá přibližně stejně dlouho. Prolomení algoritmu má zásadní vliv na jeho bezpečnost a znamená výrazné oslabení nebo úplné vyřazení role klíče v šifrovacím schématu. Prolomený algoritmus nesmí být z výše uvedených důvodů dále používán ani po změně klíče a musí být nahrazen jiným algoritmem.

Hlavními motivy hledání slabin algoritmu jsou prolomení slabého algoritmu protivníka nebo naopak ověření odolnosti vlastního kryptografického algoritmu. V případě dlouhodobého neúspěchu systematicky a odborně vedené kryptoanalýzy lze konstatovat, že kryptografický algoritmus odolává všem aktuálně známým druhům útoků.

Vývoj v oblasti kryptoanalýzy je neustálá výzva spočívající v aplikaci nových matematických poznatků na stávající algoritmy se snahou prokázat jejich odolnost nebo naopak prolomitelnost. Poněkud paradoxní je skutečnost, že u žádného z kryptografických algoritmů nebyla průkazně dokázána jeho neprolomitelnost.

Vzhledem absenci důkazu neprolomitelnosti kryptografických algoritmů se hovoří spíše o jejich schopnosti odolávat doposud známým druhům útoků po určitou předpokládanou dobu. Pravidelně bývají publikovány odborné studie odhadované doby odolnosti používaných délek šifrovacích klíčů s doporučením, jak dlouhé klíče používat pro šifrování informací s nutností velmi dlouhodobého utajení.

4.3. Klasická kryptografie

Historie kryptografie sahá podle dostupných zdrojů do období 5. století před naším letopočtem [9]. Z tohoto období pochází systém Skytalé, který sloužil k jednoduché transpozici písmen zprávy. Transpozicí rozumíme změnu pozice písmen ve zprávě, přičemž kryptogram se skládá ze stejných písmen umístěných na nové pozice ve zprávě v závislosti na šifrovacím klíči.

V případě Skytalé se na dřevěnou hůl o určitém průměru navinula v těsných závitech vedle sebe páska, na niž byla po řádcích podélně zapsána zpráva k utajení. Po rozvinutí pásky vzniknul kryptogram složený z původních písmen zprávy, uspořádaných svisle v jednom sloupci. Klíčem k sestavení původní zprávy bylo vlastnictví stejné hole o shodném průměru. Zjednodušeně se jednalo o spirálovitou transpozici z řádku do sloupce, protože útočník měl v případě zcizení kryptogramu k dispozici všechna původní písmena tvořící zprávu, uspořádaná v novém pořadí daném parametry klíče (rozměrem hole).

Na tomto více jak dvě tisíciletí starém způsobu šifrování je zajímavé, že obsahuje všechny rysy obecného schématu kryptografického systému, podobně jako moderní šifrovací systémy.

Původní zpráva byla změněna do podoby kryptogramu v závislosti na klíči. Klíč má konkrétní podobu z celé řady možných hodnot (možných kombinací průměrů hole).

Právě volba klíče neznámého útočníkovi má za následek, že i přes znalost postupu šifrování není schopen dešifrovat zprávu stejně rychle jako oprávněný odesílatel a příjemce.

Již tento systém i přes znalost algoritmu představuje pro útočníka při neznalosti klíče značnou časovou překážku v podobě nutnosti vyzkoušení velmi značného množství potenciálních klíčů.

Pokud by však nebyl omezen časově ani finančně, dokázal by v konečném čase vždy dešifrovat informaci. Tato vlastnost platí pro všechny klasické šifrovací systémy.

Nejstarší období kryptografie od počátků šifrování do doby vzniku elektromechanických rotorových šifrátorů na přelomu 19. a 20. století

zahrnuje poměrně snadno pochopitelné šifrovací postupy, založené na **transpozici** a **substituci** znaků zprávy.

Transpozice znamená systematickou záměnu pořadí znaků v závislosti na klíči. Substituce naopak spočívá v nahrazování znaků zprávy pomocí jiné sady znaků. Každé písmeno zprávy si v kryptogramu zachovává svoji pozici, ale je nahrazeno jiným znakem.

Substituční šifra je takový postup šifrování, při kterém je každé písmeno z abecedy zprávy nahrazeno (substituováno) odpovídajícím písmenem abecedy kryptogramu. Tyto dvě abecedy se od sebe zásadně liší a každému písmenu zprávy odpovídá jedno nebo více nových písmen abecedy kryptogramu.

Monoalfabetická substituce přiřazuje jednomu znaku z abecedy zprávy vždy stejný znak z abecedy kryptogramu, která je definována klíčem. Na základě klíče je uspořádána abeceda kryptogramu a pro daný klíč je vždy k šifrování používána tato abeceda. Nový klíč znamená novou abecedu kryptogramu. Níže je uveden příklad přeuspořádání abecedy pro konkrétní podobu klíče K={TAJNE}.

Abeceda zprávy = {ABCDEFGHIJKLMNOPQRSTUVWXYZ}
Klíč = {TAJNE}
Abeceda kryptogramu = {TAJNEBCDFGHIKLMOPQRSUVWXYZ}

Polyalfabetická substituce pracuje s více abecedami, které se periodicky střídají v závislosti na hodnotě klíče. Příkladem takového systému je Vigenerova šifra, která využívá 26 různých abeced, vzniklých posunutím klascické abecedy o 0 až 25 znaků. První abeceda je nepozměněná, druhá začíná písmenem „B“ a končí znaky „XYZA“. Třetí abeceda začíná písmenem „C“ a končí znaky „YZAB“. Tyto abecedy jsou uspořádány do tabulky Při šifrování je výsledný znak kryptogramu daný znakem tabulky tvořícím průsečík mezi znakem zprávy nalezeným v prvním řádku a znakem klíče nalezeném v prvním sloupci tabulky.

V případě, že nahrazujeme některá písmena abecedy pomocí střídání více znaků z abecedy kryptogramu, hovoříme o **homofonní substituční šifře**. Abeceda kryptogramu je výrazně větší, než abeceda zprávy. Důvodem

k substituci některých znaků abecedy zprávy pomocí více znaků abecedy kryptogramu je snaha zakrýt v šifrovaném textu ta písmena, která se v jazyce zprávy vyskytují výrazně častěji oproti jiným. Při dostatečně dlouhém zachyceném kryptogramu by útočník byl schopen provést frekvenční kryptoanalýzu pomocí odhadování a postupného dosazování možných významů znaků.

V českém jazyce se například ve více než 5% textu vyskytuje písmeno „E“. Ve snaze ztížit protivníkovi odhad významu tohoto znaku na základě jejich četnosti v kryptogramu se u homofonní šifry nahradí střídavě pomocí více substitučních znaků (např. E=X, *, -). Výsledkem je dosažení přibližně stejné četnosti všech znaků v kryptogramu, což vede k ztížení frekvenční analýzy šifrového textu.

Transpoziční šifra je takový šifrovací postup, při kterém dochází k systematické záměně pozic znaků zprávy při zachování jejich významu. Přeuspořádání písmen zprávy do podoby kryptogramu je závislé na klíči. Samotný systém transpozice je dán algoritmem. Všechna písmena zprávy se objeví ve výstupním kryptogramu, změní se pouze jejich pozice. Značnou slabinou transpozičních šifer je opět zachování četnosti znaků jazyka, v které byla zpráva vytvořena.

Období klasických šifer bylo charakteristické ručním šifrováním v písemné podobě a orientací na abecedy znaků zprávy a kryptogramu. Mnoho klasických šifer je v současnosti snadno luštitelných při dostatečné délce zachyceného kryptogramu. Toho si byl vědom již v 15. století Leon Battista Alberti, když přeložil a interpretoval arabské texty o kryptoanalýze. Vzájemné kombinace transpozičních a substitučních systémů v 15. – 19. století zvyšovaly v tehdejší době jejich odolnost. Z dnešního pohledu však nárůst složitosti není nikterak významný. Klasické šifry dnes nelze považovat za odolné. Alberti též zrealizoval mechanickou verzi šifrovacího disku, představující polyalfabetickou substituci. Albertiho šifrovací disk mohl být inspirací pro generaci mechanických rotorových šifrátorů, které se objevily v dvacátých letech 20. století a jejich používání postupně skončilo až v sedmdesátých letech 20. století. Již u rotorových šifrátorů typu ENIGMA bylo patrné, že v kryptografii dochází k prudkému vývoji směrem k zvýšení počtu možných klíčů. Současně se

zvyšovala složitost šifrovacích algoritmů, byť byly stále zaměřeny na práci se znaky abecedy.

4.4. Moderní symetrické kryptosystémy

Moderní **symetrické kryptografické systémy** vycházejí z klasických postupů, které představuje transpozice a substituce. S nástupem polovodičů a rozvojem výpočetní techniky se kryptografie neorientuje na znaky zprávy, ale na jejich bitovou reprezentaci. Moderní kryptosystémy tak pracují s jednotlivými bity. Stejně tak klíč je prezentován v podobě bitové postupnosti. Délka klíče se začíná uvádět v bitech.

Moderní symetrické šifry lze rozdělit na proudové šifry a blokové šifry, dle množství a uspořádání bitů zprávy při šifrování.

Proudové šifry zpracovávají postupně jednotlivé bity zprávy s klíčem. Každý bit výsledného kryptogramu je závislý na jediném bitu zprávy a jediném bitu klíče. Zpráva vstupuje do šifrátoru jako proud bitů. Nejjednodušší formu proudové šifry představuje vzájemné sčítání bitů zprávy pomocí logické operace XOR. Exklusivní disjunkce přiřazuje rozdílným vstupům výstup v logické úrovni „1“ a shodným vstupům výstup v logické úrovni „0“. Jsou-li bity klíče a zprávy shodné, výsledek šifrování je vždy „0“. Jsou-li bity klíče a zprávy rozdílné, výsledkem je bit kryptogramu v hodnotě „1“. Dešifrování se provádí opětovným sečtením kryptogramu a klíče. Nevýhodou proudové šifry je náročnost na délku klíče. Nejlepším řešením by byl klíč o délce shodné s délkou zprávy, protože periodické opakování kratšího klíče představuje slabinu. Z tohoto důvodu se proudové šifry s náhodným neopakovaným klíčem o shodné délce jako zpráva používají velmi zřídka.

Blokové šifry zpracovávají zprávu po blocích o pevně stanovené délce. Zpráva je dělena na bloky o pevné velikosti např. 64 bitů a šifrování je postupně prováděno s každým blokem. Během šifrování se provádějí permutační a substituční operace s celým blokem. Sada permutací a substitucí je označována jako rundovní operace. Runda se opakuje vícenásobně. Například pro algoritmus DES je počet rund 16, pro moderní AES je počet rund 10. Šifrovací klíč může mít délku např. 56 bitů (DES), 128-256 bitů (AES) a je používán cyklicky pro libovolně dlouhou zprávu. Ze zadaného klíče se pro každou z rund generuje rundovní subklíč.

Moderní blokové šifry mají nelineární vnitřní uspořádání konstrukčních prvků s vysokou lavinovitostí. Na podobě výstupního zašifrovaného bloku kryptogramu se kromě klíče podílí i každý jeden bit bloku zprávy. Bity v bloku zprávy tedy při substituci vzájemně ovlivňují budoucí podobu celého bloku kryptogramu. Změna jediného bitu v bloku zprávy před zašifrováním má za výsledek výstupní blok kryptogramu odlišný v polovině hodnot bitů.

Prvním veřejně publikovaným symetrickým blokovým algoritmem byl Data Encryption Standard. Jeho autorem je Horst Feistel, tehdejší zaměstnanec firmy IBM, který dle požadavku americké National Security Agency přepracoval firemní algoritmus Lucifer. DES byl publikován ve standardu FIPS PUB 46 v roce 1977 a byl používán téměř dvě desetiletí pro neutajované informace v USA. Poté byl rozšířen na trojnásobnou délku klíče 168 bitů. Tato varianta byla nazvána 3DES. V současné době je DES nahrazen pro stejné účely šifrovacím algoritmem Advanced Encryption Standard, který umožňuje délku klíče až 256 bitů. Algoritmus byl publikován v roce 2001 ve FIPS 197. Algoritmus AES je široce rozšířen v nejrůznějších koncových zařízeních i komunikačních protokolech.

4.5. Moderní asymetrické kryptosystémy

Asymetrická kryptografie je způsob šifrování a dešifrování, založený na použití **rozdílných klíčů** pro operaci šifrování a dešifrování. Tyto klíče i přes svoji rozdílnost tvoří jedinečný a nezaměnitelný klíčový pár a jsou vygenerovány společně během jednoho matematického postupu.
Oba klíče se při svém použití vztahují přímo k osobě jejich vlastníka. Jedná se tedy o veřejný a tajný klíč daného uživatele, konkrétní osoby. Přestože spolu tajný a veřejný klíč úzce souvisejí, zásadně se liší způsob jejich použití. V tomto spočívá podstata asymetrie na rozdíl od symetrických systémů, kde pro šifrování i dešifrování byl používán vždy stejný klíč a navíc tento shodný klíč používaly obě strany komunikace (odesílatel a příjemce). U asymetrické kryptografie má každý uživatel dvojici svých klíčů, svůj **klíčový pár.**

Hlavním rysem a současně největší výhodou asymetrické kryptografie je možnost zveřejnit **veřejný klíč**, pokud tajný klíč zůstane nadále utajen a ve výhradním vlastnictví jeho majitele. Zveřejnění veřejného klíče tedy nemá

vliv na bezpečnost tajného klíče. **Tajný klíč** z veřejného nejde snadno vypočítat.

Asymetrické kryptosystémy jsou vždy založeny na matematickém problému, který je velmi snadno řešitelný při úplném zadání (znalosti tajného parametru) a současně velmi velmi obtížně řešitelný při neznalosti tajného parametru.

Dalším rysem je **nesymetrické použití obou klíčů**. Použijeme-li k šifrování veřejný klíč, dešifrování se provede tajným klíčem (tedy druhým klíčem z klíčového páru). Při použití tajného klíče k šifrování je naopak použit veřejný klíč k dešifrování.

Teoretické koncepty asymetrické kryptografie byly publikovány v roce 1976 Whitfieldem Diffiem a Martinem Helmanem. V roce 1977 publikovali Ron Rivest, Adi Shamir a Leonard Adleman koncept faktorizačního systém RSA [7], který se rychle světově rozšířil a v současnosti se stále používá pro šifrování a elektronický podpis. Praktické využití asymetrické kryptografie lze nalézt například u platebních karet vybavených čipem, digitálních certifikátů a zaručeného elektronického podpisu.

Algoritmus RSA je založen na faktorizačním problému. Problém spočívá v obtížném rozkladu čísla vzniklého jako součin dvou vysokých prvočísel. Například z prvočísel $p=13;\ q=17$ je výpočetně triviální získat součin $\boldsymbol{n = p \times q}$, protože se jedná o prosté násobení $n = 13 \times 17 = 221$.

Problém faktorizace spočívá v obtížnosti výpočtu hodnot p,q při pouhé znalosti jejich součinu n. Tento problém je výpočetně obtížný právě pro prvočísla a to díky jejich nesoudělnosti. Při generování veřejného a tajného klíče je použit tzv. modulus, což je číslo n, vzniklé jako součin prvočísel p,q. Prvočísla jsou tedy hlavními prvky při generování klíčového páru. Veřejný klíč je zvolen náhodně a tajný klíč je vypočítán z klíče veřejného. K tomuto výpočtu je zapotřebí znalost prvočísel p,q. K šifrování je pak použit veřejný klíč spolu s modulusem n. Zpráva zašifrovaná veřejným klíčem příjemce je dešifrovatelná pouze tajným klíčem příjemce. Samotný princip šifrování spočívá v umocnění číselné hodnoty znaků zprávy na hodnotu veřejného klíče. Kryptogram je tvořen celočíselným zbytkem výsledku tohoto umocnění, poděleným modulusem n. Protože se jedná o celočíselný zbytek po dělení velmi vysoké mocniny, není z pouhého

výsledku možné zjistit hodnotu zprávy coby základ mocniny. Dešifrování se děje umocněním kryptogramu na hodnotu tajného klíče a vypočítáním celočíselného zbytku po dělení modulusem *n*. Tento zbytek po dělení (výsledek operace nazývané *modulo*) je roven původní zprávě. V současnosti akceptovaná délka klíče pro algoritmus RSA činí 2048 bitů.

4.6. Elektronický podpis

Elektronický podpis je takový šifrovací postup, který umožní jednoznačně a nepopiratelně prokázat identitu autora odesílané zprávy. Smyslem elektronického podpisu není utajit obsah zprávy, ale zajistit průkaznost jejího autorství. Vzhledem k odlišnosti použití klíčů nelze zprávu podepsat a utajit během jediného zašifrování. Podepsanou zprávu však lze ještě zašifrovat.

Zpráva opatřená pouze elektronickým podpisem je pro útočníka normálně čitelná, přičemž hodnota podpisu zaručuje zjistitelnost jakýchkoliv změn, kterých by se útočník ve zprávě dopustil. Elektronický podpis nevytváří pro útočníka překážku, která by mu bránila v modifikaci zprávy. Nebude ale schopen k modifikované zprávě vytvořit podpis odpovídající osobě odesílatele, schvalující obsah změněné zprávy. Proto příjemce při ověření elektronického podpisu zjistí absenci podpisu nebo rozpor mezi elektronickým podpisem a přiloženou zprávou, změněnou útočníkem během přenosu.

Mechanismus tvorby a ověření elektronického podpisu je založen na použití klíčového páru pro asymetrickou kryptografii. Pomocí jedinečnosti tajného klíče vyjadřuje odesílatel svoji vůli s podepisovanou zprávou. K ověření podpisu je zapotřebí veřejný klíč podepisující osoby, který může být volně publikován. Jeho zveřejnění nemá vliv na bezpečnost podpisu. Zprávu podepsanou odesílatelem může ověřit libovolné množství příjemců, kteří k tomu vždy použijí veřejný klíč odesílatele.

Použití asymetrické kryptografie k podepisování zpráv přináší i určitá úskalí. Hlavní nevýhodu v současné době nejrozšířenějšího podepisovacího schématu pomocí algoritmu RSA představuje jeho vysoká výpočetní náročnost. Při šifrování je datová podoba zprávy umocňována na hodnotu veřejného klíče o velikosti vyšší než 21024 a podepisování dlouhých zpráv by bylo časově náročné. Přidáním hašovací funkce do

podpisového schématu před asymetrické šifrování lze docílit toho, že zpráva libovolné délky bude podepsána vždy stejně rychle. Hašovací funkce totiž využívá ke zpracování celé zprávy do podoby haše až tisíckrát rychlejších algoritmů. Namísto podepisování celé zprávy se tak v praxi podepisuje pouze otisk zprávy, tedy haš. Elektronický podpis je tedy ve své podstatě pouze tajným klíčem zašifrovaný haš, přenášený spolu se zprávou. Haš jednoznačně reprezentuje podobu zprávy v okamžiku podepsání a je chráněn proti pozměnění tajným klíčem odesílatele.

Příjemce při ověřování elektronického podpisu dešifruje veřejným klíčem odesílatele podobu haše, který reprezentoval zprávu v okamžiku podepsání. Z přijaté zprávy je poté na straně příjemce vytvořen další haš. Pokud jsou dešifrovaný a nově vytvořený haš shodné, pocházejí z datově identické zprávy. Funkčnost veřejného klíče prokázala souvislost s tajným klíčem odesílatele. Tím je prokázán odesílatel. Rovností obou otisků je naopak prokázáno, že zpráva nebyla během přenosu modifikována.

4.7. Hašovací funkce

Vzhledem k výpočetní náročnosti faktorizačního systému RSA jako nejrozšířenějšího asymetrického systému bylo zapotřebí vyřešit, aby podepisování jakkoliv dlouhé zprávy trvalo vždy stejně dlouhou dobu a nebylo závislé na délce zprávy. **Hašovací funkce** vznikly za účelem vytvoření reprezentativního krátkého digitálního otisku zprávy, který je pro zprávu jedinečný a popisuje její obsah pomocí krátké bitové sekvence o pevně stanovené délce. Tento otisk se nazývá haš, v anglickém jazyce pak **hash** nebo message digest.

Hašovací funkcí se nazývá takový matematický postup, který dokáže z libovolně dlouhé zprávy vypočítat jednoznačný otisk o pevné délce v řádu několika stovek bitů. Výsledná podoba haše je přímo závislá na všech bitech této vstupní zprávy.

Hašovací funkce jsou jednocestné. **Jednocestnost** znamená, že výpočet haše ze zprávy je výpočetně mnohem jednodušší, než zpětná rekonstrukce zprávy z pouhé znalosti haše. Jednocestnost je dána výrazným rozdílem ve velikosti haše a možné velikosti zprávy. Například maximální velikost zprávy pro SHA-256 je až 2256 bitů a velikost produkovaného haše je 256 bitů. Z tohoto pohledu se hašovací funkce chová jako ztrátová komprese,

což je jeden z hlavních důvodů nemožnosti rekonstruovat původní zprávu ze znalosti jejího otisku.

Vypočítaná hodnota haše zprávy pomocí stejného algoritmu produkuje vždy shodný výsledný otisk. Naopak pokud by se zprávy lišily byť v jednom jediném bitu, hašovací funkce musí produkovat výsledné haše odlišné ve více než polovině hodnot bitů haše.

Vliv na výslednou hodnotu má hodnota i pozice každého bitu. Významnou změnu v haši tedy vyvolá i vzájemná záměna pouhých dvou bitů. Tomuto jevu se říká lavinovitost.

Díky hašovacím funkcím je možné například ověřit shodnost či rozdílnost dvou velmi objemných souborů. Stačí vypočítat hodnoty jejich hašů a tyto krátké otisky vzájemně porovnat. Jestliže jsou haše shodné, pak platí, že jsou shodné i vstupní zprávy, z kterých byly haše vypočítány.

Algoritmus hašovací funkce nemusí být utajen. Detailní znalost jeho fungování by neměla útočníkovi usnadnit nalezení jiné zprávy se stejným otiskem. Odolnost proti nalezení rozdílné zprávy s identickým otiskem se nazývá **bezkoliznost**.

4.8. Praktická využitelnost kryptografie

Kryptografické techniky nejsou a nemohou být univerzálním řešením veškerých hrozeb, kterým je informace během jejího zpracování, ukládání a přenosu vystavena. Kryptografie poskytuje ochranu před útočníkem, ale nedokáže například eliminovat personální rizika spojená s osobní loajalitou. V místech, kde se informace vyskytují v otevřené podobě, mohou být pozměněny nebo odcizeny osobami, které k nim mají přístup plynoucí z povahy jejich povolání. V prostředí informačních systémů představuje takové riziko i technický personál. Kryptografie chrání přenášené informace proti komukoliv, kdo k nim má přístup na celé trase přenosu. Ochranu uvnitř organizace však musí pokrývat personální bezpečnost.

Příkladem pronikání kryptografie do každodenního používání v běžném životě koncových uživatelů je téměř dnes již téměř stoprocentní použití přístupových klíčů pro přístup k bezdrátovému připojení WiFi. Prakticky každá privátní bezdrátová síť je chráněna nutností znalosti symetrického

klíče pro bezpečnostní protokol WPA 2. Ten využívá blokový šifrovací algoritmus AES, s délkou klíče až 256 bitů. Hlavním motivem použití je řízení přístupu k přenosovému prostředí, opomíjeným přínosem je ale také zabezpečená komunikace mezi přenosnými zařízeními a přístupovým bodem.

Velký potenciál v ochraně před kybernetickými útoky představuje širší používání zaručeného elektronického podpisu. I přes třináctiletou existenci právní opory elektronického podpisu [10] v českém právním řádu jde o velmi málo využívaný kryptografický nástroj. Jeho praktická použitelnost nespočívá jen v nahrazení klasického podepisování dokumentů. Elektronický podpis je využitelný k autentizaci uživatelů v informačních systémech, k řízení přístupu a k zajištění dostupnosti informačních systémů a přenosového prostředí.

Plné využití potenciálu elektronického podpisu může nejen výrazně omezit riziko kybernetických útoků na IS provozované státní správou, ale může přinést i zefektivnění a zrychlení komunikace při zajištění její autentičnosti a nepopíratelnosti. Průkaznost elektronického podpisu by urychlila nejen komunikaci fyzických a právnických osob vůči orgánům veřejné moci a státní správě, ale i mezi nimi samotnými. Přechod na zaručenou a průkaznou formu komunikace by znamenal zvýšení odolnosti proti možným útokům na podvržení identity.

Využití elektronického podpisu k zvýšení bezpečnosti před kybernetickými útoky nabízí Informační systém datových schránek [3,11]. Systém umožňuje vzájemnou komunikaci mezi orgány veřejné moci, právnickými osobami, podnikajícími fyzickými osobami a nepodnikajícími fyzickými osobami. Pomocí kvalifikovaného certifikátu lze zaručenou formou komunikovat mezi libovolnými subjekty. Z původního nástroje pro doručování doporučené korespondence od orgánů veřejné moci se díky dative zprávě může stat nástroj pro zaručenou komunikaci. Systém přiřazení uživatelských účtů a jejich identifikace vylučuje například hromadné zasílání nevyžádané pošty (spam). Pomocí komerčního certifikátu na kryptografickém tokenu lze zvolit formu šifrovaného přihlášení a použít tak vícefaktorovou autentizaci. Zcizení hesla se tím pro útočníka významně komplikuje.

Samotná práce s kryptografickými nástroji není nikterak uživatelsky náročná, což dokazuje masová rozšířenost a samozřejmost používání platebních karet s elektronickým čipem. Tyto ve skutečnosti představují hardwarový mechanismus pro podepisování finančních transakcí nakupujícího. Důvod nízké míry využívání elektronického podpisu lze spatřovat v malé informovanosti potenciálních uživatelů.

Smyslem této kapitoly bylo nastínit princip fungování kryptografie a některé zásadní vlastnosti kryptografických algoritmů. Role kryptografie v kontextu kybernetické bezpečnosti spočívá v možnosti výrazného omezení kyberkriminality pomocí zvýšení kybernetické odolnosti národní kritické infrastruktury. Aplikací certifikovaných kryptografických prostředků lze dosáhnout zvýšené ochrany nejen v oblasti utajovaných informací. Použití kryptografie v případě otevřených systémů se neobjede bez širší informovanosti a zapojení koncových uživatelů v praktickém používání kryptografických nástrojů.

Literatura

[1] Cryptographic key length recomandation. [online] [cit. 2013-06-01]. Dostupné z WWW: http://www.keylength.com/en/

[2] GEERS, K.: Strategic cyber security. NATO Cooperative Cyber Defence Centre of Excellence, 2011, ISBN:978-9949-9040-5-1.

[3] Informační systém datových schránek. [online] [cit. 2013-06-01]. Dostupné z WWW: http://www.datoveschranky.info/

[4] JOHNSON, F. N.; JAJODIA, S. : Steganalysis of images created using current steganography software. Proc. of the Second International Workshop on Information Hiding, vol. 1525 , str. 273-273, 1998.

[5] FIPS PUB 46-3 National Institute of Standards and Technology. Data Encryption Standard, 1999.

[6] NEMATI, H. R.;YANG, L.: Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering IGI Global, 2010, ISBN:978-1-61520-783-1.

[7] R. Rivest, A. Shamir, L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, Vol. 21 (2), str. 120–126. 1978.

[8] SHANON, C.: Communication Theory of Secrecy Systems. Communication Theory of Secrecy Systems, Bell Systems Technical Journal, Vol. 28, str. 656-715, 1948.

[9] SINGH, S. : The Code Book - The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography. Doubleday, 1999, ISBN:0-385-49531-5.

[10] Zákon č. 227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů. In: Sbírka zákonů. 29. 6. 2000.

[11] Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. In: Sbírka zákonů. 17. 6. 2008.

5. Bezpečnost mobilních zařízení

Život si již bez různých technických vymožeností neumíme představit. Velkého rozmachu v posledních letech zaznamenala především oblast IT technologií. Techniku spojenou s výpočetními technologiemi požíváme ve všech možných činnostech, při vzdělávání, v profesním životě při výkonu zaměstnání i ve volném čase pro zábavu. Trh je saturován nejen počítači a další s nimi spojenými zařízeními pro profesionální používání, ale značná část výrobků je zacílena na běžnou populaci. Rádi si usnadňujeme život nejen vzájemnou komunikací v libovolném místě, získávání různých informací a dokonce i využíváme možností realizovat hry se spoluhráči ze vzdáleného místa. Výrobci neustále nabízí nové modely chytrých telefonů, smartphonů, i-Padů, i-Phonů, ultrabooků, netbooků, tabletů, chytrých hodinek (i-Watch) nebo chytrých brýlí. Všechna tato mobilní zařízení osvobozují uživatele od nutnosti pevného připojení do komunikační struktury a dávají mu možnost jejich použití ve volném prostoru.

Tato výhoda včetně bohatého programového vybavení však také skrývá určité nevýhody. Jde především o rozšíření prostoru pro hackery a kyber zločince všeho druhu. Používání velkého množství přístrojů před různými útoky nechráněných, mnohdy nemožnost uživatele ovlivnit software včetně volného přenosového prostředí těmto podnikavcům mimo zákon usnadňuje aktivity. Svou roli tu hraje i obchodní politika výrobců a prodejců těchto zařízení.

Většina uživatelů si vůbec neuvědomuje skutečnosti, že jejich zařízení a také osobní data mohou být velmi lehce ukradena a zneužita. V současné době, kdy je možno realizovat i finanční transakce pomocí některých mobilních zařízení bez nutnosti potvrzení, jsou v možném ohrožení i konta či jejich části.

Lehkost zneužití potvrzují zveřejňovaná fakta. Bylo například uvedeno, že více než 55% Britů se již stalo obětí počítačově trestné činnosti. Tato skutečnost určitě souvisí i se zjištěním, že až 40% ztracených mobilních telefonů ve Velké Británii nemělo ochranu před neoprávněným přístupem k datům. Lze s velkou pravděpodobností předpokládat, že čeští uživatelé mobilních zařízení se chovají podobným bezstarostným způsobem k ochraně svých osobních dat jako ti ve Velké Británii.

Hackeři se soustřeďují na krádeže dat, při nichž získají pravé jméno uživatele a informace o účtu.[2, s. 24] Takové informace jim již otevřou dveře k možnostem manipulace s účtem. Následující tabulka ukazuje procentní vyjádření ukradených osobních dat.

Tabulka 6 - Ukradená data (Zdroj: Zpracováno podle CHIP 04/2013, s. 24)

Jméno uživatele	55 %
Údaje o účtu	40 %
Číslo průkazu totožnosti	33 %
Adresa	26 %
Finanční informace	13 %

Časopis Check Point 2013 Security Report ve své výroční zprávě z ledna 2013 uvádí, že v průměru každých 23 minut je každá organizace vystavena přímému útoku na své webovské stránky. Výzkum hovoří až o 75% organizacích napadených malwarem. Výše zmíněný titul na svých stránkách uvádí, že nejvíce malware se nachází v USA (71 %), v Kanadě, v Evropě pak ve Velké Británii a SRN. O naší republice, stejně jako o Slovensku a Francii se uvádí hodnota 2 %.[1]

Kybernetická zločinnost dosáhla vyšší, „robotické" úrovně. Ta se projevuje především v programech vytvářejících spaming ,automatické rozšiřování různých virů, distribucí škodlivého software, loupením a kradením dat a také rozličnými útoky na servery a počítače, včetně celé plejády mobilních zařízení.

Historie počítačové kriminality ukazuje zcela jasně, že hlavní pozornost zločinců je věnována nejrozšířenějším uživatelským zařízením, nejpoužívanějšímu software a nejpoužívanějšímu komunikačnímu prostředí.

Nejzranitelnější a nejvíce vystavené hrozbám se podle Check Point 2013 Security Report ukazují produkty firem Oracle, Apple, Microsoft, Firefox a další. Nejde o produkty nechráněné nebo chráněné nedostatečně, ale o software nejvíce v dnešním globálním světě používanější.

Na základě těchto a dalších poznatků můžeme zcela oprávněně usoudit, že pozornost zločinců ve světě IT se upře na mobilní zařízení a software

v nich používaných. A to zvláště za situace, kdy jejich uživatelé věnují malou, či žádnou pozornost ochraně před napadením viry nebo zneužitím dat.

5.1. Internet a bezpečnost

Jednou z nejvíce využívaných služeb, a to i při používání mobilních zařízení, je e-mail. Víme, kdo všechno čte naše e-maily?

Silný zájem o chování svých občanů na internetu není fenoménem odehrávajícím se pouze v Americe. I v Evropě státy monitorují, co jejich občané na internetu dělají. Není asi žádným tajemstvím, že vládní orgány a tajné služby mají přímý přístup k toku dat poskytovatelů internetových služeb (ISP) – u nás největší aktivity v tomto směru patrně vyvíjí BIS.

Je internet, tak jak ho známe dnes, skutečně v ohrožení? Zatímco vládní kontrola webu v USA či v Evropě je realizována prostřednictvím chytrých investic a národních zákonů, vlády v Rusku, Číně a Íránu i dalších zemí chtějí jít ještě o krok dál. Chtějí, aby celý internet přešel pod vládní dohled – a to celosvětově. „Počet vlád, které požadují cenzuru internetu, se od roku 2002 zvýšil ze čtyř na čtyřicet. A toto číslo se neustále zvyšuje," napsal Vint Cerf, jeden z otců internetu, v květnu 2012 v New York Times.

Státy, které mají zájem o kontrolu nad internetem, se snaží, aby vláda nad internetem přešla z neziskového Internetového sdružení pro přidělování jmen a čísel (ICANN) směrem k Mezinárodní telekomunikační unii (ITU), což je organizace oficiálně spadající pod OSN, ve které ale mají v praxi hlavní slovo pouze vládní představitelé. Pokud by tato snaha vyšla, přešlo by řízení základních prvků síťové infrastruktury, jako je DNS (Domain Name System), rozdělení domén nejvyšší úrovně a IP adres pod přímou kontrolu vlád států. Ty by mohly nejen v budoucnu rozhodovat, jak má web fungovat, ale také by nepřímo kontrolovaly poskytovatele a síťové uzly nebo vědecké sítě.

Také se snaží prosadit i lobbistické skupiny evropských provozovatelů sítí, které například usilují o to, přimět poskytovatele služeb typu Skype nebo YouTube platit poskytovateli připojení za přístup k jejich obsahu. Je ale jasné, že tyto poplatky budou muset být ve finále hrazeny uživatelem.

V prosinci roku 2012 proběhla v Dubaji konference WCIT-12, na které se hlasovalo o tom, jakým směrem se internet bude vyvíjet dále. Některé návrhy nových předpisů, o kterých se na konferenci rozhodovalo, se jeví jako jasná cenzura obsahu. Naštěstí konference skončila podivnou remízou. Je ale jen otázkou času, než si jednotlivé státy a organizace vynutí nad svobodným internetem mnohem větší vliv. [4, s. 36.]

Řízení či kontrolu nad provozováním internetu jako uživatelé těžko ovlivníme. Zde jsme zcela v rukou vlády a nadnárodních organizací. Máme však možnost, dokonce přímo povinnost, použít všechny znalosti a dostupné prostředky, k ochraně osobních dat a také financí.

5.2. Mobilní zařízení a bezpečnost finančních služeb

Na první pohled bezpečné internetové bankovnictví se nedávno stalo cílem nebezpečného útoku, který hackerům vynesl obrovské sumy.

Kyberzločinci zaútočili na nejslabší článek. Tímto se ukázali uživatelé pracující s PC a mobilními zařízeními. Útočníci použili sofistikované technologie, aby zahájili a automatizovali své útoky a nemohli být sledováni.

Pomocí „Eurograbberu" bylo ukradeno 36 milionů eur prostřednictvím malwaru. Eurograbber útočil na majitele bankovních účtů pomocí sofistikované kombinace malwaru zaměřeného na osobní počítače i mobilní zařízení. Útočníci propojili malware se svým řídicím serverem a nejprve napadli počítač obětí. Poté infikovali jejich mobilní zařízení, aby mohli zachytit SMS zprávy a obejít tak dvojí bankovní identifikační proces. Díky ukradeným informacím a jednorázovým autorizačním kódům (TAN – Transaction Authentication Number) pak útočníci automaticky převáděli finance v hodnotě 500 až 250 000 eur z účtů obětí na podvodné účty po celé Evropě.

Byly odhaleny hlavní charakteristiky útoku:

- Dle odhadů bylo kradeno z více než 30 000 firemních a soukromých bankovních účtů.
- První útoky byly provedeny v Itálii, rychle se rozšířily do Německa, Holandska a Španělska.

- Krádeže byly provedeny pomocí sofistikovaného malwaru, který byl namířen na počítač a mobilní zařízení bankovních zákazníků.
- Útoky byly speciálně zaměřeny na mobilní zařízení Android a BlackBerry, což jen potvrzuje rostoucí trend útoků na zařízení s OS Android.

EUROGRABBER pracuje ve čtyřech krocích:

1. krok: Trojský kůň infikuje počítač uživatele. Eurograbber zachycuje komunikaci s bankou.
2. krok: Útočníci získají číslo mobilního telefonu uživatele a infikují mobilní zařízení.
3. krok: Banka zasílá uživateli přes SMS TAN (Transaction Authorization Number). Trojský kůň na mobilním telefonu uživatele SMS zachytí a předá ji útočníkům pro dokončení nezákonné transakce.
4. krok: Při příštím přihlášení uživatele k bankovnímu účtu zahájí útočníci převod finančních prostředků z účtu uživatele na účet „bílého koně".

Podrobnosti lze nalézt ve studii zveřejněné na webové stránce zmíněného časopisu. [2]

5.3. Možnosti útoků na mobilní zařízení

Bezpečnost citlivých údajů, kontaktních informací a informací o zařízení může ohrozit a vše zpřístupnit kyberzločincům madware neboli mobilní adware.

Madware se může do telefonu dostat zcela nenápadně při stahování aplikací a nejčastěji má podobu automaticky otevíraných oken, případně může přidávat ikonky, měnit nastavení prohlížeče nebo shromažďovat osobní údaje. Jedním ze zdrojů mobilního malwaru mohou být i hry.

Velký potenciál pro útočníky představuje malware, který nakupuje aplikace z appstoru bez vědomí uživatele. Mobilní červ zneužívající díry v systému k rozšíření na zranitelné telefony představuje perfektní platformu pro malware, který takové aplikace kupuje. Jestliže není nutná interakce uživatele, nebude existovat nic, co by zamezilo mobilnímu červovi v utrácení peněz z platební karty majitele telefonu.

S pomocí jiného škodlivého softwaru - ransomwaru - mohou útočníci vytáhnout ze smartphonu rozličná citlivá data uživatele, manipulovat s nimi, komunikovat jeho jménem nebo používat systém k provádění různých operací v pozadí. Poté majitele účtu nutí zaplatit „výkupné", aby ve svých útocích nepokračovali. Vždyť mohou např. Vyhrožovat šířením nahraných hovorů a obrázků pořízených smartphonem.

Byl již detekován SMS spam botnet, který se zaměřuje na mobilní zařízení se systémem Android a rozesílá nevyžádané SMS zprávy. Zatímco klasické botnety, zaměřené na rozesílání spamu, nepřinášejí nic nového, mobilní technologie otevírají kyberzločincům nové možnosti. Trojský kůň s názvem Android.Pikspam se šíří prostřednictvím SMS zpráv, které propagují bezplatné verze populárních her, případně uživatele informují o nějaké výhře. Pokud nic netušící uživatel klikne na odkaz ve zprávě, stáhne si kromě hry i trojského koně, a zatímco sleduje instalaci hry, na pozadí se instaluje hrozba. Jakmile je trojský kůň Android. Pikspam aktivní, připojí se k řídicímu serveru a automaticky rozesílá nevyžádané SMS zprávy na telefonní čísla získaná z tohoto serveru. Uživatelé mobilních zařízení musí být ostražití nejenom před madwarem. Stále častěji se objevuje i mobilní malware, který napodobuje starší počítačové hrozby a snaží se ukrást informace o zařízení. Nový malware často jen kopíruje a vylepšuje starší varianty škodlivého kódu. Čím více se lidé zajímají o mobilní technologie, tím více se o ně zajímají i kyberzločinci.

Výzkumníci z univerzity v Severní Karolíně v USA objevili novou metodu SMS phishingu. Zranitelnost umožňuje spuštění nedůvěryhodné aplikace na telefonu, která vytvoří falešnou příchozí textovou zprávu SMS s libovolným obsahem – týká se to jak textu samotné zprávy, tak i odesílatele, kterým může být telefonní číslo ze seznamu kontaktů nebo jednoduše z vaší důvěryhodné banky. Zvláště znepokojující je skutečnost, že zranitelnost nepotřebuje ke své činnost žádné zvýšené oprávnění.

Stále více se ukazuje, že i velké softwarové firmy nevěnují patřičnou pozornost svým produktům z hlediska bezpečnosti. Například, v přehrávači Adobe Flash Player bylo nalezeno sedm zranitelností, které mohou hackerovi umožnit přístup do postižených systémů. Chybu lze označit za zvlášť závažnou i proto, že se vyskytuje ve všech verzích Flash Playeru – najdete ji nejen na počítačích se systémem Windows, ale i na

počítačích s Mac OS či Linuxem a na smartphonech a tabletech s Androidem.

Další nepříjemností je, že chyba byla nalezena i v multiplatformním prostředí Adobe AIR. Chybu objevili zaměstnanci společnosti Google a nahlásili ji Adobe. Slabiny v softwaru mohou způsobit, že útočník získá úplnou kontrolu nad zařízením. Chyba také může zapříčinit zhroucení systému. Chyba v přehrávači Flash Player umožňuje hackerům přístup k PC, tabletům a mobilním telefonům a dalším mobilním zařízením.

Technologie postupuje stále kupředu. Komunikace zařízení-zařízení (Machine-to-Machine, M2M) představuje technologii, která umožňuje jednomu zařízení bezdrátově nebo pomocí klasických sítí komunikovat s dalším zařízením. Na trhu jsou již nyní k dispozici prostředky umožňující usnadňovat celou spoustu činností ve veřejných zařízeních a také i v domácnostech. Nejde pouze o tzv. chytré domy, kdy je možno zabezpečit ovládání různých spotřebičů z jednoho místa podle předem stanoveného programu. Může jít o ledničku, která komunikuje s domácím serverem, aby upozornil obyvatele domu, že je na čase koupit mléko a vajíčka; může jít o letištní skener, který pořídí fotografii obličeje osoby a porovná ji s databází známých teroristů; může jít o lékařské zařízení, které reguluje přívod kyslíku pacienta a upozorní lékařský personál, že tepová frekvence klesla pod určitou úroveň. Zatímco praktické technologické možnosti M2M jsou úžasné a mají v mnoha případech potenciál odstranit lidskou chybu, mnoho otazníků přetrvává ohledně jejich bezpečnosti.

Dalším technologickým pokrokem, podporovaným bankovní sférou je platba omezených peněžních částek pomocí mobilních zařízení. Vyvinutá technologie NFC usnadňuje a urychluje placení v obchodech, hotelích, benzinových stanicích i jinde. Tato technologie je dalším zdrojem útoků hackerů a tím také zvýšené pozornosti uživatelů jak chránit své „digitální peněženky". Mobilní červy zaměřené speciálně na oblast NFC, se budou šířit a krást peníze především v oblastech s vysokou hustotou populace, jako jsou letiště, obchodní centra, zábavní parky a podobně.

Hackeři jsou velmi vynalézaví. Zvládli činnosti proti PC. Se svými „produkty" se dostali i do prostředí mobilních zařízení a nyní uživatelé

mohou očekávat i současné napadání obou platforem. Předpokládá se, že botnety v mobilním prostředí mají mnoho stejných vlastností jako jejich starší sourozenci určení pro PC. Tento závěr nás opravňuje ke tvrzení, že se objeví nové formy útoků odepření služby DDoS současně napadající mobilní zařízení a PC.

Infikované mobilní zařízení a PC budou sdílet stejné ovládací a řídicí servery a protokol útoku a budou schopné zaútočit společně v jednom okamžiku. Díky tomu se možnosti botnetů znásobí. [5, s. 32]

Dnešní škodlivé kódy jsou vytvářeny pro mobilní zařízení stejně jako pro stolní počítače a notebooky. Dosud přitom byla hlavním cílem pozornosti útočníků právě platforma klasických počítačů, a to proto, že jich bylo tolik a že jsou na světě přece jen delší čas. Laboratoř FortiGuard Labs dnes eviduje a sleduje zhruba padesát tisíc vzorků škodlivých kódů pro mobilní zařízení (pro PC jsou jich řádově miliony). Výzkumníci přitom pozorují významný nárůst v objemu mobilních škodlivých kódů a předpokládají, že tento trend bude v příštím roce ještě dramatičtější, mimo jiné i kvůli tomu, že se dnes prodává více mobilních telefonů než notebooků nebo stolních PC. [5, s. 32]

5.4. Bezpečnost komunikačního prostředí

Nejen mobilní zařízení a jejich programové vybavení je v pozornosti kyberzločinců, ale nemenší zájem jeví i o komunikační prostředí. V dnešní době je v provozu velké množství sítí. Sítě provozované profesionálními poskytovateli služeb jsou chráněné na vysoké úrovni. Možnosti jejich napadení samozřejmě existují, ale software provozované síťových zařízeních je ošetřované vyspělými bezpečnostními bránami. Technologie však dospěla tak daleko, že na spotřebitelském trhu existuje celá řada zařízení, které umožňují i běžnému uživateli vytvořit pro svou potřebu bezdrátové komunikační prostředí. Takové komunikační sítě nacházíme v kancelářích, restauracích, kavárnách, hotelích, obchodních centrech a v dalších objektech, kde se soustřeďuje velké množství lidí. Ne všichni provozovatelé věnují patřičnou pozornost bezpečnosti. Zde se otevírá možnost kybernetickému podsvětí krást a zneužívat osobní data uživatelů těchto sítí. Bylo již zjištěno, že přes hardwarově nastavené heslo síťového

zařízení (např. síťové tiskárny) mohou útočníci získat kompletní práva pro čtení i zápis.

Ještě více volnosti pro případné zneužití skýtají domácí sítě používané nejen pro pohodlnější použití notebooku či netbooku pro práci. Tato zařízení, včetně tabletů a smartphonů se užívají v domácnostech i pro ovládání televizorů či jiných zařízení pro zábavu včetně řízení prostředků „chytrého domu". Většina uživatelů si tyto domácí sítě nechrání. Jsou přesvědčeni, že domácí sítě při malém dosahu jsou celkem bezpečné. Prostřednictvím hacknutí routeru však mohou útočníci monitorovat celý webový provoz. Pomocí zmanipulovaného e-mailu dokáží překonfigurovat router tak, že veškerý síťový provoz je směrován na server útočníka. Toto vše se děje bez jakýchkoli příznaků, a tudíž oběť nemá jakékoli tušení o napadení. Při skutečnosti, že uživatelé těchto sítí provádí v klidu domova celou řadu bankovních transakcí, nechávám na uvážení čtenáře, jaké důsledky nechráněná domácí síť může způsobit.

Jak se chránit?

Za prvé, mít vždy na paměti, že existují jedinci či skupiny lidí, kteří chtějí podvodnou činnost páchat a mají k tomu intelektuální a technické prostředky.

Za druhé, po uvedení zařízení do provozu ihned zrušit hardwarově nastavená hesla a nahradit je vlastními bezpečnými hesly.

Za třetí, hesla měnit a chránit před dalšími osobami.

Za čtvrté, činnost s důvěrnými osobními daty a bankovní operace provádět pouze v prověřeném a chráněném komunikačním prostředí.

Literatura

[1] Check Point 2013 Security Report. Check Point Software Technologies, Ltd., leden 2013.

[2] *CHIP 04/2013*. Magazín o informačních technologiích, ročník 23. ISSN 1210-0684.

[3] *A Case Study of Eurograbber:How 36 Million Euros was Stolen via Malware* [online]. Check Point Software Technologies, Ltd., prosinec 2012. Dostupné z: www.checkpoint.com/products/downloads/whitepapers/Eurograbber_White_Paper.pdf.

[4] CHIP 02/2013, Magazín informačních technologií, ročník 23, ISSN 1210-0684; MK ČR 5361.

[5] *CHIP 03/2013, Magazín informačních technologií, ročník 23*. Předpověď FortiGuard Labs: Šest trendů pro rok 2013. Praha: Burda Praha, 2013. ISSN 1210-0684; MK ČR 5361.

Závěr

Bezpečnost informací představuje poměrně rozsáhlý obor, který se stal nedílnou součástí studia v oblasti informačních systémů a s rostoucím objemem zpracovávaných dat stále více roste i jeho důležitost. Čím větší hodnotu informace mají, tím by se měla věnovat větší pozornost jejich zabezpečení. Důležitým aspektem kybernetické bezpečnosti je ochrana před krádeží identity. **Cílem bezpečnosti informací je chránit data a informace od velkého množství hrozeb tak, aby byla zajištěna jejich bezpečnost.**

Dnešní svět si bez moderních technologií nedokážeme ani představit. A právě komunikace mezi moderními technickými prostředky se odehrává v kyberprostoru. Obecně si kyberprostor můžete představit jako **virtuální svět vytvořený moderními technologickými prostředky, v němž se informace vytvářejí, zpracovávají, ukládají a šíří pomocí elektromagnetického vlnění**. V posledních letech dochází ke koncipování nových organizací, které se aktivně zabývají ochranou kybernetického prostoru.

O závislosti společnosti na kybernetickém prostoru může být zneužita v případě teroristického nebo kybernetického útoku. A právě v tomto prostoru je možné vést v budoucnu kybernetické války. **Kybernetickou válku** lze chápat také jako využití počítačů a informačních technologií k provádění aktů války na úrovni vlád a velkých organizací. Spouštěčem kybernetické války může být jednotlivec, organizace anebo jiná vláda. Je mnoho různých druhů kybernetické války, od specializovaných hackerských až k obecně zacíleným útokům na vyřazení určité služby nebo ochromení kritické infrastruktury napadeného státu. Nejvyšším stupněm kybernetické války je útok, který kompletně odstraní schopnost všech připojení k Internetu. Proto také ve vyspělých armádách vznikají vojenské jednotky specializující se na oblast kybernetických útoků a kybernetické obrany.

Budoucí možné kybernetické války jsou důvodem k vážnému znepokojení nás všech. Na rozdíl od tradiční války, která vyžaduje obrovské množství zdrojů, jako jsou zbraně, personál a vybavení, kybernetické války potřebují jen někoho, kdo má správné znalosti,

výpočetní techniku a chce způsobit zmatek. Nepřítel může být kdekoli, dokonce i vně vlastního národa. Silný útok může provést pouze několik hackerů za pomoci standardních počítačů.

Každý uživatel informačního systému ovlivňuje úroveň národní informační a komunikační infrastruktury proti kybernetickým hrozbám. Ač si to běžní uživatelé ani uvědomují, jejich role při boji s kybernetickými útoky a obecně v oblasti bezpečného provozu sítí a služeb je nezanedbatelná. To oni jsou pověstným lidským faktorem, který často rozhoduje o účinnosti kybernetických útoků. Ne nadarmo se říká, že koncový uživatel je klíčem k bezpečnosti.

Řízení rizik je součástí našeho každodenního života, kdy hrozby ovlivňující nás a naše blízké řídíme většinou intuitivně, ale někdy i záměrně s jasně definovaným cílem. Řízení rizik kybernetické bezpečnosti nemůže být intuitivní záležitostí, ale záměrnou, koncepční a cyklickou. Proces řízení rizik není věcí vybraných jedinců, ale všech zainteresovaných stran, které se pohybují v kybernetickém prostředí a mají zájem (odpovědnost) za velikost ztrát způsobených riziky. Řídit rizika kybernetické bezpečnosti proto také znamená **řídit správné věci správně a tedy i efektivně**.

Z **kryptografie** se postupně stává bezpečnostní nástroj, který je neodmyslitelnou součástí veškerých informačních a komunikačních systémů. **Šifrování** již není doménou pouze utajovaných informací a umožňuje zamezit útokům i v Internetu. Pomocí šifrování lze data nejen ochránit před jejich únikem, ale též odhalit jejich modifikaci útočníkem. Pro rozšíření šifrování a jeho správné používání je zásadní překážkou pochopení jejího přesného účelu. Porozumění roli kryptografie a nemožnosti jejího nahrazení jinými metodami a postupy by pro čtenáře této publikace mělo kryptografii přesněji vymezit vůči bezpečnosti informačních a komunikačních systémů. Účelem stati o kryptografii bylo vybavit čtenáře základními znalostmi, díky kterým bude schopen identifikovat místa pro zasazení šifrování a posoudit vhodnost konkrétních již zasazených algoritmů. Zároveň je tento text východiskem pro podrobnější studium matematických principů, na kterých stojí jednotlivé algoritmy.

Používání **mobilních zařízení** je velmi rozšířené. Jejich hardwarové a softwarové vybavení dosáhlo a někdy i překročilo schopnosti běžných PC. Uživatelé je používají nejen pro zábavu, ale i pro řešení pracovních povinností. S tímto úzce souvisí i jednoduchá dostupnost bezdrátového komunikačního prostředí. Rostoucí počet uživatelů mobilních zařízení a jejich používání také k finančním operacím vzbuzuje velkou pozornost kyberzločinců. Jejich činnost jim umožňuje také malé uvědomění uživatelů o možnostech zneužití jejich osobních dat. Důsledným používáním bezpečnostních hesel a dalších bezpečnostních opatření mohou uživatelé zúžit prostor kyberzločincům a přispět k ochraně kyberprostoru.

A na závěr ještě jedno malé **zamyšlení. Kybernetický rok, měsíc, den, hodinu, minutu** zatím nikdo nespecifikoval a ani nezměřil. Říká se, že jeden lidský rok je zhruba 7 let psího života. Jak je to ale s tím kybernetickým časem? Jaká je jeho rychlost? Je rovna rychlosti světla? Podle toho, jak rychle se zdvojnásobují každé dva roky počty tranzistorů v čipech, tak je možné jeden rok lidského života přirovnat k jednomu kyberměsíci, kyberdnu či dokonce k jedné kyberhodině? Ale to nechám na vás čtenářích.

Seznam použitých zkratek

Zkratka	Vysvětlení
ACTA	Anti-Counterfeiting Trade Agreement
AČR	Armáda České republiky
BIS	Bezpečnostní informační služba
CCD COE	Cooperative Cyber Defence Centre o Excellence
CDMA	Cyber Defence Management Authority
CERT	Computer Emergency Response Team
CIRC	Computer Incident Response Capability
CMX	Crisis Management Exercise
CSIRT	Computer Security Incident Response Team
ČR	Česká republika
ČSN	Česká technická norma
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
ENISA	European Network and Information Security Agency - Evropské agentury pro bezpečnost sítí a informací
EU	Evropská unie
FBI	Federal Bureau of Investigation - Federální úřad pro vyšetřování
GPS	Global Positioning System
GSM	Groupe Spécial Mobile - Globální Systém pro Mobilní komunikaci
https	Hypertext Transfer Protocol Secure
ICANN	Internetové sdružení pro přidělování jmen a čísel
ISMS	Information Security Management Systém - Systém řízení bezpečnosti informací
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
ITU	Mezinárodní telekomunikační unie
IT	Informační technologie

Zkratka	Vysvětlení
MO	Ministerstvo obrany
M2M	Machine-to-Machine
NATO	North Atlantic Treaty Organization - Severoatlantická aliance
NBÚ	Národní bezpečnostní úřad
PDCA	Plan-Do-Check-Act
PDF	Portable Document Format
PoC	Point of Contact
SCADA	Supervisory Control and Data Acquisition
USA	United States of America - Spojené státy americké
TAN	transaction authentication number

Rejstřík

Představení autorů kapitol

Ing. Petr HRŮZA, Ph.D. (*1969)

Vysokoškolské vzdělání dosáhl v roce 1995 na Vojenské akademii v Brně. Disertační práci obhájil v roce 2005. Za dobu působení na Vojenské akademii v Brně a Univerzitě obrany zastával řadu pedagogických i akademických funkcí. Ve své vědecko-výzkumné, publikační a pedagogické činnosti se zabývá problematikou managementu, bezpečností informačních systémů, kybernetickou bezpečností, ochranou kritické infrastruktury, geografickými informačními systémy, informační podporou velení a řízení. Publikuje na vědeckých konferencích jak v tuzemsku, tak i v zahraničí.

Ing. Jaromír PITAŠ, Ph.D. (*1964)

Vysokoškolské vzdělání dosáhl v roce 1987 na Vysoké vojenské škole pozemního vojska ve Vyškově. Disertační práci obhájil v roce 2008. Působil na velitelských funkcích do roku 1994, kdy přešel zpět na Vysokou vojenskou školu pozemního vojska ve Vyškově. Od roku 2004 pracuje na Univerzitě obrany, kde zastával řadu pedagogických i akademických funkcí. Ve své vědecko-výzkumné, publikační a pedagogické činnosti se zabývá problematikou managementu, projektového managementu, použitím zbraňových systémů bojových vozidel. Publikuje jak v tuzemsku, tak i v zahraničí.

doc. Ing. Bohumil BRECHTA, CSc. (*1948)

Je absolventem Vojenské akademie v Brně z roku 1971. Disertační práci obhájil v roce 1981. Od roku 1979 působil na Vojenské akademii v Brně v různých pedagogických a akademických funkcích v oboru automatizace velení. V roce 1989 habilitoval. Byl členem týmů řešících úkoly automatizace velení vojskům v armádě České republiky. V letech 1995 – 2003 pracoval v nadnárodní společnosti jako specialista pro bezpečnost informací. Nyní se znovu věnuje pedagogické činnosti na Univerzitě obrany. Zabývá se teorií managementu ve vojenském prostředí a především otázkami bezpečnosti KIS.

Ing. Jaroslav ŠANDA (*1978)

Vysokoškolské vzdělání dosáhl v roce 2003 na Vojenské akademii v Brně. Od roku 2003 do současnosti se jako asistent Skupiny bezpečnosti informací věnuje výuce kryptografických technik a administrativní bezpečnosti. Zabývá se problematikou ochrany utajovaných informací a kryptografickou ochranou. Vyučuje ve specializačních kurzech pro obsluhy certifikovaných kryptografických prostředků. V posledních letech se zaměřuje na bezpečnostní aspekty propojování e-governmentu se spisovou službou, elektronickým podpisem a digitálními archivy.

Název:	Kybernetická bezpečnost II
Autoři:	Petr HRŮZA, Jaromír PITAŠ, Bohumil BRECHTA, Jaroslav ŠANDA
Vydavatel:	Univerzita obrany, Brno
Tisk:	MONIKA Promotion s.r.o., Praha
Náklad:	100 ks
Počet stran:	100
Rok vydání:	2013
Vydání:	první
Cena pro vnitřní potřebu:	200 Kč

Publikace neprošla jazykovou úpravou.

ISBN 978-80-7231-931-2