Vážení přátelé,

S cílem dát co největšímu počtu uživatelů počítačů do ruky co nejsilnější „zbraň“ v podobě vědomostí a znalostí pořádala AEC ve spolupráci s vydavatelstvím a nakladatelstvím VOGEL Publishing již pátý ročník konference zaměřené na ochranu a bezpečnost dat stejně jako na antivirovou problematiku. Oproti uplynulým ročníkům této akce, které nesly název "Virus", bula letošní akce pojmenovaná Security 2000.

Konference proběhla ve dnech 1. a 2. června 2000 v Praze. První den bylo důkladně probráno, k jakému vývoji došlo ve „světě virů“ a jakými prostředky mohou uživatelé počítačů (což je dnes už téměř každý) disponovat na svou obranu. Přednášli, jako se stalo zvykem, přední specialisté z oboru. Na konci prvního dne byl každý účastník konference teoreticky i prakticky (součástí je CD s antiviry) „vyzbrojen do dalšího boje“ s tímto již trvalým ohrožením bezpečnosti počítačových dat.

Druhý den konference byl věnován problematice ochrany dat na bázi moderní kryptografie (tedy šifrování) a dalším bezpečnostním prvkům. Dnes již nejsme na pochybách, že je to téma pro široký okruh lidí, zodpovědných za provoz počítačové techniky. Podobně jako v případě předchozích konferencí šlo o to nabídnout účastníkům konference srozumitelnou formou ucelený obraz jednak o všech hrozbách, kterým je třeba čelit na počítačích, v sítích a při komunikaci, a jednak o možnostech a prostředcích moderní kryptografie, založené na PKI (Public Key Infrastructure), která tato nebezpečí zcela eliminuje.

Celkový a podrobnější přehled o přednášené problematice, naleznete na následujících stránkách, kde je k dispozici sborník přednášek z této konference.

AEC, spol. s r.o., Bayerova 30, 602 00 Brno
tel.: 05 / 4123 5466-7, fax: 05 / 4123 5038
www.aec.cz, www.trustcert.cz

AEC
DATA SECURITY COMPANY

AEC
DATA SECURITY COMPANY

&

VOGEL

pořádají konferenci

Vydala **AEC** při příležitosti konference SECURITY 2000
květen 2000

Všechna jména produktů, zmiňovaná v tomto dokumentu, jsou obchodní značky nebo registrované obchodní značky svých vlastníků. Společnost AEC, spol s r.o. nemá žádné vlastnické zájmy na těchto značkách a jménech. Ačkoliv společnost AEC, spol. s r.o. vynaložila veškeré úsilí k zajištění přesnosti informací uvedených v tomto dokumentu, není zodpovědná za jakékoliv chyby nebo opomenutí faktů zde uvedených. Společnost AEC, spol s r.o. si rezervuje právo modifikovat specifikace citované v tomto dokumentu bez předchozího upozornění.

Žádná část tohoto dokumentu nesmí být reprodukována ani přenášena v jakékoliv formě nebo jakýmikoliv prostředky, elektronickými nebo mechanickými, za jakýmkoliv účelem, bez předchozího výslovného písemného povolení autorů jednotlivých příspěvků.

Pozn.: Tato publikace neprošla redakční ani jazykovou úpravou.

Obsah

OBRAZ VIROVÉ PROBLEMATIKY V ROCE 2000

Pavel Baudiš
ALWIL Software, Průběžná 76, 100 00 Praha 10
e-mail: baudis@asw.cz, www: http://www.asw.cz

Anotace: Příspěvek se zabývá událostmi, které se odehrály na virové scéně (nejen) v období posledních dvou let. Kromě konkrétních příkladů se zabývá i příčinami současného stavu a možnými způsoby řešení.

Motto: - Jsem zvědav, kdy se vrátí normální situace.

- Ale tohle je normální situace!

e-mailový rozhovor dvou antivirových odborníků ze dne 7.5.2000, 2:30 GMT

Viry obecně

Definice počítačového viru není a nikdy nebyla jednoduchou záležitostí. Různých, často i protichůdných názorů existuje celá řada, přesto se na jedné základní věci všichni shodnou: viry se od jakéhokoli ostatního programu liší v tom, že se množí, a jsou tedy schopny se šířit z jednoho programu do druhého, z jednoho počítače na druhý.

Proč o tom vůbec hovořím? Viry jsou programy, a jako takové je nutno je pro jejich aktivaci spustit. Bez aktivace se jedná pouze o mrtvá data. Právě z této základní vlastnosti jsou odvozeny všechny typy a dokonce i vlastnosti počítačových virů.

Kdysi dávno (to je asi před dvanácti lety) byla situace jednoduchá: existovaly pouze dva základní typy virů: boot viry, které napadají zaváděcí sektory disků a souborové viry, které napadají klasické programy, uložené v souborech. Situace se ale rychle stala mnohem složitější: přišly multipartitní viry (tj. kombinace obou uvedených technik), spolu s Windows se objevily viry pro prostředí Win, Win32, Win95, WinNT, dále makroviry a v poslední době i skriptové viry. V menší míře se objevily viry, které napadají dokonce dávky, či které pracují pod dalšími operačními systémy (OS/2, Linux). Ukázalo se, že prostředí není až tak podstatné – jde pouze o to, že virus pro své úspěšné šíření musí mít šanci být spuštěn!

Vždy, když se objevil nový typ viru, však docházelo k tomu, že se nejprve objevily ty nejjednodušší viry, které pouze dokazovaly, že na dané platformě je možno virus vytvořit, řada jejich následníků již byla složitějších, pak se objevily polymorfní, multipartitní viry. Vývoj se zkrátka neustále pohybuje po jakési spirále… Na virovou situaci má však samozřejmě vliv i řada dalších faktorů: vývoj operačních systémů, aplikací a hlavně Internet.

Tak se po klasických souborových virech objevily v roce 1995 viry, které byly založeny na jiném principu. Šlo o makroviry, vytvořené ve WordBasicu (později ve VBA, Visual Basic for Applications) a šířící se mimo jiné i ve zdrojovém tvaru. VBA časem získával stále větší podporu a začal se objevovat i v dalších aplikacích, podporu získal dokonce i v samotném operačním systému (Windows Scripting Host).

Kromě virů se v poslední době stále častěji setkáváme i s dalšími škodlivými programy: wormy, trojany, backdoory. Wormy jsou podmnožinou virů, liší se od nich tím, že pro své šíření nevyžadují

hostitelský program a naopak vždy využívají síťové prostředky. Trojské koně jsou programy, které (podobně jako známý výrobek Řeků před starověkou Trójou) vykonávají skrytou škodlivou činnost, o které uživatel nemá ani tušení. Na rozdíl od virů se samy nemnoží, přesto s dalším rozvojem Internetu nabývá jejich nebezpečí na významu. Backdoory jsou vlastně speciálním druhem trojského koně, který nechává v napadeném systému „otevřená zadní vrátka„ pro útočníka, který tak získává nad daným počítačem úplnou kontrolu. To pak umožňuje například získat citlivá data či zneužít počítač oběti k případným útokům typu DDoS (distributed denial of service) na další počítače, jako tomu bylo v únoru tohoto roku.

Všechny tyto programy můžeme shrnout do kategorie „malware„ (malicious software – škodící programy). Jestliže však na definici virů existuje řada různých názorů, pak na dostatečně obecné a použitelné definici malware se odborníci nedokáží shodnout vůbec. A není divu – neexistuje zde totiž žádné objektivní kritérium (jako u virů), podle kterého by bylo možno jednoznačně rozhodnout o charakteru programu. Co pro jednoho uživatele může být trojanem, může být pro jiného neškodným žertíkem, jindy zase může jít o docela užitečnou utilitu. Objevily se i docela vážně míněné názory, že pokud se jedná o komerčně distribuovaný a dokumentovaný produkt, tak nemůže jít o malware (takže antivirové programy by měly detekovat přítomnost dokumentace?). Jednoznačná definice ale nikdy existovat nemůže.

Vraťme se ale od malware zpět k virům. Za poslední roky se změnila opravdu řada věcí. Klasické boot viry jsou dnes na vymření, hlavním distribučním kanálem již není disketa ale elektronická pošta. Proto se dnes nejúspěšněji šíří právě viry, které jsou schopny tohoto způsobu šíření dokonale využít.

Elektronická pošta má z hlediska virů spoustu výhod: vysokou rychlost šíření, provázanost aplikací a z toho plynoucí jednoduše dosažitelný přístup k dalším zdrojům na infikovaném počítači, seznam dalších případných obětí, možnost jednoduše „přeposlat„ sama sebe dalším a podobně. Nevýhodou a hlavním slabým místem z hlediska viru zůstává i nadále uživatel: ten musí virus na daném počítači spustit. Proto viry v poslední době využívají řadu psychologických triků, kterými se snaží uživatele k tomuto kroku přinutit.

Elektronickou poštou se posílají hlavně dokumenty, a proto častěji dochází k šíření makrovirů. Klasické viry nemají zdaleka tak vysokou šanci na úspěch, to už jsou na tom lépe wormy typu Ska (Happy99) či PrettyPark, maskující se za zábavné programy.

U klasických virů není jejich analýza či případná modifikace vůbec triviální. Zcela jiná je ale situace u makrovirů či skriptových virů. Zde se vlastně virus šíří ve zdrojovém kódu, což jednak usnadňuje jeho analýzu, jednak jeho další modifikaci. Proto jsme často svědky toho, že se objevuje řada variant takového viru, které se liší třeba jen změnou textů či manipulační činností.

Zvláštní „formu„ počítačových virů tvoří tzv. hoaxy, tedy poplašné zprávy o neexistujících virech. Ty mají většinou řadu shodných rysů: nepřesné udání času (včera, dnes), neurčitý odkaz na známou a velikou firmu (Microsoft, IBM), popisovaný virus „nelze detekovat„ a zejména žádost o zaslání zprávy dalším lidem, čímž vzniká klasický řetězový dopis. Zajímavé je i to, jak se projevy a ničivé účinky viru s časem proměňují a kolik lidí je schopno bez přemýšlení takový dopis poslat dál.

Ani antivirové firmy samozřejmě nezahálejí a drží krok se všemi novinkami, které se v poslední době objevily. Problémem zdaleka není nějaký konkrétní virus či nová metoda (tj. jeho analýza či detekce). Jedná se spíše o množství nových virů, které se každý měsíc objevují (nyní je jich tak kolem 500) a u několika konkrétních virů i o rychlou odezvu. I to se však dá celkem bez problémů zvládnout. Navíc ne všechny viry se objevují volně mezi uživateli. Seznam těch, které byly skutečně zjištěny, vytváří asi šedesát lidí z celého světa pod hlavičkou WildListu. V současné době je na tomto seznamu pouhých 203 virů, hlášených více než jedním pozorovatelem.

Antivirové firmy spolupracují i v dalších oblastech. Koncem dubna byl například uveden v činnost systém REVS (Rapid Exchange of Virus Samples), který umožňuje rychlou reakci na jakýkoli nový virus. Jde o zcela bezpečný systém, který je schopen přijímat a dále rozesílat vzorky nových virů, šifrované pomocí PGP. Pokud se tedy kdekoli na světě objeví nový virus, během několika vteřin jsou o něm uvědoměny další antivirové firmy, které též dostanou šifrovaný vzorek viru. První ostrý test systému REVS proběhl velmi brzy po zahájení jeho provozu v souvislosti s virem LoveLetter.

Modelové případy virů

Michelangelo

O tomto viru se zmíním jen krátce, protože k jeho masivnějšímu výskytu došlo již před osmi lety. Jde o klasický boot virus s velmi destruktivní manipulační činností: dne 6. března přepíše 256 stop na pevném disku.

komentář: Virus se objevil na podzim 1995 a i když byl poměrně dost rozšířen, uživatelé měli spoustu času se jej zbavit. Přesto média i některé antivirové firmy rozpoutaly doslova hysterii, ve které nechyběly katastrofické předpovědi způsobených škod. Ty zaznamenané přitom nebyly zdaleka tak veliké, i když občas velice nepříjemné.

Win32:Ska

Program známý i jako Happy99, si spíš zaslouží označení worm než virus. Šíří se jako připojený soubor prostřednictvím elektronické pošty. Připojený soubor se jmenuje Happy99.exe a je dlouhý přesně 10000 bytů. Po spuštění se na obrazovce objeví okno s docela zajímavým ohňostrojem, ale zatímco na obrazovce vybuchují rachejtle, virus modifikuje systémový soubor wsock32.dll, aby byl schopen monitorovat veškerou poštu odcházející z daného počítače. Přes tuto knihovnu prochází veškeré spojení počítače s Internetem. Virus pak připojuje kopii sebe sama pod originálním jménem Happy99.exe ke všem zprávám, které z daného počítače odcházejí.

komentář: Tento worm je schopen posílat sebe sama i do diskusních skupin Usenetu a je dlouhodobě nejrozšířenějším virem v této oblasti Internetu, když se v různých diskusních skupinách objevil více než 3000 krát.

Word97Macro/Melissa

Tento virus se objevil ze dne na den koncem března 1999. Je schopen rychle se šířit pomocí elektronické pošty. Nebezpečí hrozilo zejména uživatelům programů Outlook a Exchange. I když je virus schopen šířit se klasickým způsobem, nejčastěji proniká do systému jako připojený soubor ke zprávě s předmětem „Important Message From [Application.UserName].„ (tj. „Důležitá zpráva od...„). Zpráva obsahuje následující text: „Here is that document you asked for ... don't show anyone else ;-)„ (tj. „Toto je dokument, o který jsi žádal ... neukazuj jej nikomu jinému„).

Pokud je infikovaný dokument otevřen, virus zjišťuje, zda již daný počítač byl napaden, a pokud ne, Melissa si přečte seznam lidí v adresářích programu Outlook a prvním padesáti adresátům ze všech adresářů odešle sebe sama ve zprávě s výše uvedeným předmětem a textem zprávy.

Pokud je den roven minutě, přidá na pozici kurzoru v právě otevřeném dokumentu text: „Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here.„. Jedná se o citát z jednoho dílu Simpsonových.

komentář: Virus se dokázal rozšířit opravdu velice rychle a dokázal zahltit řadu Exchange serverů velkých firem zejména v Americe, v neanglicky mluvících zemích nebylo jeho rozšíření zdaleka tak veliké.

Win95:CIH

Jde o virus, který napadá nativní aplikace Windows 95/98 (PE - soubory Portable Executable). Je dlouhý přibližně 1Kbyte. Instaluje se do paměti, monitoruje přístup k souborům a napadá soubory typu PE EXE, které jsou otevírány. CIH ukládá sám sebe do „děr„ mezi jednotlivými PE sekcemi, takže délka napadeného souboru zůstává stejná. Virus má velmi nebezpečnou manipulační rutinu: 26. dubna (jiné, ne tolik rozšířené varianty 26. dne v každém měsíci) manipuluje s porty obsluhujícími Flash BIOS a snaží se přepsat paměť typu Flash nesmyslnými daty. To je možné pouze tehdy, pokud základní deska a chipset umožňují zápis do paměti Flash. U řady počítačů je možné zápis do paměti Flash zakázat přepínačem DIP, ale v principu záleží na designu základní desky. Řada moderních základních desek ochranu přepínačem DIP neumožňuje. Virus po zničení obsahu paměti Flash přepíše data na všech instalovaných pevných discích.

komentář: Jde o virus médii často nazývaný Černobyl. I když se objevil již v létě 1998 a všechny antivirové programy jej bez problémů detekovaly již brzy po tom, napáchal v dubnu roku 1999 řadu škod zejména v Asii – jen Korea hlásila asi 300 000 postižených počítačů. Zaznamenal také obrovskou mediální kampaň, a to i letos, kdy došlo k dalším i když zhruba o řád menším škodám. Virus se šíří klasickým způsobem (aktivně nevyužívá elektronickou poštu) a přesto se během relativně krátké doby dokázal značně rozšířit. K tomu bezesporu přispělo i to, že se hlavně v Asii šířil s oficiálně (drivery) i neoficiálně (pirátské Win98) šířenými programy.

Win32:ExploreZIP

Tento worm se začal rychle šířit v červnu 1999. Posílá sebe sama jako přílohu elektronické pošty pod jménem „ZIPPED_FILES.EXE„. Předmět zprávy může být různý (je to totiž odpověď na existující předchozí zprávu). Zpráva obsahuje následující anglický text:

```
Hi <Receipient Name>!
I received your email and I shall send you a reply ASAP.
Till then, take a look at the attached zipped docs.
bye
```

Po spuštění připojeného souboru se objeví chybové okno s hlášením o neplatném archívu ZIP. Worm se pak zkopíruje do systémového adresáře Windows a přidá jeden řádek do souboru WIN.INI, popř. do registry. To následně způsobí, že je worm aktivován při každém startu operačního systému. Worm pak získá e-mailové adresy z poštovního klienta (pomocí příkazu MAPI nebo z MS Outlook) a posílá sebe sama na další počítače. Worm je schopen vyhledávat instalace Windows i na dalších sdílených discích, a pokud takovou instalaci najde, umí se zkopírovat a změnit příslušný soubor WIN.INI. Napaden tak může být i uživatel, který worm v poště nedostal nebo připojený soubor nespustil, pokud poskytuje plná přístupová práva ke svým diskům někomu jinému.

Tento worm obsahuje velmi nepříjemnou manipulační rutinu - hledá na dostupných discích (a to i na síťových, popř. sdílených, pokud je na nich právo zápisu) soubory s rozšířením .C, .CPP, .H, .ASM, .DOC, .XLS a .PPT a ničí je tak, že je zkrátí na nulovou délku. To může způsobit nevratné ztráty dat!

komentář: Na rozdíl od předchozích je tento virus destruktivní, což také loni prokázal. Jako ostatní masově se posílající viry rychle zazářil a dost rychle zmizel, další zapakovaná varianta se objevila na podzim 1999. Škody opět způsobil zejména v anglosaských zemích, i když i u nás tu a tam nějaké soubory zničil.

Win32:PrettyPark

Tento worm se poprvé objevil v květnu 1999 ve Francii. V současné době se vyskytuje několik „variant„, které jsou funkčně totožné, ale jsou buď nezapakované či zabalené různými kompresními programy. Trojan je schopen pracovat pod systémy Windows 9x/NT. Do počítače přichází e-mailem od uživatele, který jej rovněž spustil. E-mailová zpráva má následující formát:

```
------------ Subject: C:\CoolProgs\Pretty Park.exe
Test: Pretty Park.exe :) ------------
```

Připojený soubor se nazývá „Pretty park.exe„ nebo „Pretty~1.exe„.

Worm se pak snaží posílat sebe sama automaticky každých 30 minut všem adresátům z adresáře programu Outlook Express.

Worm se též pokouší připojit k serveru IRC a ke specifickému kanálu IRC. Po připojení zůstává připojen a zpracovává příkazy z tohoto kanálu. Autor může využít tohoto připojení k získání vzdáleného přístupu k danému počítači a získat jméno počítače a jeho uživatele, a dále jméno a heslo pro Dial Up.

Po spuštění na daném počítači se worm zkopíruje do souboru FILES32.VXD v adresáři WINDOWS\SYSTEM a modifikuje jeden kritický klíč v registrech.

Tato změna způsobí, že soubor FILES32.VXD bude spuštěn spolu s libovolným EXE souborem.

komentář: Uvedený zásah do registrů přináší jeden vedlejší efekt: odstraněním uvedeného VXD souboru dojde k tomu, že nelze spustit žádný program. Proto je nutno napřed uvést do pořádku registry a teprve potom mazat soubor. Tento worm patří i u nás k velmi rozšířeným a je pravděpodobně nejvíce hlášeným virem současnosti.

VBS:Bubbleboy

Virus se objevil v listopadu 1999. Jde o první virus, který je aktivován pouhým čtením elektronické pošty. Je schopen pracovat pod operačními systémy Windows 98 a Windows 2000 s nainstalovanými programy Outlook a Internet Explorer. Worm je obsažen přímo v těle zprávy a při jejím čtení je programy Outlook či Outlook Express spuštěn bez nutnosti spustit/otevřít připojený soubor. Tělo zprávy obsahuje kód HTML a VB Script. Bubbleboy se dosud nevyskytuje volně mezi uživateli, nevykonává žádnou nebezpečnou manipulační činnost.

Bubbleboy vyžaduje pro svoji činnost Internet Explorer 5 a Windows Scripting Host (WSH je standardně instalován pod Windows 98 a Windows 2000 a při instalaci MSIE 5.x). Virus napadá uživatele produktů Microsoft Outlook a Outlook Express. V Outlooku je pro aktivaci viru třeba, aby uživatel zprávu „otevřel“. V Outlook Express se Bubbleboy aktivuje i v případě, že je zpráva zobrazena v „náhledovém okně „.Worm se nešíří, pokud je bezpečnost v Internet Zone IE5 nastavena na stupeň High.

Po svém spuštění Bubbleboy pošle sebe sama na každou e-mailovou adresu ze všech adresářů programu Outlook či Outlook Express. Pak nastaví klíč v Registry tak, že při své příští aktivaci se již

odesílat nebude. Pro svoji činnost zapíše sebe sama do souboru UPDATE.HTA v systémovém adresáři Windows. Worm je schopen pracovat pouze pod anglickou a španělskou verzí Windows. V současné době existují dvě varianty viru, druhá varianta je kódována.

Virus se pokusí změnit vlastníka a organizaci v systému (přes registry) na „BubbleBoy„ a „Vandelay Idustries„. Zpráva, pomocí které se virus šíří, obsahuje následující informace:

```
From: <infected person>
Subject: BubbleBoy is back!
Body: The BubbleBoy incident, pictures and sounds
```

komentář: Jde skutečně spíše o prokázání toho, že uvedená metoda funguje a je „průchodná„. Bohužel je možno očekávat, že se v blízké budoucnosti objeví další viry tohoto typu, možná i s mnohem nebezpečnější či destruktivní manipulační činností. Microsoft uvolnil bezpečnostní patch, který by se měl umět vyrovnat s touto bezpečnostní dírou.

VBS:Kak

Tento worm se připojuje ke každé zprávě, odcházející z napadeného systému. Pro svoje šíření nevyžaduje přiložený soubor (podobně jako BubbleBoy).

Kak je vytvořen v jazyku JavaScript a pracuje s klientem Outlook Express 5.0.

Pro aktivaci viru stačí zobrazení zprávy v náhledovém okně. Kak pak změní nastavení programu Outlook Express tak, že soubor s připojeným podpisem je vlastně soubor s virem. Každá odeslaná zpráva pak obsahuje worm!

komentář: Kak využívá známé bezpečnostní chyby programu Outlook Express pro vytvoření lokálního souboru HTA. I tento worm se šíří do diskusních skupin Usenetu a podle posledních odhadů možná brzy vytlačí Win32:Ska z prvního místa.

VBS:LoveLetter

Tento worm se stal „hitem letošní sezóny„. Udeřil 4. května a během několika málo hodin zasáhl celou Asii a Evropu (Amerika přišla kvůli časovému posunu na řadu o něco později).

LoveLetter je worm vytvořený ve VBS (Visual Basic Script language). Do počítače přichází pomocí e-mailu, je aktivován dvojklikem na přílohu dané zprávy se jménem LOVE-LETTER-FOR-YOU.TXT.vbs. Pro svoji činnost vyžaduje, aby byl instalován software Windows Scripting Host.

Pro svoji distribuci používá hlavně e-mail, je však schopen se šířit i pomocí klienta mIRC.

VBS:LoveLetter se po aktivaci zkopíruje do několika systémových souborů a modifikací Registry zabezpečí svoje spuštění po každém startu Windows.

Posílá sebe sama pomocí programu Outlook jako připojený soubor takřka stejným způsobem jako Melissa. Posílá však infikovanou zprávu všem příjemcům ze všech adresářů. Infikovaná zpráva má předmět „ILOVEYOU„ a obsahuje následující text:

```
kindly check the attached LOVELETTER coming from me.
```

Worm se snaží pomocí Internet Exploreru stáhnout a zajistit spuštění EXE souboru z jednoho filipínského serveru. Tento program pak mimo jiné sbírá hesla použitá na daném počítači a snaží se je e-mailem posílat na Filipíny.

VBS:LoveLetter hledá na všech lokálních i vzdálených discích určité soubory. Pokud nalezne soubor s rozšířením vbs či vbe, přepíše jej sebou samým. Soubory s rozšířením js, jse, css, wsh, sct, hta jsou rovněž přepsány a navíc přejmenovány na *.vbs. Také soubory jpg a jpeg jsou přepsány a přejmenovány na *.jpg.vbs, zatímco soubory mp3 a mp2 nejsou přepsány, ale je vytvořen soubor na *.mp?.vbs obsahující virus a originálnímu souboru je změněn atribut na hidden.

Pokud VBS:LoveLetter nalezne klienta mIRC, přepíše soubor „mirc.ini„ a je pak schopen poslat sebe sama ostatním uživatelům IRC.

Worm též vypouští soubor HTM, a tak se snaží zvýšit svoji šanci na další rozšíření.

komentář: Worm je ještě v živé paměti, i u nás jím byla postižena řada uživatelů. Po pachateli se stále ještě pátrá. Osobně si myslím, že autor (podobně jako kdysi v roce 1988 Robert Morris) neodhadl rychlost šíření svého díla. Pokud chtěl získat několik přístupových hesel k Internetu na Filipínách (a vše nasvědčuje tomu, že to bylo jeho hlavním cílem), pak worm totálně selhal. Místo toho, aby se tajně po delší dobu pomalu šířil, zaplavil rychle celý svět, čímž na sebe samozřejmě upozornil. Tento efekt by měl být mementem těm, kteří čas od času vytáhnou koncepci „užitečných virů„.

Po originálním viru se bohužel velmi rychle objevila řada variant a modifikací. Důvody jsme si už objasnili dříve. Některé z nich se liší pouze formátováním, jiné mají změněné i texty, psychologicky to na uživatele zkouší z různých stran. Jedna varianta zasílá vtip, jiná upozorňuje na nebezpečí viru LoveLetter, další se tváří jako zpráva od Symantecu, výrobce antivirových programů. Psychologicky nejzajímavější je určitě ta, která oznamuje stažení 326 dolarů z kreditní karty a žádá o vytištění přiložené faktury. Variant se objevily desítky, žádná z nich však nedosáhla „úspěchů„ prvního „zamilovaného„ dopisu. Ten měl totiž veliké štěstí, když se mu podařilo proniknout do velkých firem, které používají Outlook a v jejichž adresářích se nacházejí tisíce kontaktů do dalších velkých firem po celém světě. Řada variant vznikla bohužel i z „dobrých„ úmyslů, když se objevil LoveLetter na webovských stranách okomentovaný – bohužel tak, že zůstal nadále funkční.

Přidat detekci viru jako je LoveLetter není pro antivirovou firmu žádným problémem. Jiná je ale otázka, kdy a jak informovat uživatele o nebezpečí a jak k nim aktualizaci dopravit. Ukažme si nyní, jak to vlastně celé dne 4. května z pohledu naší firmy probíhalo:

10:52 dorazila první infikovaná zpráva, odeslaná nic netušícím uživatelem

10:53 během následujících několika minut dorazily další zprávy

10:59 s dotazem se ozval první uživatel

11:20 došla první zpráva ze zahraničí, že se něco děje

11:23 vzorek viru odeslán ostatním AV firmám přes REVS

11:40 mnoho zpráv o masivní hlášení z celé Evropy všem AV firmám

12:10 zveřejněna první aktualizace antiviru na našem webu

12:40 informace o viru poslána do mailing listu našich uživatelů

13:15 odeslána tisková zpráva pro média

14:00 na webu zveřejněna první vlastní analýza a detailní popis wormu

Podobný průběh měl onen čtvrtek jistě i u ostatních antivirových firem. Před každou pak stálo velké dilema: jak rozpoznat, že se jedná o vážné nebezpečí, kdy stojí za to informovat uživatele, vytrhnout jej z toho, co právě dělá a „nutit„ je k aktualizaci? Ve kterém okamžiku už bylo jasné, že se nejedná o planý poplach, ale o věc zásadního významu?

Během deseti dnů se média na celém světě zabývala dvěma odlišnými viry: 26. dubna virem CIH a 4. května virem LoveLetter. Jaký je rozdíl mezi těmito dvěma viry? Co od kterého z nich hrozí uživatelům? Který je nebezpečnější?

CIH je klasickým virem, který napadá výkonné programy, šíří se relativně pomalu, v době aktivace jeho destrukční činnosti byl již dlouho znám a uživatelům, kteří používají jakýkoli antivirový program a alespoň čas od času jej aktualizují, od něj vlastně žádné nebezpečí nehrozilo. Destrukční rutina je ale velmi nepříjemná a může vést ke kritické ztrátě dat.

LoveLetter představuje na druhou stranu novou generaci nebezpečných programů. Je schopen se rozšířit velmi rychle po celém světě a napáchat značné škody. Využívá bezpečnostních děr v operačním systému a aplikacích i psychologické prvky a je velmi účinný. Bohužel se s takovými útoky budeme setkávat i v budoucnosti. A je jen otázkou času, kdy se budou muset přizpůsobit nejen antivirové firmy, ale i uživatelé a hlavně výrobci operačního systému a aplikačních programů. Ti totiž v posledních několika letech implementovali do svých programů řadu nových a velice mocných funkcí, ale bohužel bez ohledu na jakoukoli bezpečnost.

Nejvíce je tento trend vidět na příkladu firmy Microsoft. Ta si sice nebezpečí virů před dlouhou dobou uvědomila a zavedla řadu opatření pro to, aby se viry nemohly dostat například na firemní webové stránky (i k tomu v minulosti došlo, ale náprava byla velice rychlá) či dokonce do produkce – například na CD se softwarem. Z hlediska vývoje produktů je však situace zcela jiná. To se ukázalo již u makrovirů, kdy několik zcela zásadních chyb v koncepci produktu umožnilo to, že makroviry jsou dnes reálnou hrozbou: makra nelze vypnout, existují automaticky spouštěná makra, makra v dokumentu mají vždy přednost před globálními makry, makra jsou součástí stejného souboru jako vlastní data.

Podobné problémy má i operační systém Windows: implicitně nejsou „známé„ přípony souborů zobrazovány, a tak řada poučených uživatelů neviděla ono .vbs u wormu LoveLetter a otevírala dle svého nejlepšího přesvědčení pouze textový soubor. Můžeme ale pokračovat: implicitní instalace Windows Scripting Host, provázanost aplikací, příliš silný jazyk VBS, nemožnost oddělit nastavení bezpečnosti jinak pro Internet Explorer a jinak pro poštovní klienty, implementace HTML a dokonce VBS do poštovních klientů, spouštění kódu (programy, skripty) přímo z poštovních klientů a tak dále. To jsou všechno věci, kterými zejména Microsoft (ale i další vývojáři aplikací) přímo přispívají k šíření virů a nad kterými by se měli co nejdříve zamyslet. Jinak může po několika podobných incidentech dojít k tomu, že uživatelé začnou přemýšlet, zda jim poskytovaný komfort a uživatelsky přítulné vlastnosti stojí za všechno to nebezpečí, které jim hrozí.

Microsoft se s tímto nebezpečím zatím vypořádal po svém: v rozhovoru pro týdeník Time upozornil Bill Gates na nesmyslnost případného rozdělení společnosti z hlediska virů takto: „Aktualizace a nové verze (operačního systému) Windows a (programu pro zasílání elektronické pošty) Outlook by mohly mít například lepší ochranu proti útokům, jaký podnikl vir ILOVEYOU, a proto by uživatele v budoucnu stěží postihly„ (citace dle ČTK). Ve světle výše uvedených problémů se naskýtá otázka, proč tomu tak už dávno není…

Budoucnost

Pokud rychle nezareagují autoři aplikačních programů, pak nás čekají další nové a bezpochyby potřebné vlastnosti, které přinesou další bezpečnostní díry. Provázanost aplikací se ještě zvýší, nabízí se

dokonce binární kompatibilita jejich dat. Ostatně na úrovni makrojazyka k ní již není daleko: VBA od Microsoftu licencovala řada firem z nejrůznějších oblastí. A pokud se dnešní koncept „klikni a pak teprve přemýšlej„ změní na „klikni a pokud možno nepřemýšlej vůbec“, tak se máme na co těšit. Jsem hodně zvědav na to, kde se vytyčí hranice mezi komfortem a bezpečností, na tom totiž záleží to, co nás v budoucnu čeká. Mimochodem – virus LoveLetter byl úspěšně transformován do skriptu pro Unix shell, kde je schopen se též bez problémů šířit. Od uživatele to chce ovšem jediné: přiložený soubor uložit na disk a pak spustit shell s příslušnými parametry. To je ovšem mnohem víc práce než jediný dvojklik a každý si během ní uvědomí, co a proč právě dělá …

Jak se tedy proti počítačovým virům a ostatní havěti bránit?

Obrana proti virovému nebezpečí skutečně není složitá. Stačí přemýšlet, nevěřit, a proto nespouštět žádnou přílohu z nevyžádané pošty (byť od známých osob), správně nastavit dostupné bezpečnostní parametry aplikací, používat antivirové programy (a pravidelně je aktualizovat!), ale i další prostředky jako jsou firewally. Ty se vyplatí nejen v podnikových sítích ale i u domácích uživatelů (například freewarový ZoneAlarm). Důležitá data je nutno pravidelně zálohovat, ale to už jste jistě někde slyšeli, že ☺ ?

JAKÁ PROSTŘEDÍ DNES TVOŘÍ ŽIVNOU PŮDU VIRŮM

Petr Odehnal
Grisoft Software s.r.o.

Životní prostředí

Ne. Nezešílel jsem (tedy možná ano, ale projevuje se to jinak) a nebudu vás obtěžovat zavíráním jaderných elektráren ani otevíráním studánek. Životní prostředí, o kterém se chci zmínit, je životním prostředím ve kterém se dnes pohybují počítačové viry všeho druhu - jde o operační systém ve kterém dokáží žít a o cesty šíření, které mají k dispozici.

Poznámka: V dalším textu budu občas používat slůvko malware. Jde o souhrnné označení pro škodlivý software všeho druhu (MALicious softWARE) - tedy pro to, co známe jako viry, wormy, trojské koně, backdoor servery apod.

Bylo nebylo

Začněme stručným historickým přehledem. Ono totiž staré úsloví "kdo se nepoučí ze své minulosti, je odsouzen prožít ji znovu" opravdu platí.

Malá exkurze do pravěku

Vraťme se na chvíli do doby kdy byli odvážlivci ještě nebojácní, rizika vysoká, muži byli praví muži, ženy byly pravé ženy a malá chlupatá stvoření z Alfy Centauri byla pravá malá chlupatá stvoření z Alfy Centauri.

V těch krásných dobách byl DOS na PC považován za operační systém, data se přenášela na disketách s kapacitou 360kB, honosný název lokální síť byl používán už pro úspěšné propojení dvou počítačů sériovou linkou a modem vlastnilo pouze pár snílků.

Už v těch idylických dobách můžeme potkat první počítačové viry, ale jde o jev tak nový a okrajový, že i Peter Norton (autorita těch časů s velkým A) je považoval za obdobný mýtus jako přítomnost aligátorů v kanalizačním systému New Yorku.

Nejrozšířenějším typem infekce jsou v pravěku boot viry. Disketa je hojně užívaným médiem pro přenos dat a občas ji v mechanice zapomene každý. Souborových virů sice existuje mnohem víc a šíří se také veleúspěšně (vždyť se bavíme o době kdy opravdu velká počítačová hra - nejčastěji to kopírovaný druh softwaru mezi uživateli - měla pár stovek kB), ale stejného rozšíření jako boot virům se jim do příchodu Windows dosáhnout nepodařilo.

V dobách pravěkých se také objevují první antivirové praprogramy - obvykle šlo o jednoúčelové utility pro odstranění nějakého konkrétního viru a obzvlášť dokonalé uměly odstranit i pět nebo šest různých virů.

Typickým životním prostředím úspěšných pravěkých virů tedy byl operační systém MS-DOS a vhodným médiem přenosu 5.25" disketa.

A začíná středověk

Určení přesnějšího data začátku virového středověku ponechme softwarovým archeologům. Je to doba, kdy sice boot viry zůstávají nejčastějším typem infekce, ale souborové viry přestávají hrát roli opomíjené Popelky. Třeba Tremor se v roce 1993 masivně rozšířil v zejména německu. Je těžké odhadnout jako roli v tom hrálo, že byl v květnu vysílán stanicí PRO7 na jejich datovém kanálu Videodat, ale určitě to trošku pomohlo.

V našich luzích a hájích zahájil v dubnu 1994 své tažení velmi úspěšný multipartitní virus OneHalf. Toho ostatně můžeme v reálném světě potkat dodnes a patří tak k "služebně nejstarším" souborovým virům.

Středověk přináší první "univerzální" antivirové programy, schopné detekovat (a občas při troše štěstí i léčit) většinu tehdy známých virů. Pokud vás zajímají vzácné relikvie té doby, tak na ftp://ftp.sac.sk/pub/pc/avmuseum/ najdete takové skvosty jako jeden z prvních McAfeeho SCANů - verzi, která najde 19(!) různých virů nebo třeba VSUM ze začátku roku 1990 obsahující popis 70 virů.

Typickým životním prostředím středověku zůstává MS-DOS, občas vybavený jednoduchou grafickou nadstavbou známou jako Windows. Nejčastějším přenosovým médiem zůstává disketa ale význam sítí všeho druhu výrazně vzrůstá. Zejména lokální sítě se starají o rychlou distribuci nákazy v rámci jedné instituce. Internet je u nás sice stále ještě výsadou vyvolených, ale modemem přístupné BBS stanice obsahující komukoli přístupné vzorky virů se už zabydlely.

Novověké radovánky

V srpnu 1995 se narodil makrovirus WM/Concept a začala se tak psát nová éra historie počítačových virů. Makroviry totiž zbouraly dlouho slavně hlásanou pravdu, že "manipulace s datovými soubory je neškodná". Netrvalo to dlouho a makroviry se v tabulkách úspěšnosti dostaly do čela a spokojeně tam setrvávají dodnes.

U nás jsme krátký čas měli výhodu - makroviry ve WordBasicu (t.j. makroviry pro starý Word) byly závislé na lokalizaci Wordu a česká verze jim nedělala dobře. Jediným makrovirem této éry, který se i u nás obstojně šířil, byl WM/CAP. Jeho autor totiž přišel na prostou (a geniální) myšlenku – názvy jazykově závislých funkcí odvozoval z příslušných položek v menu programu. Příchodem Office 97, kde byl původní WordBasic nahrazen VBA (Visual Basic for Applications) tuto výhodu ztrácíme a makroviry se i u nás stávají nejrozšířenějším typem infekce.

Novověk je také dobou reinkarnace souborových virů - tentokrát v prostředí Windows. Objevují se první vlaštovky v podobě technicky velmi pokročilých virů - dočkali jsme se silně polymorfních virů a dokonce i virů, které jsou schopny se pod Windows NT usadit v paměti jako SYS driver – tedy s možnostmi takřka neomezeným. Ale většina z technicky dokonalých virů je zatím příliš složitá a tedy nestabilní, takže jen málo z nich je schopno rozumějšího šíření. V každém případě je to ale příslib pro nejbližší budoucnost. Máme se ještě na co těšit.

Typickým životním prostředím novověku jsou Windows všeho druhu a aplikace z MS Office (především Word a Excel).

Přenosovým médiem se stále častěji stává elektronická pošta a internet vůbec. Zejména používání DOC a XLS souborů jako de facto standardního formátu pro přenos dat se makrovirům velmi zamlouvá. Zlozvyk posílat komprimované soubory v "self extract" tvaru zase oceňují souborové viry.

A je tady milénium

Rozsáhlé debaty o tom, zda nové tisíciletí začíná prvního ledna roku 2000 nebo 2001 nás nemusí zajímat. V oblasti počítačových virů totiž milénium začalo 26.března 1999. Toho dne se v několika alt.bin.rozcapeny.bobr objevil soubor LIST.DOC, který obsahoval hesla pro přístup k pár placeným

porno stránkám. Neověřoval jsem zda ta hesla fungují, ale připojený makrovirus W97M/Melissa fungoval docela obstojně.

Ostatně autor tohoto výtvoru ještě bude mít příležitost se nad sebou zamyslet. V prvním kole soudního řízení již byl uznán vinným a nyní už se čeká jenom na určení výšky trestu.

Trend přímého využití internetu k rozeslání infikovaného souboru je stále silnější. Po internetovém červu ExploreZip jsme se 4. května dočkali zatím nejrychleji se šířící infekce - VBS/Iloveyou (resp. VBS/LoveLetter).

Životním prostředím dneška zůstávají Windows všeho druhu a aplikace MS Office. Úloha elektronické pošty jako přenosového média je ale mnohem silnější. Tím že viry nečekají na vaši laskavou spolupráci a odešlou se samy - na adresy, které pro ně udržujete ve svých adresářích - je jejich šíření mnohem rychlejší. To těší zejména výrobce antivirových systémů, kteří tak mají mnohem kratší čas na reakci (vydání aktualizací apod.) než dříve.

And now for something completely different

A teď něco málo o situaci z pohledu jednotlivých typů virů.

Boot viry

Disketa jako přenosové médium v době lokálních sítí a internetu vymírá a dnešní PC jsou obvykle konfigurována tak, že nejprve startují z pevného disku. Výrazně to snížilo rozšíření tohoto typu infekce, ale na listinu ohrožených druhů se asi hned tak nedostane.

Souborové viry pro DOS

Klasické souborové viry fungující pod MS-DOSem jsou na tom mnohem hůře. Už jejich schopnosti přežít v prostředí Windows nejsou nijak skvělé a především vymřel jejich přirozený kanál šíření - kdo si dnes posílá DOSové spustitelné soubory, že.

Souborové viry pro Windows

Ani nová generace souborových virů - určených pro Windows - nemá na růžích ustláno. Daří se jim sice přežívat v rámci jednoho počítače vcelku úspěšně, ale další šíření už je komplikované. Dnes už není možné jednoduše přenést vyinstalovanou aplikaci z jednoho počítače na druhý. Patří k ní spousta obskurních DLL, podivných fontů atp. - to vše poházeno v mnoha různých adresářích a doprovázeno kryptickými záznamy roztroušenými v registry nebo v .INI souborech.

Aby podobný typ malwaru úspěšně přežil, musí být schopen využít jiných způsobů šíření a nespoléhat se na přenos infikovaného EXE souboru.

Modelem nejúspěšnějším je přímé využití (zneužití?) internetu, ale to je téma které si zaslouží samostatnou kapitolku, takže se k němu ještě vrátím.

Nadějně vypadající vkládání infikovaných souborů do archivů (ZIP, RAR, ARJ etc) se kupodivu v praxi příliš neosvědčilo.

Zdá se, že pro spoustu lidí je pohodlnější stáhnout si archiv z internetu, než si ho nechat poslat mailem (nebo nedejpříroda na disketách) od někoho ze svého okolí.

Pochybnou čest být jediným masivně rozšířeným souborovým virem pro Windows má Win32/CIH (díky lásce novinářů k dramaticky znějícím jménům také známý jako Černobyl). Na počátku jeho popularity bylo silné lokální rozšíření na dálném východě. Pokud uvážíme odkud pochází většina komponentů dnešních PC (a samozřejmě CD s ovladači), tak asi nepřekvapí, že značnou část incidentů Win32/CIH lze vystopovat k použití CD od výrobce nějaké karty - t.j. ke zdroji obecně pokládanému za dostatečně bezpečný.

CD distribuce stojí i za dalšími incidenty. Například W95/Marburg se dostal na CD jednoho britského časopisu pro notorické hráče počítačových her a po několik měsíců díky tomu patřil k často se vyskytujícím příšerkám.

Jen mimochodem - mnohé viry pro Windows vědí (na rozdíl od mnoha uživatelů), že šetřiče obrazovky (.SCR) mají ve skutečnosti EXE formát a infikují je také. Dalším "podporovaným" formátem, jehož obliba v poslední době roste, je soubor s nápovědou (.HLP), který umožňuje vložit dropper viru.

Makroviry

Příchod makrovirů (zanedlouho budeme slavit páté výročí této radostné události) změnil virový svět výraznějším způsobem než jakékoli předchozí události. Makroviry jsou dnes zcela bezkonkurenčně nejrozšířenějším typem infekce. Jejich podstatnou výhodou je přímá vazba na datový soubor, který prostě lidé chtějí a potřebují sdílet. Nějakou instalaci Wordu a Excelu má na svém počítači téměř každý a tak jsou přenosové možnosti pro makroviry fantastické.

Další milou vlastností je hluboká integrace VBA (Visual Basic for Applications - Microsoftí jazyk určený pro páchání makrovirů) do prostředků MS Office (a do Windows vůbec). V kombinaci s dětskou jednoduchostí jazyka a celkem slušnými vývojovými nástroji je dnes vytvoření nového makroviru natolik triviální, že to bez obtíží zvládne i jednoruká hrbatá opice. A mimořádně tupá jednoruká hrbatá opice alespoň dokáže vzít zdrojový text existujícího makroviru a změnit ho - přinejmenším dopsat komentář "tento strašlivý virus jsem napsal JÁ" a případně vložit zavolání "FORMAT C:" (to v případech, že zbytky inteligence v tom zabránily původnímu autorovi makroviru).

Jenom pro představu, toto je počet variant několika makrovirů:

X97M/Laroux	329
WM/Npad	284
WM/CAP	263
WM/Wazzu	217
W97M/Class	139
WM/ShowOff	127
WM/Concept	117
W97M/VMPCK1	108

Ta tabulka je platná cca k poledni 18. ledna - nemám čas, chuť ani důvod podobné přehledy nějak pravidelněji udržovat, ale pro představu to snad stačí.

Makroviry dnes existují pro Excel, Word, PowerPoint, Access, Project, Visio a pár (spíše experimentálních) kousků by se našlo i pro AmiPro nebo Corel Draw. Reálný význam ovšem mají

pouze viry schopné šíření v DOC a XLS formátech, které jsou pro výměnu informací používány nejčastěji.

Za zmínku snad stojí ještě jeden důsledek dokonalého popropojování aplikací z balíku MS Office - můžete totiž do své PowerPointové prezentace vložit třeba tabulku z Excelu a to tak, že velmi důkladně - t.j. včetně případného viru. Takový virus tam spí jako Růženka a jakákoli manipulace s prezentací v PowerPointu je neškodná. K probuzení viru není nutný polibek prince (ani uživatele). Stačí prezentaci editovat a infikovaný sheet otevřít - na tuto práci bude spuštěn Excel a makrovirus se ve známém prostředí okamžitě zabydlí.

Internetová havěť

Pro malware dnes není libovolné využití internetu žádný problém. Po počátečních nesmělých krůčcích – posílání informací z vašeho počítače na nějaký anonymní FTP účet a nebo třeba posílání vulgárních mailů vašim jménem a z vaší adresy - došlo i na přímé aktivní šíření virů a wormů prostřednictvím internetu. Rychle se ukázalo, že pro tvůrce podobných legrácek nejde o technický problém. Obtížné je donutit příjemce emailu ke spolupráci - t.j. ke spuštění přiloženého EXE souboru nebo otevření dokumentu.

Třeba Win32/Ska (známější jako Happy99) ke každé zprávě odeslané z infikovaného počítače odešle ještě další prázdnou zprávu, ke které je připojen spustitelný soubor. Příjemce takové dvojice zpráv musí být nadán mimořádnou dávkou odvahy aby takto zaslaný soubor spustil.

Fikanější techniku přinesl worm ExploreZip, který naopak na emaily odpovídá. Scénář je jednoduchý - pokud na infikovaný počítač dorazí mail, tak worm okamžitě odpoví ve smyslu "teď fakt nestíhám, odpovím jakmile budu mít čas - zatím se podívej na přiložený soubor". Asi nepřekvapí, že v přiloženém souboru se jménem ZippedFiles.exe je kopie wormu. Aby iluze byla dokonalá tak je tento EXE file vybaven ikonou, kterou používá WinZIP pro archivy typu ZIP. V ideálním případě má navíc uživatel vypnuté zobrazování přípon u souborů "známých typů" a tak vidí pouze text ZippedFiles a ikonku typickou pro zaZIPovaný soubor. I uživatel věci znalý může v takovém případě (nic zlého netuše) spustit přiložený soubor v domnění, že se mu otevře oblíbené barevné prostředí WinZIPu a zobrazí mu obsah archivu.

Zatím posledním (a doufám, že se na tom do vytištění tohoto sborníku nic nezmění) rychle se šířícím virem na internetu byl VBS/Iloveyou (aka LoveLetter). Přestože byl závislý na instalovaném Outlooku z jehož adresářů si stejně jako W97M/Melissa bral adresy na které stojí zato se poslat a na instalovaném Windows Scripting Hostu, který je nutný k interpretaci VBS souborů, dosáhl rychlosti šíření kterou jsme zatím neviděli. Během pár hodin se mu podařilo zasáhnout v podstatě celý internetový svět. Odpustím si přesný popis tohoto viru (a jeho vzápětí se vyrojivších variant) - jde o natolik aktuální téma, že se o něm určitě vše podstatné dozvíte v ostatních přednáškách.

Netroufám si odhadnout proč vlastně takové množství otevřelo připojený soubor LOVE-LETTER-FOR-YOU.TXT.vbs. Snad ta přípona .TXT vedla k přesvědčení, že se nemůže nic stát (vždyť přece textové soubory nemohou obsahovat nic škodlivého), možná pomohlo, že virus se posílá na úplně všechny adresy z adresáře. Nevím.

Stále ale zůstává (pro virového pisálka nepříjemná) pravděpodobnost, že opatrný člověk si dá pozor a neznámý soubor neotevře. Nevadí. Microsoft pokročil v integraci svých technologií tak daleko, že není nutné spoléhat na spolupráci uživatele. Virovým pisálkům se podařilo objevit (a vzápětí velmi úspěšně využít) drobnou chybku v defaultním nastavení bezpečnosti a dosáhnou automatického spuštění kódu VBScriptu, který dorazí v HTML zprávě do Outlooku. První vlaštovkou byl VBS/BubbleBoy (zneužívající plnou verzi Outlooku) a vzápětí se objevil VBS/Kakworm

(spolupracující s daleko rozšířenějším Outlook Express). Microsoft sice velmi rychle publikoval "security update", který tahle vrátka zavírá, ale ruku na srdce (nebo na nějaký jiný orgán), kdo pravidelně sleduje všechny patche, updaty a service packy a snaží se jimi opečovávat svůj systém ?

Zvláštní kapitolu zneužití internetu představují trojské koně typu Backdoor (asi nejznámější jsou BackOrifice, NetBus a SubSeven). Na rozdíl od běžných (a poněkud tupých) trojských koní, jejichž nejčastější akcí po příchodu do systému je chvilku počkat a smazat disk, ponechává backdoor trojan veškeré aktivity v rukou osůbce, která vám ho poslala. Ta pak se znalostí vaší IP adresy získá vzdálený přístup k vašemu PC. Kvalita tohoto přístupu se u jednotlivých trojských koní liší, ale souborové operace a spouštění programů zvládnou všechny - a to bohatě stačí.

Ideální kombinaci pak představuje spojení schopnosti vlastního šíření s backdoor interfacem a nějakým systémem "nabonzování světu", že váš počítač je nyní otevřen a vítá návštěvníky. Worm PrettyPark je vybaven přesně takto a patří dnes k velmi populárnímu malwaru.

Backdoor trojany jsou velmi pohodlným způsobem jak zajistit distribuci programů typu Win32/Trin00 (určených pro DDoS útoky).

Po emailu je nejoblíbenějším způsobem šíření infikovaných souborů využití chatovacích programů - nejčastěji mIRC. Původní pokusy psát IRC viry, které modifikací SCRIPT.INI donutily mIRC k jejich dalšímu šíření, jsou dnes spíše nahrazovány zneužitím mIRC pouze pro transport infikovaného objektu. Tuto techniku používá například právě VBS/Iloveyou.

Ještě pár slov o Linuxu

Linux (při vší úctě k tlupám mládenců s tučňáčkem v klopě) zatím nepředstavuje prostředí dostatečně rozšířené a dostatečně jednotné, aby se mohl stát úspěšným prostředím pro přežívání virů.

Linux je sice výrazně bezpečnější než Windows, ale to rozhodně neznamená, že je nějak "absolutně" bezpečný. Jen ho zatím častěji používají lidé, kteří vědí co dělají a svou konfiguraci si dokáží sami rozumně ošetřovat (ono jim ostatně ani nic jiného nezbývá). Nástup nejrůznějších "hotových distribucí" Linuxu už je sice velmi patrný, ale dovolil bych si trošku optimismu - je velmi nepravděpodobné, že se Linux v dohledné době dočká stejného rozšíření (a mezi stejnými typy uživatelů) jako dnes mají Windows a stane se tak obdobně kamarádským prostředím pro šíření virů.

Hoax

Jistě to znáte - dorazí mail s varováním o strašně nebezpečném viru, který dorazí mailem a "znásilní vám manželku a vyžere ledničku tak dokonale, že vám tam nenechá ani jednu Plzeň". Nezbytnou součástí je douška "pošlete toto varování úplně všem".

Poprosil bych tedy - pokud vám dorazí podobná zpráva, tak nevěřte uvedenému "FBI tvrdí, firma XYZ oznámila" a než ji začnete rozesílat na dalších pár set adres, tak si u nějakého zdroje (nejlépe u antivirové firmy dle vlastního výběru) ověřte zda ta zpráva obsahuje alespoň stopové prvky reálné informace nebo zda jde o další nesmyslný hoax.

"Press release" viry

Jde o speciální kategorii virů, které jsou k spatření především v tiskových zprávách všeho druhu. Na rozdíl od hoaxů jsou podloženy existencí nějakého reálného viru, jehož šance na šíření jsou ale pramalé a jediným důvodem proč o něm informovat svět je touha marketingových mužíčků upozornit na existenci a kvality jejich firmy.

Obvyklý scénář šíření je následující: firma XYZ vydá tzv. "press release", kterou promptně převezmou různé internetové časopisy. Následuje smršť dotazů uživatelů "A co váš program - detekuje nový zákeřný virus Pepík ?". Jediný způsob jak takovému nevítanému zahlcení hot line zabránit je zveřejnit vlastní press release a lavina se valí dál.

Čerstvým příkladem takové viru může být třeba další pokus inspirovaný VBS/Iloveyou - virus VBS/NewLove. Jeho autor se pokusil napsat "dokonale" polymorfní virus a dosahuje toho vkládáním komentářových řádků do generovaného VBS kódu. Nic proti tomu, je to jistě zábavný pokus (jaká škoda že většina antivirů dokáže komentáře ignorovat) ale pisálek to poněkud přehnal - výsledné VBS soubory mají několik stovek kB. Navíc virus provádí celkem drsnou destrukci - na všech discích nevratně zlikviduje všechny soubory, které se mu podaří otevřít. Podobného monstra s takovým projevem si nelze nevšimnout a spolu s nedávnými událostmi vyvolanou pozorností uživatelů (bohužel jen dočasnou) na VBS přípony to efektivně snižuje šance viru alespoň na náznak přežití.

Přesto se kolem tohoto zmetku strhnul skoro stejně velký mediální kolotoč, jako okolo reálně nebezpečného viru.

Velmi mne podobné incidenty mrzí. Opakovaný pokřik kvůli takovým pitomostem snižuje "citlivost" veřejnosti a v záplavě podobných "taky varování" se může snadno ztratit zpráva o něčem opravdu důležitém.

Konečně něco o životním prostředí

Z uvedeného přehledu se dá snadno určit co je pro nás největším nebezpečím - internet, internet a troška toho internetu. To ale neznamená že další formy distribuce dat smíme podcenit. Americká ICSA pravidelně monitoruje virové incidenty ve třech stovkách velkých amerických společností. Výsledky určitě stojí za pozornost:

Zdroj infekce	1996	1997	1998	1999
disketa	74%	88%	67%	39%
email	9%	26%	32%	56%
download	12%	24%	14%	16%
neznámý	15%	7%	5%	9%

Šťouralové si možná všimnou, že součty jsou o trošku větší než 100%. Je to v pořádku - některé firmy si dopřály ten luxus, že byly zasaženy z různých zdrojů.

Ostatně ta čísla sama o sobě pro nás příliš velkou vypovídací schopnost nemají - virová situace v nadnárodním koncernu s nějakou tou stovkou tisíc počítačů (a tomu odpovídající přísnou administrací sítí a nasazením všech dostupných ochran) je asi o něčem trošku jiném než v typickém podniku u nás. Trend vymírání disket, stability downloadu a nárůstu infekce dorazivší mailem je ale zřejmý a bezpochyby platí i pro nás.

NOVÉ HROZBY A MODELOVÉ ÚTOKY (KRYPTOVIROLOGIE)

Zpracoval Ing. Jiří Mrnuštík
AEC, spol. s r .o.

Úvod

Problém ochrany dat se stává velmi rychle stále komplexnější. Před nedávnem ještě málokdo uvažoval o jiné než antivirové ochraně dat pro běžného uživatele.

Dnes na scénu vstoupily šifrovací programy, ochrana komunikací před cizíma očima, Internet jako fenomén s rozporuplným přínosem a ochrana proti makrovirům, které zcela převrátily logiku dřívějších návyků antivirové profylaxe.

Ochranné prostředky proti útokům na počítačová data se vyvíjejí závratným tempem. Bohužel, čím jsou dokonalejší a bezpečnější, tím (logicky) kladou větší nároky na hardware, uživatele a jeho svobodu. Jsou to právě znalosti a zkušenosti, které umožňují uživateli chránit se efektivně proti virům a přitom minimálně zatěžovat svůj systém.

Naprosto neodmyslitelnou vlastností ochrany IS se stávají digitální podpisy a šifrování. Zákony České republiky upravují i potřebu ochrany informací a připravovaný zákon o digitálním podpisu tuto skutečnost přenáší i do civilních sektorů a staví elektronický digitálně podepsaný dokument na úroveň tištěného dokumentu s notářsky ověřeným podpisem.

Cílem tohoto dokumentu je osvětlit některá nová nebezpečí v podobě virových a hackerských útoků nové generace a důležitost digitálního podpisu dokumentů a šifrování elektronických dokumentů.

1. Hodnocení současné situace

Nárůst používání Internetu, expanze mamutích společností a jejich sítí a výskyt makrovirů – to vše změnilo charakteristiku hrozby, kterou viry pro jednotlivé podniky představují. Dříve dominantní hrozba (tj. boot-sektorové infekce šířící se pomocí disket) není zcela vyloučena, ale přeci jen je dnes již zastíněna mnohem pronikavější hrozbou makrovirů šířících se pomocí e-mailu (elektronické pošty). V intranetovém „groupwarovém“ prostředí stovek připojených stanic může jeden neukázněný uživatel s nechráněnou stanicí způsobit lavinu infekcí. Finančně dost náročný správce sítě pak mrhá svým časem vysvětlováním uživatelům, proč jim na stanici antivirový program hlásí virus, a kde se tam vzal.

Kromě toho je zde ještě hrozba pro budoucnost, prezentovaná dynamicky se zavádějícími applety, kterou teprve pocítíme. Nicméně již nyní některé antivirové firmy do svých programů zakomponovaly detekci Java appletů a ActiveX objektů, které mohou působit škodlivě.

Řada produktů společnosti *Microsoft* představuje prostředí, ve kterém se virová infekce šíří nejrychleji.

Hlavními faktory, které k tomu přispívají, jsou:

- velká četnost sdílení dokumentů mezi uživateli,
- velké rozšíření produktů *Microsoftu.*
- *Visual Basic for Applications* (VBA). *Microsoft* nahradil jazyky *WordBasic* a *Excel Macro* novým programovacím jazykem, *VBA*, který běží ve všech aplikacích od *Office 97*

- Přímé spojování a prohlížení souborů přes *Hypertext Markup Language* (HTML).
- Možnost OEM použití jazyka *VBA* v rámci dalšího softwaru. Představme si situaci, že například společnost *AutoDesk* použije univerzální vývojový prostředek *VBA* pro psaní maker v systémech *CAD*.

2. Prognóza do budoucnosti

Přechod do informační společnosti sebou přináší další netušené možnosti pro získávání informací a rozvoj propojení. Ruku v ruce s tím jde i nové nebezpečí útoků. Dokonalé spojení pro výměnu informací je dvousměrné a přináší i stejně dokonalé propojení pro výměny virů.

Je třeba si uvědomit, že žádný antivirový program není schopen dopředu podchytit potenciální útoky tvůrců virů.

Celá řada faktorů – např. jak je navržen kus škodlivého kódu, technologie prostředí, ve kterém bude virus pracovat, a určité lidské procesy a chování – to všechno určuje schopnost života škodlivého kódu a schopnost jeho šíření. Vztah mezi typem škodlivého kódu a technologiemi, které potřebuje k přežití, je možné v historii virů vystopovat. Ochrana proti útoku škodlivého kódu je ve své podstatě obecně reaktivní (zpožděně reaguje na již vzniklou reálnou hrozbu).

3. Kryptovirologie – nové nebezpečí

Tradičně je použití šifer a jejich aplikace považováno spíše za záležitost defenzivní obrany, která poskytuje uživateli soukromí, autenticitu a bezpečnost.

Kryptologie ale může být v hackerském a virovém prostředí i velmi ofenzivní. Mám tím na mysli, že může být použita k útokům založeným na vydírání, které vedou ke ztrátě přístupu k informacím, ke ztrátě důvěrnosti a k úniku informací, tedy k tomu, čemu většinou kryptologie naopak zabraňuje. Potenciální hrozby a útoky s použitím kryptografie mohou vést i ke tvorbě škodlivého softwaru (viry, trojské koně, logické bomby apod.). Odtud je již jen krok k tomu, aby kryptologie vedla od antivirových ochranných vlastností k virovým a velmi nebezpečným koncům. Se znalostí kryptologie není totiž vůbec komplikované vytvořit a implementovat velmi nebezpečnou novou třídu virů – tzv. kryptoviry.

Možné útoky, které lze očekávat, spojují unikátní použití silných kryptografických technik (algoritmů s veřejnými klíči a symetrických šifer) s technologií počítačového viru a trojského koně. Tato nová technologie může umožnit nepřátelskému pisateli virů získat explicitní kontrolu přístupu k datům, ke kterým má jeho virus přístup.

To ukazuje, že viry mohou být použity také jako nástroje vydírání, potenciální kriminální aktivity, a jako munice v kontextu informační války, a nikoliv pouze tak, jak jsou tradičně chápány, tedy jako zdroj nepříjemností, vyrušování a finanční újmy.

Obecně definujeme kryptovirologii jako studium aplikace kryptografie na počítačové viry a ochranu proti nim.

Autoři virů se velmi snaží, aby učinili své produkty obtížně detekovatelnými, protože vědí, že uživatelé se pokusí virus odstranit v okamžiku, kdy jej najdou. Jinou metodou, zajišťující přežití počítačového viru, je vytvoření takového vztahu mezi virem a jeho hostitelem, že přežití viru se stává kritickým i pro přežití hostitele.

Představme si, že nás zajímá, jak učinit hostitele maximálně závislým na viru. S tímto cílem je použito právě šifrování. To znamená, že virus tím snáze přežije v hostiteli, čím více na něm bude hostitel kriticky závislý, a vliv viru na hostitele bude odstranitelný a napravitelný pouze autorem viru (tedy závislost je aproximována tím, že nyní je hostitel závislý na autorovi viru, nikoliv na viru samotném).

Tím je připravena půda pro vydírání, virové útoky, nevratné poškození dat apod. Takový virus lze detekovat, avšak není možno jej prostě smazat, nebo jej jinak bez pomoci jeho autora úspěšně odstranit, protože by došlo k nevratné ztrátě dat hostitele.

3.1 Kryptoviry

Čtyři takové kryptoviry, u nichž se zdá, že odrážejí snahu zůstat rezidentní po detekci, se objevily již v minulosti. Těmito programy jsou virus One_Half, virus LZR, trojský kůň AIDS Information a virus KOH.

Virus One_Half

Virus pracuje se zašifrováním pevného disku počínaje posledním cylindrem a pomalu se pohybuje dopředu o dva cylindry s každým resetem. To znamená, že po určitém počtu resetů je zašifrován již téměř celý disk. Používá symetrické šifrování a ukládá tajný klíč do sebe sama. Chcete-li se zbavit vlivu viru na hostitele, můžete získat klíč z virového kódu, a bez poškození virus odstranit a data obnovit.

Virus KOH

Virus KOH šifruje data hostitele algoritmem IDEA.

Virus LZR

Virus LZR přebírá kontrolu nad čtením a zápisy na pevný disk použitím relativně neznámého systémového volání. Zapisuje informace o opravě chyb na disk spolu s daty, i když ve skutečnosti není oprava chyb operačním systémem provedena. Všechny informace zapsané na disk jsou doprovázeny daty o opravě chyb, která zvolil virus. Jestliže je virus odstraněn, virová rutina nebude aktivována a informace na disku nebudou pro uživatele použitelné.

Poškození způsobené virem LZR je možné obejít zkopírováním všech poškozených souborů na diskety. Potom lze virus odstranit příslušným antivirovým programem bez ztráty dat. Rutina pro opravu chyb není v okamžiku zápisu na diskety aktivována, a proto lze virus takto obelstít. Ze znalosti funkce systému a ze znalosti práce viru se dá napsat specializovaný program, který by data opravil a virus odstranil.

Trojský kůň AIDS Information

I když trojský kůň AIDS Information není virus, má přece jenom vlastnosti podobné vlastnostem viru. Poskytuje informace o riziku setkání se s nositelem AIDS a asi po 90 restartech zašifruje uživatelův pevný disk. Uživatel je pak informován, že musí zaplatit poplatek za dešifrovací klíč. Tento trojský kůň představuje jeden z prvních vyděračských pokusů.

4. Modelové útoky

Modelovým útokem, který ukazuje opravdové nebezpečí virových útoků je například útok na databáze. Velmi drastické, nicméně velmi reálné je například napadení databázového systému nemocničních informací. Hypotetický virus (velmi podobný například viru Jack Ripper) je infiltrován do nemocničního informačního systému a velmi pomalu a postupně přehazuje v databázovém systému položku Jméno například tak, že zamění první se čtvrtou, pátou s osmou a podobně. Jde o velmi jednoduchý algoritmus, který ve svém důsledku povede ke dvěma výsledkům. Při trochu sofistikovanějším útoku bude ještě kontrolovat věk a další možné atributy, které útok udělají ještě méně odhalitelný.

Zaprvé databáze nebude jevit známky poškození, a proto se na útok s největší pravděpodobností nepřijde, nebo až za dlouho, a za druhé, podle kroku algoritmu, bude-li dostatečně dlouhý (ne každý čtvrtý, ale čtyřicátý) dojde k zdánlivě náhodnému selhání terapie a k procentuálně zvýšené úmrtnosti v dané nemocnici.

Děsivé na tomto útoku je, že bude-li dobře promyšlen, nemusí být vůbec odhalen a povede ve svém důsledku ke zhoršení pověsti nemocnice a ke zdánlivě náhodným úmrtím, zmrzačením při nežádoucích operacích a podobně.

Takový útok může být proveden kýmkoliv a virus se do systému může dostat mailem, hrou, spuštěním sexuálních či pornografických animovaných sekvencí, reklamou, jakkoliv.

Děsí Vás to? Mě ano.

Armádní informační sytém, který zobrazuje bojové situace v terénu, zaznamenávající pohyb nepřátelských, vlastních a neutrálních jednotek, je v dnešní době asi zcela reálnou skutečností. Hypotetický virový útok je zde ještě snazší a bude pravděpodobně veden přes útok na vojákovu psychiku. Vojáci, dlouho udržovaní ve stavu pohotovosti, s napjatými nervy a podobně, se rádi odreagují a jednou z možností je i provozování počítačových her a animovaných pornografických sekvencí. Alkohol a sex je velmi účinný útok na vojenskou mysl. V takové aktivní animaci schovaný virus bude vykonávat jednoduchou činnost změn barev na základě nějakého jednoduchého či složitějšího rozhodovacího algoritmu.

Všichni vědí, že modří jsme my a červený je nepřítel. Taková drobná barevná změna, ne příliš rozsáhlá, provedená při rekognoskaci před dělostřeleckou přípravou, může docela dobře demoralizovat vlastní řady. Jiný podobný útok, při kterém se mění barva neutrála na červenou může slibně vést k eskalaci konfliktu.

Takto do detailu promyšlené možnosti útoků a jejich zasazení do reálného, všem známého, světa ukazuje pisatele virů a hackery v trochu jiném světle. Nejsou to jenom neškodní podivíni, kteří občas způsobí nějakou finanční ztrátu. Jsou to společensky nebezpeční zločinci, kteří mohou v naší informační společnosti například i rozpoutat novou nukleární válku.

5. Způsoby ochrany

Existuje několik základních způsobů, jak si chránit informační systém jak před viry, tak před zneužitím informací a proti hackerským útokům.

Pro ochranu před útoky v takovém množství a „kvalitě“, jaké se očekává na základě boomu internetových propojení, je třeba nasadit speciální prostředky nad běžnou ochranu proti virům i proti ostatním útokům.

Je nezbytné podotknout, že žádná ochrana není stoprocentní a antivirové programy jsou vždy krok za novými virovými technologiemi.

Proto významnou roli ve vlastnostech nasazené ochrany bude hrát autentizace, kontrola neporušenosti a šifrování. Jinými slovy použité dokumenty, elektronickou poštu a distribuované soubory je třeba digitálně podepisovat a pokud možno i šifrovat.

Současně se softwarovými prostředky musí paralelně následovat i příslušná bezpečnostní politika.

Bezpečnostní šifrovací programy

Bezpečnostní šifrovací programy představují velmi diskutované pole celkem bezpečné ochrany. Problémem je, že je tu uvedeno slovo diskutované. Skutečné nasazení šifrovacího softwaru (a je třeba otevřeně říct, že nejde o žádný tzv. skrytě „bezpečnostní“ software a nebojme se slova šifra použít) je zatím v plenkách, a to zvláště v ČR. Pouze společnosti s nadnárodními mateřskými firmami a nebo společnosti, které již byly virovému, hackerskému nebo vyděračskému útoku podrobeny, začínají takový software instalovat.

Ostatní o šifrovacím softwaru jako prostředku ochrany dat a prostředku pro antivirovou prevenci, jen mluví. Doba však nazrává velmi rychle, a kdo bude chtít přežít, bude muset svoje data chránit moderními prostředky proti moderním útokům.

Základem tohoto typu (i antivirové) ochrany je zabránit neautorizovaným uživatelům v přístupu do počítače, v používání dat, která jim nepatří, zabránit modifikaci datových struktur na discích neautorizovanou osobou a autentizace používaného softwaru a přenášených dat tak, aby nemohlo dojít k podvrhu, který by mohl obsahovat některý z typů soudobých virových útoků. Jde například o datové soubory obsahující makroviry, podvržené programy s klasickými viry, bombami, trojskými koňmi a nebo časované vyděračské programy.

V poslední době se ve světě objevují útoky, které bychom mohli nazvat vyděračskými a virovými aférami v bankovních a vládních kruzích. Finanční instituce jsou tak nuceny k zaplacení ohromných částek často mezinárodním gangům tzv. cyber-teroristů, kteří těmto institucím vyhrožují (a mnohdy nejen planě), že zlikvidují jejich operační systémy a data. Banky, zprostředkovatelské firmy a investiční domy raději tajně platí výkupné, jen aby zabránily drahému zničení svých počítačových dat a především kolapsu důvěryhodnosti svých zákazníků.

O identitě tohoto nového útoku na počítače, spojeného nejen s anonymním virovým útokem, ale také s vydíráním a terorismem, se toho zatím moc neví. Útočníci zůstávají v anonymitě i proto, že poškozené instituce nejsou ochotny vést oficiální vyšetřování a ani prozradit, že byly cílem útoku, a už vůbec nechtějí prozradit jeho povahu. Takový průnik a zavirování počítačů snižuje kredit především finančních institucí a důvěru jejich klientů v bezpečnost svých uložených financí.

Protože neexistuje program, který by byl schopen podchytit všechny existující viry a možné podobné maligní útoky, je nasnadě, že jediným skutečným opatřením je prevence.

Prevence má dvě části, a to školení na jedné straně a donucení uživatelů nepoužívat neindentifikovatelné a nelegální zdroje softwaru a informací na straně druhé. Tuto skutečnost lze zabezpečit pouze jedinou cestou, a tou je použití asymetrické kryptografie a digitálního podpisu dokumentů.

Nezpochybnitelnost odesilatele, autenticita a kontrola nezměnitelnosti dokumentu či softwaru přináší silný preventivní prostředek ochrany i proti virům.

6. Závěr

Je třeba si uvědomit, že ochrana informací, kontrola jejich neporušenosti a autenticita vlastníka je jedním z nejdůležitějších prostředků ochrany IS. V současné době je navíc tato ochrana nejen podporována, ale dokonce vyžadována legislativními opatřeními státu.

Existuje dostatek řešení pro ochranu IS dodávaných firmami ze zahraničí. Jejich nespornou nevýhodou je nedosažitelnost takové firmy na území státu, uzavřenost řešení a v neposlední ředě i exportní regulace, platící v některých oblastech světa.

Základní nevýhodou však je skutečnost, že software je dodáván „jak je ..as is“, což neskýtá důvěru v jeho bezchybnou implementaci a především v to, že neskrývá nějaká zadní dvířka pro rozkrytí zašifrovaných informací.

Naopak nespornou výhodou lokálních firem je jejich flexibilita, která umožňuje do určité míry přizpůsobovat software specifickým požadavkům odběratele.

Nezanedbatelnou výhodou je i možnost kontrolované implementace šifrovacího algoritmu na míru dodaného přímo odběratelem.

JAKÉ VÝZVY ŘEŠÍ ANTIVIROVÉ A „IT SECURITY“ FIRMY

Miloš Kuchař
AEC, spol. s r.o., milos.kuchar@aec.cz

Problematika počítačových virů je jedna z mála lidských oblastí, kde se výsledky z oblasti výzkumu a vývoje dostávají do reálného světa během několika dnů nebo dokonce hodin. Je to věčný závod mezi výrobci virů a antivirů. Síly však nejsou vyrovnané. Zatímco tvůrců virů může být prakticky neomezené množství, tvůrců antivirů může být jen tolik, kolik jih uživí jejich zákazníci. A protože se neustále vyvíjení běžně používané operační systémy a programy, jsou také tvůrci virů stále o krok dopředu. A držet minimální odstup mezi výrobcem virů a antivirů je právě onou základní výzvou pro antivirové firmy. Rychlost reakce je oním základním předpokladem pro úspěch antivirové firmy. Tyto kvality lze posuzovat například na základě nezávislých testů antivirových motorů, tj. schopností detekovat, ale také odstraňovat konkrétní viry s minimálními možnými následky.

„Národní viry neexistují“

Největším problémem antivirových firem paradoxně není psaní antivirových programů, ale získávání nových vzorků virů, jejichž detekci by programátoři mohli přidat do motoru antivirového systému. Dnes, kdy čas šíření virů lze počítat na hodiny je například pro české vývojáře problémem dostat se k „funkčním“ vzorkům viru dříve než zachvátí jejich uživatele. Dále postupem času padá argument českých producentů, že české firmy by měli používat české antivirové programy, protože tyto lépe detekují „české“ viry. Důvod je prostý. Dnes je nejlepší živnou půdou pro šíření virů Internet, který nezná hranic. A díky tomu nebezpečí napadení virem vzniklým v Čechách je prakticky totožné, jako pravděpodobnost napadení virem, který vznikl v kterékoli jiné zemi.

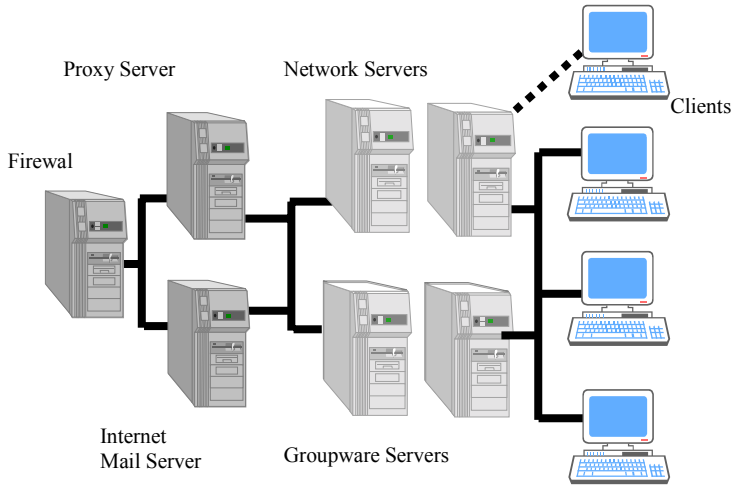
Platformy

Mezi hlavní problémy menších (řekněme národních) antivirových firem je kromě získávání vzorků virů pro studium také implementace antivirových programů do celé škály platforem. Každý zákazník je jiný, každý má jinou strukturu sítě a používá jiné programy. Protože je však velice náročné vyvíjet současně antivirové systémy pro mnoho, někdy i zcela odlišných, platforem. A zde se uplatní pouze opravdu silní výrobci s rozsáhlými programátorskými týmy.

Centrální instalace a aktualizace:

Pokud se zeptáte uživatele, jak si představuje ideální antivirový systém, odpoví vám, že ideální bude takový, který by žil svým vlastním životem. Jinými slovy takový, který by nevyžadoval žádnou práci administrátorů sítě a byl schopen samostatně řešit všechny pokusy o průnik viru do sítě. V praxi to znamená, že by se sám udržoval v aktuálním stavu, byl by centrálně nainstalovaný a pokrýval všechny kanály, kterými by se viry do systému mohly dostat.

Abychom se mohli této představě přiblížit, musíme k antivirovému motoru přidat síťovou nástavbu, která se bude starat o spolupráci jednotlivých částí systému dohromady. Ta má na starosti šíření aktualizací z centra do všech částí systému a také systém hlášení o detekovaných virech z jednotlivých částí systému.



Podepisování aktualizací antivirového systému

Pro bezpečnost celého systému je důležité, abychom zaručili častou aktualizaci antivirových update od výrobce. A protože díky Internetu je rychlost šíření nových virů dnes závratná, je nutné, aby i antivirový systém byl aktualizován minimálně jednou týdně. A tak se přímo nabízí jednoduché řešení – tj. aktualizovat antivirové systémy také po Internetu. To však s sebou přináší i mnohé problémy. Internet totiž ve svém jádru nenabízí žádné prostředky pro autentizaci přenášených dat. Proto pokud jsou aktualizace stahovány pouze prostřednictvím služby FTP, existuje zde reálné nebezpečí, že v dobré víře stáhneme data z úplně jiného serveru a ty spustíme v naší lokální síti. Pokud by tento server byl například podvržen hakerem, mohl by se stát dobrou základnou pro šíření jeho nového viru nebo trojského koně. Takovéto počínání by pak mohlo zničit nejenom data v síti zákazníka, ale samozřejmě také pověst antivirového systému, jehož server byl napaden. Jediným účinným způsobem, jak tomuto nebezpečí čelit je možnost digitálně podepisovat rozesílané aktualizace. Na straně příjemce se nejprve digitální podpis ověří a teprve poté se povolí instalace nového update do systému. Díky tomu získá uživatel jistotu, že data nebyla během jejich transportu změněna a že skutečně pocházejí od jejich poskytovatele antivirového systému. V dnešní době se stejným způsobem zabezpečují i licenční klíče k prodanému software.

Nové technologie

Jednou z velkých výzev pro antivirové firmy je zamezení šíření nových specifických typů virů, které se šíří elektronickou poštou přes Internet. Problémem je, že každý z těchto virů používá jiné technologie a především to, že rychlost jejich šíření je nesmírná. Jsou schopny během několika hodin zachvátit prakticky celou planetu. A účinné zamezení těmto elektronickým teroristům je v současnosti prakticky největší výzvou antivirovým firmám.

Závěr

Jak vidíme, před antivirovými firmami stojí řada výzev. Ta největší však zůstává již řadu let. A to je osvěta mezi uživateli počítačů. Ve chvíli, kdy je počítač uživatele infikován, je pomoc antivirových firem mnohdy neúčinná, protože prostě není co zachraňovat. Dále stojí za pozornost, že, i když se pokusíme vyjmenovat výzvy firmám vyvíjející antivirové systémy dnes, můžeme si být prakticky jistí, že budou jiné, než za půl roku. Před vývojáři antivirových systémů se stále otevírají nové a nové dveře, za kterými se skrývají další a další výzvy.

"HORROR SHOW"

Ing. Jiří Mrnuštík
AEC, spol. s r.o.

Jaké jsou každodenní bezpečnostní problémy?

- Viry
- Neautorizovaný přístup k datům
- Sniffing
- Cracking hesel

Proč se bezpečnostní problémy objevují?

- Nejslabší článek jsou lidi
- Hlavní a nejpoužívanější programy mají bezpečnostní díry
  - Word
  - Excel
  - Outlook
  - Windows
  - Sendmail
  - Apache
- Slabá kryptografie je široce rozšířena a lidi jsou hlavními producenty tohoto paskvilu přesvědčování o její dostatečnosti.
- Síťové prostředí není bezpečné
- Data nejsou ukládána bezpečně
- Není zaručena dobrá autentizace

Nešifrovaná data

- Jestliže máte přístup do počítače, můžete ukrást data na něm uložená
- Ukradení laptopu se stává stále častějším případem
- Windows NT nenabízí žádnou ochranu

Hesla

- Heslo je jako kartáček na zuby
  - pravidelně je měňte
  - s nikým je nesdílejte
- Dobrá hesla...
  - minimálně 8 lépe více jak 13 znaků
  - obsahuje speciální znaky
  - nesmí být obsaženo ve slovníku
  - musí se snadno pamatovat
  - **"stupidní#nudný šéf "Práce_mi_sakra_smrdí...!**

Techniky pro narušení bezpečnostni

- DNS Spoofing
- UDP Packet Storms
- Odhadování TCP číslování
- Obcházení Firewallů
- SNMP díry
- Zranitelnost vzdáleného vytáčení
- Přednastavená hesla dodavatelů
- ICMP Reset
- **Socialní inženýrství**
  "Tady je IT manager z oddělení v New Yorku. Co to sakra máte za problém ve vašem systému? Nemohu se dostat do databáze objednávek! Klient čeká v zasedačce a pokud se mi to ihned nepodaří, půjde utratit peníze ke konkurenci.

Trochu demonstarce

- Excel macro virus
- Objevení hesla
- Sniffing
- .....

VIRY EXISTUJÍ (ZKUŠENOSTI Z PRAXE)

Igor Hák
www.viry.cz

1. PC Viruses in the Wild

Na začátek bych rád řekl, s jakými viry se vůbec v praxi můžeme setkat. Hodně může napovědět například seznam „PC Viruses in the Wild“, který obsahuje takzvané In-the-Wild viry. Pojem In-the-Wild, což v češtině znamená „v divočině“ označuje viry, které jsou v praxi nejvíce rozšířené. Tento seznam je vlastně souhrnem hlášení z celého světa. Českou Republiku zastupuje Pavel Baudiš (Alwil) a pokud se v seznamu vyskytuje i virus, u jehož názvu jsou uvedeny písmena „Pb“, je zřejmé, že se tento virus vyskytuje i na území ČR. Seznam In-the-Wild vychází každý měsíc a často se stává základem pro srovnávací testy antivirů, které provádí například časopis Virus Bulletin.

Kousek seznamu „PC Viruses in the Wild“

Již ze zmiňovaného seznamu je zřejmé, že nejrozšířenější jsou makroviry a to nejčastěji pro aplikaci Microsoft Word 97 či Word 2000. Méně rozšířenou skupinou jsou souborové viry pro Windows 95, 98, NT či 2000. Patří sem i červi, které se šíří prostřednictvím emailů. Červa však nelze v tomto případě označovat jako virus, ale spíše jako „křížence“ trojského koně a viru. Do postupně mizející skupiny virů patří především ty, které jsou určeny pro operační systém DOS.

2. Makroviry

Nejprve bych se důkladněji věnoval makrovirům. Většina produktů kancelářského balíku Microsoft Office obsahují takzvanou „antivirovou ochranu maker“ (verze 97), či „zabezpečení“ (verze 2000). I když se názvy odlišují, v obou případech jde o stejnou věc. Tato vymoženost umožňuje zablokovat aktivaci případných maker v otevíraném dokumentu a zabránit tak i případné aktivaci makroviru (makrovirus je jak známo složen právě z takových maker).

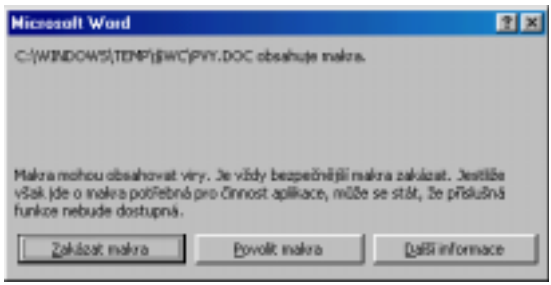
V MS Office 97 má ochrana pouze dvě polohy:

- Vypnuto – uživatel není o existenci maker vůbec informován – jsou automaticky spuštěna.
- Zapnuto – uživatel musí vždy rozhodnout, zda případná makra zakáže, či je provede.

V MS Office 2000 má zabezpečení tři stupně:

- Vysoké – automaticky je zakázáno spouštění všech maker. Uživatel se nemůže ani nijak jinak rozhodnout.
- Střední – ekvivalentní k poloze Zapnuto v MS Office 97.
- Nízká – ekvivalentní k poloze Vypnuto v MS Office 97.

V MS Office 97 i 2000 je ochrana standardně nastavena na maximum, a tak není makrovirus prakticky vůbec schopen se v tomto prostředí šířit. Až po zásahu uživatele do nastavení, má makrovirus větší šance. Pokud je ochrana MS Office 2000 nastavena v poloze Střední, stačí již jedno zaváhání uživatele a makrovirus se v systému pohodlně „usadí“. Většina makrovirů navíc tuto ochranu vypíná, např. vhodnou modifikací registrů Windows, či přímo zásahem do nastavení programu.



Pokus o otevření dokumentu, který obsahuje makra (MS Office 2000 – Zabezpečení: střední)

Makroviry pro Word 97 toho můžou například dosáhnout následujícími příkazy:

- *Options.VirusProtection = False*
- *System.PrivateProfileString("", "HKEY_CURRENT_*

  USER\Software\Microsoft\Office\8.0\Word

  Options", "EnableMacroVirusProtection") = "0"

Kromě toho se makrovirus většinou po aktivaci snaží trvale usídlit v systému. K tomu mu poslouží globální šablona *NORMAL.DOT*, která se automaticky spouští po startu Wordu. V případě Excelu stačí infikovaný list uložit do adresáře *XLStart*, který se nejčastěji vyskytuje v *C:\Program Files\Microsoft Office\Office*.

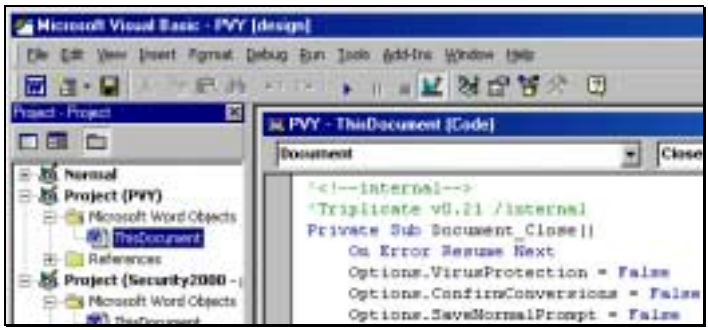
2.1. Příznaky napadení makrovirem

Jaké jsou příznaky napadení makrovirem ? Třeba právě vypnutá ochrana maker (pokud ji nevypnul uživatel záměrně). Pokud tomu tak je, doporučuji:

- Antivirovou ochranu maker opět zapnout, či nastavit na nejvyšší úroveň.
- Vypnout a opět aktivovat postiženou aplikaci (Word, Excel).
- Znovu se podívat na nastavení ochrany maker.
- Pokud je opět vypnutá, za vším stojí s největší pravděpodobností makrovirus a je dobré pokračovat následovně:
- Smazat globální šablonu *NORMAL.DOT* v případě Wordu, či vyprázdnit adresář *XLStart* v případě Excelu.
- Spustit Word, Excel – podle situace.
- Antivirovou ochranu maker opět aktivovat.
- V případě, že se u libovolného otevíraného dokumentu zobrazí dialog informující o existenci maker, zvolit „zakázat makra“ a dokument uložit ve formátu *RTF* (tj. menu *Soubor/Uložit jako…*/ - typ souboru: *RTF*).

Převodem do formátu *RTF* jsou odstraněna veškerá makra z dokumentu, tedy i případná makra viru.

Většina dnešních makrovirů využívá techniku „*Class*“, díky níž ukládají svoje tělo do modulu *ThisDocument* (Word 97/2000) či *ThisWorkBook* (Excel 97/2000). To má za následek, že makra viru nejsou vidět v menu Nástroje/Makro. Tělo takového makroviru lze snadno odhalit přes menu *Nástroje/Makro/Editor jazyka Visual Basic*, kde stačí „poklepat“ myší na objekt *ThisDocument* popřípadě *ThisWorkBook*.



Ukázka jednoho z makrovirů řady Class – O97M/Triplicate v objektu ThisDocument.

3. Červi – Internet Worms

Počítačový červ je vlastně „křížencem“ viru a trojského koně. Po viru zdědil replikační schopnosti a od trojského koně schopnost obejít se bez hostitele – červ tak není připojen k žádnému původnímu souboru.

Červi se, jak známo, šíří prostřednictvím e-mailových zpráv, ke kterým jsou nejčastěji připojeni ve formě souboru, v několika málo případech jsou vnořeny přímo ve zprávě – ve formě VBSkriptu. V tomto případě je nutné, aby e-mailový klient podporoval příjem v HTML formátu.

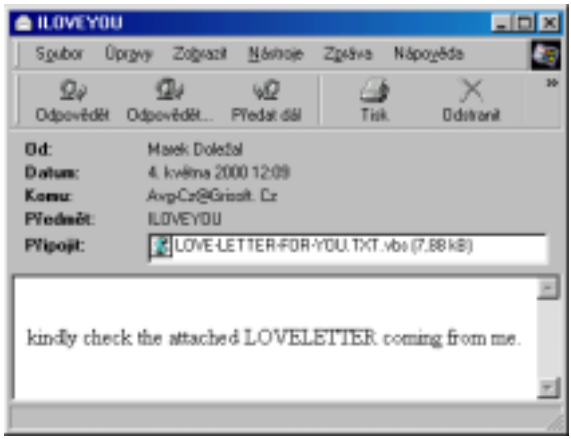
V dnešní době lze rozdělit červi například následovně:

- Červi nezávislí na použitém poštovním klientovi
- Červi závislí na použitém poštovním klientovi

První skupinu zastupuje například červ *Haiku*, který kromě skládání veršů hledá emailové adresy dalších obětí v některých souborech po celém disku. Na získané emailové adresy pak hromadně, za účasti SMTP protokolu, odesílá svoje kopie (tj. soubor *haiku.exe*, který tvoří attachment – přílohu emailové zprávy). Červ *Happy99* (alias *Ska*) pro změnu modifikuje soubor *WSOCK32.DLL* tak, aby se při volání služeb *Connect* a *Send* aktivoval kód červa, který připojí svoje tělo k odesílanému emailu.

Do druhé skupiny pak patří především všechny typy makrovirů, které jsou založeny na principech makroviru *W97M/Melissa*. Některé antiviry přidávají na konec takových makrovirů označení *@mm*. Patří sem i *VBS/LoveLetter* (*I_Love_You*).

Tyto lidské výplody jsou závislé především na klientu MS Outlook, který je součástí kancelářského balíku MS Office 97, 2000. Majitelé "odlehčeného" Outlooku, tj. Outlooku Express, mohou zůstat v klidu. Nebudou šířit infekci na další počítače, o infekci vlastního počítače však přijít nemusí, záleží, zda přílohu spustí, či ne.



MS Outlook Express 5 a setkání s červem VBS/LoveLetter.

Jak už bylo řečeno, červi se nacházejí v souboru samostatně a nepotřebují žádného hostitele. Antivirové programy tak ve většině případů mažou všechny soubory, které si červ pro svůj chod v systému vytvořil. Nevracejí však do původního stavu registry Windows, popřípadě soubory, které červ zmodifikoval tak, aby si zajistil včasnou aktivaci po každém startu operačního systému Windows.

Většina červů si zajistí automatické spuštění nejčastěji:

- pomoci modifikace registrů.

- pomoci modifikace souboru *WIN.INI* nebo *SYSTEM.INI* (v adresáři s instalací Windows).

K chaosu, kterému se říká "registry", lze přistoupit například pomoci příkazu *regedit.* Červi mají v oblibě především klíč:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

V něm vytvářejí nové položky s údaji obsahující cestu k souboru, který se pak při každém startu Windows aktivuje. Mezi další využívané klíče patří především:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

V souboru WIN.INI je občas pod útokem červa řádek *RUN=* v sekci *[WINDOWS].*

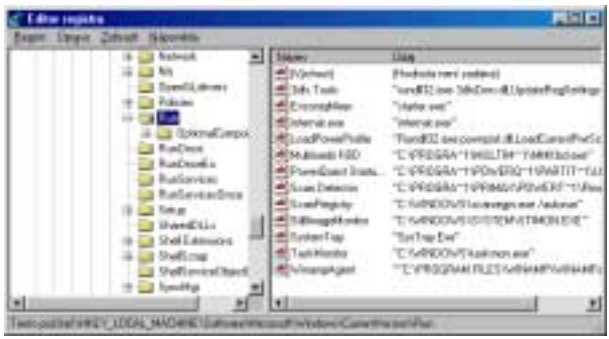
Podobně je na tom může být i sekce *[BOOT]* s řádkem *SHELL=* v souboru *SYSTEM.INI.* Za sekvencí znaků *RUN=* se zpravidla nic nenachází. Pokud ano, může to být známka toho, že na počítači je / byl červ. Nemusí se však vždy jednat o červa, občas tyto možnosti využívají i některé užitečné programy.

Za řádkem *SHELL=* se pak běžně vyskytuje pouze příkaz *EXPLORER.EXE.*

3.1. Jak se zbavit případného červa

Ještě před tím, než se antivirem odmažou infikované soubory, doporučuji odstranit škody v registrech, popřípadě ve *WIN.INI* či *SYSTEM.INI*. Tento postup je někdy nutné dodržet. V případě červa *PrettyPark* se totiž může stát, že díky špatnému postupu, nebude spuštění programu *regedit*, který je východiskem ze situace, možné. Taky je nutné zjistit, co že to máme z registrů vůbec odstranit. Posloužit můžou některé „Virové encyklopedie“, kterých je ve světě Internetu hned několik desítek (www.viruslist.com, www.sarc.com). Detailní popisy, i když ne v takovém množství lze najít i v češtině – www.viry.cz, www.asw.cz, www.grisoft.cz.

Dalším krokem je záloha stávajících registrů. Je dobré zálohovat soubory *C:\WINDOWS\SYSTEM.DAT* a *C:\WINDOWS\USER.DAT*, které se pak budou hodit v případě nezdaru.



Jeden z životně důležitých klíčů v registrech. Stav před infekcí červem VBS/LoveLetter.

A stav po infekci. V klíči přibyl řádek MSKernel32 – za jeho vznikem stojí červ VBS/LoveLetter.

V případě infekce červem *VBS/LoveLetter.A,* lze dále postupovat například následovně:

- spustit utilitu regedit (menu Start/Spustit).
- dostat se v levé části okna až do větve / klíče: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- (v řadě případů stačí pouze 6x správně poklepat levé tlačítko myši).
- v pravé části okna označit kliknutím myši řádek MSKernel32, kde sloupec „údaj“ ukazuje na soubor MSKernel32.VBS.
- tlačítkem DEL tento vybraný řádek odstranit.

Podobný postup je nutné zopakovat i v klíči:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

Zde je nutné odstranit řádek s názvem *Win32DLL,* který ukazuje (sloupec „údaj“) na soubor *Win32DLL.VBS.*

Po modifikaci registrů, popř. souborů *WIN.INI*, *SYSTEM.INI* (platí i pro drtivou většinu červů) je vhodné celý systém Windows restartovat a pak již antivirem odstranit všechny soubory, které si s sebou červ přinesl.

4. Souborové a další viry

4.1. Viry pro DOS pod Windows

Výskyt virů, které jsou napsány pro operační systém MS DOS již není v této době příliš běžný. Prsty v tom má především operační systém MS Windows 9x/NT. Viry, které jsou napsány pro operační systém MS-DOS, se mohou pod MS Windows 9x/NT chovat následovně:

- fungují korektně, Windows jim nevadí.
- fungují jen „na půl“. Něco, co by měli dělat, nedělají.
- nefungují vůbec.

K první jmenované skupině není prakticky co dodávat. Všechny DOS viry pod Windows samozřejmě mají svá omezení. Dokáží se šířit jen v „DOSovském okně“, ve kterém běží nějaká aplikace pro DOS. Typickým příkladem může být souborový manažer M602. Společně s uzavřením okna končí i život viru. Důležité je poznamenat, že souborový virus pro MS DOS se šíří pouze v rámci jednoho DOS okna, ve kterém byl aktivován. Pokud je souborový virus spuštěn přes nějakou aplikaci typu „Průzkumník“ (Explorer), nemá šanci. O něco větší šance má souborový virus, který se stačí zavést dříve, než samotný operační systém Windows. To si může zajistit například napadením souboru WIN.COM. Pokud se tak stane, dokáže se takový virus šířit v jakémkoliv „DOSovském okně“. Má to však i jednu nevýhodu. Monstrum, jakým je Windows, totiž kvůli tomuto „drobečku“ – viru, musí naběhnout v daleko pomalejším režimu, který vyhovuje viru. Windows 95 na tento fakt dokonce vůbec neupozorní. Windows 98 už ano:

Po stisknutí tlačítka ANO se zobrazí trošku detailnější informace:

K zmiňovanému problému samozřejmě dochází pouze v případě, že se jedná o paměťově rezidentní souborový virus pro DOS, či boot virus, který je vždy paměťově rezidentní.

Další skupinou jsou viry, které pracují „na půl“. Do této skupiny patří například klasický virus OneHalf.3544, který pod operačním systémem MS DOS napadá soubory pouze na disketách. Na pevném disku se zajímá pouze o jeho zaváděcí sektor. V případě, že je nedostupný, napadá soubory i na disku. To je i případ Windows. OneHalf tedy pod Windows napadá pouze soubory – zaváděcí sektor pevného disku je nepřístupný.

Poslední jmenovaná skupina virů to řeší s Windows rychle a rázně. Po spuštění takového viru obdržíme ihned zprávu o chybě v chodu programu.

DOS viry doporučuji odstraňovat pomocí „bootovací“ diskety, která by měla kromě základních nástrojů (*FORMAT, FDISK* atd.) obsahovat i antivirový program.

4.2. Win32 viry aneb viry přímo pro Windows

První Win32 viry se začaly objevovat až s příchodem Windows 95. Za těch několik let posbíraly řadu věcí od svých starších „bratříčků“ pro operační systém MS DOS. Dodnes však platí, že drtivou většinu Win32 virů lze odstraňovat v režimu MS-DOS (menu *Start/Vypnout/Restartovat v režimu MS-DOS*). Nejlepší je samozřejmě použít „bootovací“ disketu, či dokonce „bootovací“ cédéčko.

5. „Igiho stránka o virech“ – www.viry.cz

„Igiho stránka o virech“ je jedna z nejrozsáhlejších webových stránek na českém Internetu, která se zabývá problémem počítačových virů. Stránka existuje již více než dva roky a za tu dobu se toho hodně změnilo. Původně se jednalo o ne příliš často aktualizovanou webovou stránku. Důvod byl jednoduchý, neměl jsem modem.

Dnes ho již mám a tak mohu reagovat na virové, ale i ostatní novinky prakticky okamžitě. Jistou brzdou jsou však telefonní poplatky Českého Telecomu. Jako jediný člověk, který na „Igiho stránce o virech“ pracuje, musím tomuto koníčku věnovat hodně času. Na existenci stránky mají zásluhu i její čtenáři, kteří mě svou návštěvou utvrzují v domnění, že celou tu práci nedělám jen pro sebe. Je opravdu příjemný pohled na statistiky návštěvnosti obzvláště v době, kdy „řádí“ nějaký rozšířený virus (*Win95/CIH*, *VBS/Loveletter*, *W97M/Melissa* apod.). Na existenci má významný podíl i služba www.woko.cz, díky níž jsem u všeho včas.

„Igiho stránka o virech“ v dnešní době nabízí:

- aktuální novinky o virech/antivirech.
- knihu o virech – elektronické informace o všem, co se virů / antivirů týče.
- popisy nejrozšířenějších virů.
- recenze antivirových programů – tak, jak je vidím já.
- rozhovory s antivirovými experty, ale i s lidmi, kteří viry píšou. V ČR existují tři lidé, kteří aktivně píšou viry - Benny, Prizzy, Mort. Nutno podotknout, že některé jejich viry vynikají i v celosvětovém měřítku.
- rozsáhlou sbírku univerzálních antivirů.
- výsledky srovnávacích testů, jinak prakticky nedostupného časopisu Virus Bulletin.
- možnost přihlásit se do emailové konference o virech & antivirech, ve které je dnes přihlášeno skoro 300 lidí včetně odborníků s českých firem Alwil, AEC, Grisoft. Zastoupen je i slovenský Eset (výrobce antiviru NOD).

Úvodní stránka „Igiho stránky o virech“ – www.viry.cz

HROZBY HACKERŮ INFORMAČNÍM SYSTÉMŮM, AKTUÁLNÍ PROBLÉM DETEKCE PRŮNIKU

Doc.Ing. Jaroslav Dočkal, CSc., Ing. Josef Kaderka, Tomáš Bouček
všichni Vojenská akademie Brno

První část článku popisuje, v čem je výpočetní systém zranitelný, druhá část článku je věnována typům útoků hackerů, třetí část je věnována problémům s použitím bezpečnostních mechanismů a nástrojů proti útokům ze sítě a čtvrtá (poslední) část popisuje řešení aktuálního problému jednoho ze síťových bezpečnostních mechanismů - návrh standardu formátu výměny informací o detekci průniku.

1. V čem je výpočetní systém zranitelný

Zranitelnost výpočetního systému má svůj původ již v etapě jeho návrhu. V [Knig00] jsou rozlišovány čtyři typy zranitelných míst výpočetních systémů, v závislosti na tom, kdo je cílem a jak rychle působí:

	Cíl je osoba	**Cíl je počítač**
Okamžitý účinek	Sociální inženýrství	Logická chyba
Potřebuje delší čas	Nedostatky bezpečnostní politiky	Slabina

Logická chyba je většinou taková chyba, která umožňuje neoprávněný přístup k výpočetnímu systému. Jedná se o různé omyly a chyby při programování a při návrhu programů. V současné době jsou programy navrhovány se zřetelem na bezpečnost, ale s jejich rostoucí komplexnost se zvyšuje riziko, že se nepodaří vše uhlídat. Jakékoliv výhody pro uživatele jsou výhodami i pro útočníka, mnohdy tedy dobré úmysly mají za následek velké bezpečnostní díry. Logická chyba se od slabin odlišuje tím, že logická chyba je absolutní nedostatek bezpečnosti, která byla buď špatně zajištěna anebo úplně opomenuta při návrhu. Od sociálního inženýrství se liší tím, že nepotřebuje žádnou reakci od uživatele, protože vše nutné ke zneužití zranitelnosti se vyskytují na počítači oběti a nebo na síti.

Můžeme je rozdělit na:

- Chyby operačních systémů – většina lidí si myslí, že špatná administrace systému vede k umožnění přístupu hackerů do systému, ale není to vždy jen chyba administrátora. Velké množství problémů vzniká chybami, které jsou ve vlastním operačním systému. Velmi známé jsou chyby typu přetečení vyrovnávacích pamětí, které umožňují podstrčení části kódu systému. Chyby operačních systémů jsou nejpřímějšími metodami útoku, mají okamžité výsledky a předvídatelné výsledky. Navíc stejný problém je na všech počítačích se stejným operačním systémem, což vede k částečné univerzálnosti útoku.
- Chyby aplikací – aplikací může být cokoliv od hry až po webový server. Někdo je musel naprogramovat a administrátor si nemůže být jist, zda to náhodou nebyl někdo, kdo nemá ani ponětí o bezpečnosti a kdo tedy může ohrozit jeho systém. Chyby aplikací se většinou nemohou projevit kdykoliv, ale pouze při splnění určitých podmínek. Základní podmínkou pro útočníka je, aby obět spustila danou aplikaci.
- Síťové protokoly – většina systémů věří informacím, které přijdou od jiných systémů, což velmi jednoduše umožňuje „spoofing“ (vydávání se za někoho jiného).

- Zneužití vnucené důvěry – jde zřejmě o jeden z největších problémů počítačové bezpečnosti. Pokud znáte někoho, kdo vám věří, a pokud jemu věří zamýšlená oběť, pak to znamená, že je asociativně zranitelná. Síť důvěry se samozřejmě netýká pouze lidí. Administrátorský přístup umožňuje přístup k počítači na nízké úrovni a správa těchto přístupů si vytváří vlastní síť důvěry.

Slabina je chyba na systému, která může vést k průniku. Typické příklady ohrožených částí jsou:

- ochrana díky obtížnosti – není to zabezpečení, které by odstranilo chybu, ale pouze stíží možnost jejího využití;
- kryptografie – je to jedna z nejdůležitějších částí počítačové bezpečnosti, avšak je to přídavné zabezpečení, s vlastními slabinami. Každá šifrovací technika se potýká s těmito problémy
    - šifrovací zkratky – hodně typů šifrování je oslabeno použitím optimalizací a zkratek kvůli rychlosti. Kryptografie je takový druh výpočtů, u kterých je lépe postupovat pomalu než rychle. Pomalejší metody šifrování jsou většinou méně náchylné k dešifrování než metody rychlejší;
    - rychlost počítače – každá šifra a délka jejího klíče je navržena s ohledem na rychlost počítače. Pokud by byla příliš pomalá, nedala by se ve většině aplikací použít. Pokud by byla příliš rychlá, byla by málo bezpečná;
    - nutnost dostatečně náhodného klíče – pokud by se dal jednoduše zopakovat postup, pomocí něhož bylo získáno náhodné číslo, byla by šifra příliš slabá, protože by nebyl problém duplikovat šifrovací klíč;
- zabezpečení heslem – zde jde evidentně o největší slabinu celého zabezpečení. Většina lidí si kvůli zapamatování zvolí takové heslo, které je lehce uhodnutelné a útočníkovi potom stačí vzít slovník běžných hesel a zkoušet. Celé šifrování tedy může být úplně k ničemu, pokud je jako jeho základ zvoleno lehce uhodnutelné heslo;
- kontrolní součty vytvořené pomocí hash algoritmů (např. MD5). Problémem ale může být, že hašovací algoritmus, který nejsou dnešní počítače schopny dekódovat, může být za deset let nepoužitelný;
- zastaralý software, zastaralý hardware – v každém produktu se časem najdou nějaké chyby, dobrým příkladem mohou být operační systémy, kde se u každého najde v průběhu každého roku několik desítek až stovek chyb;
- lidé – největší slabina jakéhokoliv zabezpečení. Lidé trvají na konvencích, které jsou často v rozporu s bezpečnostními zájmy svého zaměstnavatele, jsou také ovlivnitelní sociálním inženýrstvím; dalším problémem jsou sabotáže a korupce.

Sociální inženýrství je založeno na získání přístupu do počítačového systému prostřednictvím komunikace s lidmi, kteří si myslí, že poskytují informace někomu důvěryhodnému. Tyto informace použijete, abyste získali od jiného člověka další informace.

Nedostatek v bezpečnostní politice spočívají v tom, že se zapomíná na naplánování potřebných opatření vůči všem rizikovým situacím. Typickými oblast přehlédnuté oblasti jsou

- obnova dat – důležitým základem je vytváření záloh všech potřebných dat, útočník může data změnit nebo úplně zničit, a pak je nutné data rychle obnovit. Pro zálohování dat je

k dispozici velmi mnoho specializovaného software a stačí jen vybrat vhodné řešení pro danou organizaci;

- obnova poškozeného hardwaru – to, že hardware je chybový, ví každý, navíc jeho selhání mohou způsobit další faktory jako je požár, voda, elektrický výboj, fyzické zničení a mnoho dalších. Je tedy jej nutné v případě selhání rychle nahradit jiným. Například pokud je třeba zajistit naprosto spolehlivou činnost serverů, je vhodné zvolit clusterové systémy, kde pokud jeden ze serverů v clusteru vypadne, tak jsou ostatní funkční dál a lze provést výměnu hardware;
- nalezení vetřelců – na zjištění vniknutí do sytému je nutné reagovat okamžitě. Ačkoliv samozřejmě nevíme, co útočník v daný okamžik dělá, je nutné jej lokalizovat a zabránit v proniknutí do dalších systémů organizace;
- vyšetření nařčení organizace z útoku na někoho jiného – i do této situace se (bohužel) někdy můžete dostat. A často je pak problém zjištění, kdo je za tuto situaci odpovědný. Je tedy nutné mít přehled, jaké zaměstnance organizace zaměstnává a především o jejich případných problémech se zákonem. A tedy mít připravené postupy vedoucí ke zjištění viníka a omezení možnosti jeho lhaní;
- žaloba na vetřelce – nemusí být těžké odhalit identitu vetřelce, ale mnohem větší problém je jeho usvědčení u soudu, což může stát organizaci velmi mnoho peněz. Tento důvod vede mnoho organizací k tomu, že takové útoky na své počítačové systémy nehlásí a útočníci zůstávají nepotrestáni. Druhým důvodem, který řadu firem vede k „zametání problému pod koberec“, je obava o jejich pověst;
- žaloba na kriminálně činné zaměstnance – pokud zaměstnanec provádí v pracovní době soukromou činnost, která se navíc ukáže jako kriminální, pak je vhodné spolupracovat s policií a poskytovat jí potřebné informace;
- oznámení vetřelců a kriminálně činných zaměstnanců příslušným agenturám – pokud dojde k průniku do počítačového systému, je vhodné toto oznámit organizacím, které se tímto zabývají. Ve světě se takovéto organizace označují jako CERT (Computer Emergency Response Team), autorům příspěvku zatím o existenci takového týmu v České republice není nic známo. Je ale nutné vědět, že i kdyby někdo takovýto tým u nás vytvořil, nikdy nepůjde o orgány činné v trestním řízení a že i tak je vždy nutné kontaktovat i policii, příp. jiné vyšetřovací úřady;
- fyzická ochrana sítě – je nutné zabezpečit přístup pouze dostatečně identifikovaným zaměstnancům, důsledné zamykání chráněných prostor, omezené přístupy zaměstnanců k informacím atd. Zaměstnancům je nutné vnutit správné návyky a dbát na jejich dodržování, protože mnoho problémů může vzniknout právě nedostatečnou fyzickou ochranou;
- elektronická ochrana sítě – zařízení může být poškozeno špatným napájecím napětím, může dojít ke ztrátám informací vlivem výpadku napájecího napětí. Je tedy vhodné používat záložní zdroje, které zabezpečují stabilizaci napětí pro počítač a udrží ho v provozu po dobu výpadku energie. V případě delšího výpadku musí být zabezpečeno regulérní vypnutí počítačového systému;
- krádež vybavení – je nutné přesně zjistit, co se ztratilo a jaké to bude mít následky;
- krádež software – je snazší odcizit software než hardware. Je nutné pečlivě chránit zdrojové kódy aplikací, pokud jsou odcizeny, je velmi pravděpodobné, že za účelem získání

vlastnictví programu. Proti krádeži programů resp. jejich neautorizovanému používání je dobré se chránit jejich patentováním a důrazným uplatňováním autorských práv.

Jaká známe slabá místa sítě?

a) Hraniční směrovač: Díky špatně nakonfigurovanému řízení přístupu (ACL – Access Control List) na směrovači může hacker získat neautorizovaný přístup ke službám v DMZ (Demilitarised Zone).

b) Server pro vzdálený přístup: Neutajený a nemonitorovaný vzdálený přístup bývá jeden z nejsnadnějších způsobů, jak proniknout do sítě.

c) Operační systém a aplikace na systému v DMZ: může jít o konfigurační chybu, povolení nepotřebné služby atd.

d) Firewall anebo interní směrovač: díky chybné konfiguraci může umožňovat přímý přístup do sítě.

e) Software: pokud je zanechán v defaultní konfiguraci, ve starších verzích, nezalátán.

f) Uživatelský účet: mohou být přidělena nadbytečná privilegia.

g) Souborový systém: u Windows je citlivým místem sdílení souborů, u Unixů NFS export.

h) Vztahy důvěry: např. u Windows NT je to NT Domain Trust, u Unixů jsou to soubory .rhosts a hosts.equiv.

i) Služby typy X Windows: tyto služby mohou být neautorizované.

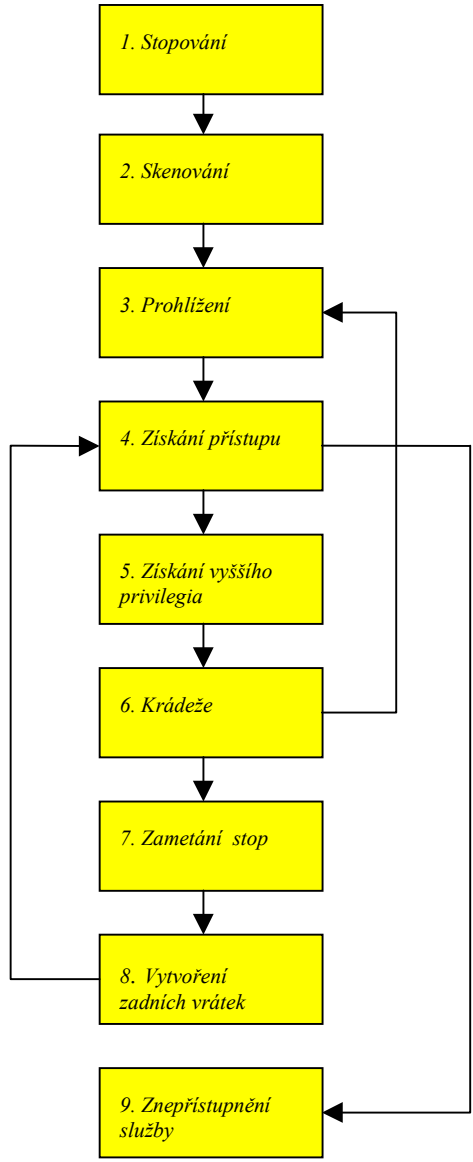
j) Úroveň sítě i jednotlivých hostů: lze se setkat s nedostatečným logováním, monitorováním a detekcí průniku.

k) Bezpečnostní politika a bezpečnostní procedury: mohou být nedostatečně propracované resp. akceptované.

2. Jak hackeři útočí

Internet dává prostor jak pro působení hackerů, tak pro výměnu informaci mezi nimi. Dle [McC99] lze při hackingu postupovat v krocích dle obr. 1. V čem je jejich podstata a jaké nástroje se používají?

Cílem je umožnit útočníkovi vytvořit komplexní profil postoje dané organizace k otázkám bezpečnosti. Mnohdy je třeba sbírat a dávat dohromady střípky informací. Konkrétní techniky závisí na typu cíle, zda jde o Internet, Intranet, Extranet nebo vzdálený přístup. Např. z Internetu a Intranetu hackeři identifikují doménová jména, IP adresy, UDP a TCP služby, mechanismy pro řízení přístupu, použití detektoru průniku, uživatelská a skupinová jména, systémové bannery, směrovací tabulky, SNMP informaci, typ systémové architektury; u Extranetu zdroj a cíl spojení, typ spojení atd., u vzdáleného přístupu telefonní čísla, typ vzdáleného mechanismu, autentizační mechanismus.



Obr. 1 Posloupnost kroků při hackingu

1. Stopování

Dílčí kroky v etapě stopování jsou následující:

Určení rozsahu aktivity

Je se třeba rozhodnout, zda útok bude podniknut na celou organizaci nebo její konkrétní část. Mnohdy lze vyjít z veřejně publikovaných informací o dané organizaci a jejích zaměstnancích. Řadu informací si lze přečíst na webových stránkách organizací, např. o lokalitě společnosti, e-mail adrese, telefonních číslech, odkazech na další webové servery dané organizace atd. Další informace lze získat z poznámkách v tagech typu „<", "!", "--".

Z nástrojů lze použít libovolný vyhledávací stroj resp. nástroj pro vyhledávání vyhledávacích strojů, např. FerreSoft firmy FerretPRO (viz http://www.ferretsoft.com). Jiným použitelným nástrojem je databáze EDGAR (http://www.sec.gov), samozřejmě, pokud je cílem nějaká americká společnost.

Orientace v síti

Ve většině Unixů lze použít whois: whois <jméno domény>, whois <IP adresa> atd. Dále se používají příkazy nslookup, host a traceroute.

Nejlepším základem obrany proti „stopování" je omezení toku ICMP a UDP paketů v rámci konfigurace směrovačů, přes které jsou uživatelé připojeni do Internetu. Dále lze použít řadu detektorů průniku a některé programy pro vyhledání paketů traceroute (RotoRouter, tdetect atd.)

2. Zkoumání (skenování)

Zde se určuje, které systémy jsou „živé" a dosažitelné. Jde o tři kategorie skenování:

Ping na sadu IP adres (ping sweeps)

Jako nástroj se pro skenování IP adres se u unixových systémů obvykle používá `fping` a u Windows `Pinger`.

Identifikace naslouchajících TCP a UDP portů

Pro skenování naslouchajících TCP a UDP portů existuje celá řada variant útoků, např. TCP connect scan (s plným handshakingem), TCP SYN scan (napůl otevřené skenování), TCP FIN scan, UDP scan atd. V prostředí Unixu skenování TCP portů zajišťují programy `Strobe` a `TCP scan`, skenování UDP portů `UDP scan` a skenování TCP i UDP portů `nmap` a `netcat`. V prostředí Windows slouží ke skenování TCP portů programy `PortPro` a `Portscan`, TCP i UDP portů program netcat.
K detekci TCP skenování lze použít shareware Genius nebo komerční software `BlackICE` firmy Network ICE. Pro detekci ICMP pingu lze použít detektory průniku typu `NFR` (Network Flight Recorder) i celou řadu unixových detektorů pingu, např. Scanlogd.

Určení typu skenovaného operačního systému

K rozlišení mezi typy operačních systémů se používá tzv. otisků. Východiskem je různá implementace TCP stacku u různých operačních systémů. Používá se celá škála metod, např. `FIN probe` (mj. Windows NT odpovídají, i když to není korektní), `Bogus flag probe` (mj. Linux odpovídá na nedefinovaný příznak v TCP záhlaví) ad., jejichž kombinací lze velmi přesně určit operační systém a někdy i jeho verzi. V prostředí Unixu toto zajišťují programy nmap, queso. Pro odhalení takového útoku lze použít nástroje pro detekci skenování portů.

3. Prohlížení

Tento krok se liší od předchozích hloubkou útoku – dochází zde k přímému spojení se systémem a jsou kladeny řízené dotazy. Od této etapy jsou útoky specifické pro každý operační systém.

Síťové zdroje

Vezměme si pro příklad Windows jako nejvděčnější objekt útoků. Základní přehled o síťových zdrojích nám umožní získat příkaz net view s parametry nejprve /domain a /<jméno domény>. Pokud se chcete prokousat do operačního systému hlouběji, musíte investovat do NT Resource Kitu (NTRK), ne nadarmo se ve světě také označuje jako Windows NT Hacking Kit. Z něj se například hodí `nltest` pro nalezení primárního a záložního doménového řadiče. Dalšími vhodnými nástroji z NTRK jsou `rmtshare, srvcheck a srvinfo`, případně pro procházení SNMP MIB `snmputil`.

Uživatelé a skupiny

Nejjednodušší cesta, jak identifikovat uživatele Windows NT, je použít příkaz `nbtstat`. Více informací lze získat pomocí nástrojů NTRK `usrstat, showgrps, local` a `global`.

Aplikace a bannery

Zde je vhodné začít starým a dobrým telnetem. Zjistit typ běžící aplikace lze například nástrojem `netcat` hackera Hobbita, který má ve zvláštní oblibě produkty firmy Microsoft.

Obdobnou sadu nástrojů lze najít i pro další operační systémy, je ale pravdou, že jejich výrobci snahu o „user friendly“ přístup tolik nepřehání jako Microsoft.

4. Získání přístupu

Pro získání přístupu je vhodné použít některý z nástrojů pro odposlech uživatelských hesel (`tcpdump, L0phtcrack, readsmb`), zmocnění se silou sdílených souborů (`NAT, legion`), krádež hesla souboru (`tftp, pwdump2`) a vynucení přetečení vyrovnávacích `pamětí (ttdb, eEye, IISHack`).

5. Získání vyššího privilegia

Samozřejmě, snem každého hackera je získat heslo administrátora (supervisora). K tomu slouží různé nástroje na luštění hesel (`crack, L0phtcrack`) .

6. Krádeže

Znovu začíná proces sběru informací, nyní s cílem objevit mechanismus, který by umožnil přístup do chráněného systému. Typickou možností je pátrání po heslu v otevřeném tvaru, v konfiguračních souborech, v registrech (u Windows).

7. Zametání stop

Hackerova činnost se chýlí ke konci, je třeba za sebou „uklidit“. To znamená vyčistit logy (`zap, elsave`) a ukrýt použité nástroje (např. adresáře).

8. Vytvoření zadních vrátek

Zadní vrátka jsou části kódu uložené na různá místa systému s cílem zajistit privilegovaný přístup při návratu útočníka do systému. Dosáhnout toho lze vytvářením falešných uživatelských účtů, naplánováním spouštění jistých skriptů (např. cron), infikováním setup souborů, instalací monitorovacích mechanismů, nahrazením aplikací „Trojskými koňmi“ atd.

9. Znepřístupnění služby, jiný termín odmítnutí služby (DoS – Denial of Service)

Pokud není útočník úspěšný při získání přístupu do systému, může ho vyřadil z činnosti jeho přetížením, v důsledku čehož napadený systém není schopen poskytovat po jistou dobu své služby (odmítá je). V [Doc00] jsou popsány útoky Ping-of-Death, Teardrop, SYN attack, Land attack, Smurf UDP flood a především poslední útok DDoS (Distributed DoS). Útoky DoS ovšem nejsou vyhrazeny jen pro operační systémy serverů, např. IOS 12.0 firmy Cisco je citlivý na UDP scan cílený na port 514 (syslog). Samozřejmě, v daném případě lze útok eliminovat zablokováním syslogu z vnější sítě.

3. Problémy s použitím bezpečnostních mechanismů a nástrojů

Bezpečnost komunikace v Internetu zajišťuje celá škála nástrojů. Páteř této bezpečnosti zajišťuje šest klíčových komponent:

- firewally;
- virtuální privátní sítě (VPN);
- monitory slabin;
- detektory průniku;
- antivirový software;
- infrastruktura veřejného klíče.

Jednotlivé komponenty jsou postupně popisovány v časopise Data Security Management, například problematice PKI je věnováno poslední, tj. 3. letošní číslo. V tomto příspěvku se zaměříme na právě aktuální problém spojený s nasazením detektorů průniku, kterým je jejich vzájemná interoperabilita.

Na co je ale třeba upozornit je, že všechny tyto nástroje mají omezené možnosti a že samy o sobě mohou být cílem úspěšných útoků. Dále si je třeba uvědomit, že bezpečnost je proces, ne produkt ani technologie. Neboli jinak řečeno ani nejdokonalejší bezpečnostní technologie nás neuchrání před útoky

(a v prostředí Microsoft to platí dvojnásob). Například firewall může zabránit, aby byly z konkrétních internetových adres do vaší vnitřní sítě zasílány pakety jistých protokolů. Ale ani když omezíte přílohy e-mailu na pouhé ASCII textové soubory, neuchrání vás to např. před zneužitím protokolu Simple Object Access Protocol firmy Microsoft, založeného na XML, protože tok jeho zpráv je nerozlišitelný od jednoduchého textu. Pro takové situace sedí přirovnání firewallu k „pancéřovým dveřím nasazeným na stan“ (viz http://www.3com.com/nsc/500619.html).

Anebo pokud odesilatel mailu využije chybu v ActiveX kontroleru (Explorer 5.0) scriptlet.typelib, pak příjemci takového mailu nepomůže, že zavirovanou přílohu nebude spouštět – k zavirování dojde již při otevření dopisu. Obecně platí, že nejlepší ochranou před novým virem je včasná aktualizace daného antivirového prostředku. V daném případě to neplatí,. odstranit tuto hrozbu lze jedině stažením potřebného nástroje z web serveru Microsoftu (http://www.microsoft.com/msdownload/iebuild/scriptlet/en/scriptlet.htm).

Otázkou je, jakou vhodnou kombinaci těchto nástrojů nasadit a to tak, toto nasazení nebylo kontraproduktivní ať již pro nadbytečnou režii, nákladnost provozu, nároky na správu atd. Historicky prvotní přístup k bezpečnosti výpočetních systémů a síti byl založen na vyhledávání jejich slabin. Jako konkrétní příklad lze uvést nasazení firewallu. Řada dnešních organizací a firem používá velký počet páteřních a vnitřních sítí, různorodých klientských stanic a serverů, internetových a intranetových služeb atd., rozhodnutí o rozmístění firewallů pak vůbec není jednoduché.

Variabilnost a komplexnost takovýchto sítí postupně ve světě vedla k širšímu použití monitorů slabin. Tyto nástroje začaly být používány nejen na úrovni jednotlivých sítí, ale v rámci různorodých scénářů na úrovni rozsáhlých sousítí. V rámci těchto scénářů lze modelovat následky potenciálních hrozeb pro celou síť. Monitory slabin jsou v posledních letech u některých výrobců doplňovány nástroji umožňujícími predikovat ztráty na aktivech organizace. Neboli nejde jenom o zjišťování slabin sítě a existující hrozeb, ale i o odhady ztrát na aktivech organizace.

Maximální úsilí při zabezpečovaní informačních zdrojů je nejčastěji věnováno zábraně v neoprávněném přístupu k datům. Jinou kategorií jsou detektory průniků, které tyto nežádoucí činnosti „pouze“ registrují. Tyto informace lze použít pro:

- operativní korekci nastavení jiného bezpečnostního nástroje (např. firewallu);
- vyhodnocení efektivnosti již přijatých bezpečnostních opatřeních.

Pokud podává detektor průniku informaci o aktuálním stavu v daném místě sítě, je tato informace efektivně využitelná nanejvýš pro řešení kritických situací. Ale do jaké míry je informace o konkrétním symptomu hrozby z hlediska celé sítě relevantní, to lze vyhodnotit pouze za situace, kdy jsou jednotlivé detektory průniku schopny vzájemně si vyměňovat zprávy mezi sebou a s managementem počítačové sítě. Tomuto tématu bude věnována závěrečná část našeho příspěvku.

4. Výměna údajů mezi detektory průniku

Detektor průniku je představován buď specializovaným počítačem vybaveným náležitým programovým vybavením, nebo programovým modulem běžícím jako jedna z úloh například v serveru.

V klasickém pojetí lze detektory průniku rozlišovat podle různých kritérií, například:

Podle umístění:

- detektory průniku do hostitelských systémů (běží jako jedna z úloh, někdy se zvlášť vyčleňují detektory narušení konkrétních aplikačních programů);

- síťové detektory průniku (pasivně sledují provoz v přilehlé síti).

Podle principu činnosti:

- detekce statistické anomálie (upozornění na podezřelé úchylky od dlouhodobým sledováním stanoveného „normálního“ chování);
- porovnávání vzorů (signatur - vyhledávání sekvencí charakteristických pro potenciální útok);
- korelace (vyhledávání souvislostí mezi jevy na první pohled nezajímavými).

Podle okamžiku vyhodnocování:

- v reálném čase;
- mimo reálný čas (zpracovávání záznamů o chodu systému).

Detektor průniku vyhodnocuje aktivity vztažené k zájmovému objektu (počítači, síťovému prvku apod.) a pokud objeví podezřelou okolnost, vyvolá definovanou reakci. Podezřelou okolností může být třeba neúspěšný pokus o přihlášení se či zkoumání stavu zájmového objektu. Jako reakce připadá v úvahu například zápis do souboru, informace operátorovi, vyhlášení poplachu a někdy i aktivní zásah, spočívající v zamezení další nežádoucí činnosti.

Detektor průniku může nastávající útok nejen včas odhalit, ale také upozornit s určitou pravděpodobností na dosud neznámý typ narušení. Detektor průniku pracující mimo reálný čas může provádět náročné statistické výpočty, porovnávat data pocházející z řady zdrojů a také na základě nových poznatků přezkoumávat staré záznamy.

Detektory průniku dnes dodává řada výrobců (viz např. http://lib-www.lanl.gov/la-pubs/00416750.pdf). Na počátku vývoje představovaly detektory průniku isolované systémy a nebyla požadována jejich interoperabilita. V současnosti se pohled na věc změnil a objevila se potřeba budování systémů detekce průniku. Jejich cílů je několik, například:

- zjednodušit správu rozsáhlejších systémů;
- urychlit předávání informací o bezpečnostních incidentech;
- urychlit reakci na ně;
- umožnit distribuci konfiguračních údajů apod.

Klíčovou podmínkou činnosti systémů pro detekci průniku je spolupráce jednotlivých komponent. Tato oblast je v současnosti předmětem zájmu sdružení IETF (The Internet Engineering Task Force, **http://www.ietf.org**), mj. vydávající známá standardizační doporučení RFC (Request For Comments), které vytvořilo speciální pracovní skupinu idwg (Intrusion Detection Working Group).

Rozsáhlejší systémy pro detekci průniku bývají pod trvalým dozorem operátora a skládají se z následujících komponent (viz též níže uvedený obrázek):

- Zdroj dat - nejzákladnější informace, kterou systém pro detekci průniku používá ke zjištění neoprávněné nebo nežádoucí aktivity. Zdroj dat zahrnuje například datové pakety nebo rámce, soubory se záznamy o chodu operačního systému nebo aplikací, případně systémem generované kontrolní údaje.
- Senzor – s požadovanou frekvencí sbírá data pocházející od zdroje dat.

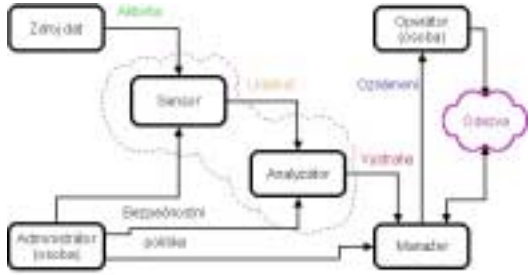
- Analyzátor – relativně samostatná komponenta systému pro detekci průniku nebo proces, který analyzuje data zachycená senzorem a vyhledává v nich příznak neoprávněné nebo nežádoucí aktivity, případně výskyt událostí, které mohou být z bezpečnostního hlediska významné. Obecněji se termínem analyzátor může rozumět ta komponenta, která generuje informaci o narušení a odesílá ji manažeru.
- Manažer – samostatná komponenta systému pro detekci průniku nebo proces, pomocí kterého operátor spravuje různé elementy tohoto systému. Správní funkce typicky zahrnují:
    - konfigurace senzorů;
    - konfigurace analyzátorů;
    - správa systému oznamování událostí;
    - konsolidace dat;
    - výstupní hlášení.

Schéma činnosti systému pro detekci průniku předpokládá, že analyzátor vyhodnotí událost detekovanou senzorem jako podezřelou a zašle výstrahu manažerovi. Základním problémem je návrh jednotného formátu zpráv a veškerých náležitostí spojených s jejich přenosem. Pokud by se podařilo tento jednotný formát zavést, bylo by možno snadno „propojit“ detektory průniku různého původu a vytvářet sítě pro včasnou výstrahu o hrozícím nebezpečí. Případ červa „I Love You“ názorně ukázal na potřebu takového řešení.

5. Pojem IDEF

Jedním z konkrétních předmětů zájmu skupiny idwg je návrh formátu výměny informací o detekci průniku (Intrusion Detection Exchange Format - IDEF). Tento formát představuje jeden z dalších, byť značně specifických protokolů pro výměnu dat. Účastníci této výměny jsou v asymetrickém postavení. Obecně se požaduje poskytnutí maximálního množství podkladů, ale ponechává se značná volnost při jejich zpracování, některé údaje nemusí být použity vůbec. To je v souladu s požadavkem pružnosti systému pro detekci průniku. V dalším textu se termínem zpráva IDEF rozumí libovolný údaj, předávaný v tomto formátu.

Jaká jsou výchozí kritéria pro návrh takového formátu? Není jich mnoho - předpokládá se, že analyzátor je oddělen od manažeru a že vzájemně komunikují pomocí protokolu TCP/IP (IPv4, IPv6 nebo jejich kombinace). Žádné další formy komunikace těchto entit se nepředpokládají. Veškeré údaje budou dopravovány stejnými kanály společně s běžnými uživatelskými údaji.



Komponenty systému pro detekci průniku

Naopak mezi nepodstatné nebo neřešené oblasti či problémy patří např.:

- Zda jsou senzor a analyzátor integrovány do jednoho systému, nebo zda jsou odděleny;
- zda jsou analyzátor a manažer odděleny anebo zda jsou propojeny v rámci hierarchie vyššího stupně;
- zda manažer oznamuje událost člověku, provádí akce automaticky, nebo jenom analyzuje příchozí výstrahy a zaznamenává je;
- zda jedna entita může sloužit pro jiné entity jako analyzátor a současně jako manažer pro další.

Působnost skupiny idwg má poměrně široký záběr. Skupina například předložila návrh protokolu IAP (Intrusion Alert Protocol) pracujícího na aplikační vrstvě, který je určen pro předávání urgentních zpráv o průniku a zabývá se také využitím jazyka XML (Extensible Markup Language) pro oblast detekce průniku.

Speciální požadavky na IDEF

Zprávy musí plně podporovat požadavky na provoz v internacionálním prostředí včetně lokalizace do různých jazyků a musí být formátovány takovým způsobem, aby mohly být prezentovány operátorovi v jeho místním jazyce s přihlédnutím k místním zvykům. Protože se dá očekávat požadavek některých manažerů na filtraci dat nebo jejich agregaci, musí být zprávy náležitě strukturovány.

Požadavky na autentizační a komunikační mechanismy

IDEF musí podporovat vzájemnou a oboustrannou autentizaci mezi manažerem a analyzátorem. Analyzátor se autentizuje manažeru pomocí veřejných klíčů nebo jinou metodou, obdobně postupuje manažer vůči analyzátoru. Autentizace se nesmí opírat o mechanismy nižších vrstev síťových protokolů, neboť je riziko, že mohou být napadeny a znehodnoceny.

IDEF musí podporovat přenos zpráv přes firewally. Tato komunikace nesmí vyžadovat takové změny nastavení firewallů, které by znamenaly snížení bezpečnosti chráněných sítí. Rovněž by k tomuto účelu nemělo být používáno sloučení přenosu IDEF zpráv s běžnými daty (např. metoda HTTP/POST), protože by mohlo být obtížné aplikovat různou bezpečnostní politiku pro dopravu zpráv IDEF a ostatních zpráv.

Zprávy IDEF obsahují důležité informace (mimo jiné i hesla) a mohou být předmětem mimořádného zájmu narušitele. Jejich obsah musí možno utajit šifrováním, přičemž musí být zachována možnost volby i snadné záměny šifrovacích modulů. Důvodem jsou odlišné národní legislativní normy ve světě a jejich časté změny. IDEF by měl standardně nabídnout dva odlišné šifrovací moduly, jeden z nich by měl používat délku klíče 56 bitů, druhý pak 168 bitů.

IDEF musí zabezpečit integritu obsahu zprávy. Zvolený návrh musí být schopen podporovat různé mechanismy zabezpečení integrity a musí být schopen adaptace do různých prostředí. Součástí návrhu IDEF by měly být hešovací algoritmy, např. MD5.

Komunikační mechanismy IEDF by měly být odolné vůči útokům typu odepření služeb. Komunikační mechanismus IDEF by měl být odolný vůči zlomyslné duplikaci zpráv. Obvyklým způsobem zhoršujícím výkonnost bezpečných komunikačních mechanismů je odeslat kopii zprávy, aniž by jí narušitel rozuměl. Jeho cílem je zmást přijímající stranu. Je žádoucí, aby komunikační mechanismy IDEF byly vůči duplikaci zpráv odolné.

Obsah zpráv a reakce na ně

Volba IDEF musí pokrýt nejen všechny momentálně známé typy mechanismů detekce průniku, ale vytvořit i prostor pro budoucí rozvoj. Součástí IDEF zprávy musí být standardizovaný název události, je-li znám. Pokud dosud neexistuje, může být použit jiný. Způsob vytváření a aktualizace standardizovaného seznamu událostí je předmětem vývoje.

Význam standardizace názvů vysvětlí následující příklad: Narušitel se pokusí stejným mechanismem zaútočit proti dvěma různým systémům. Tento útok je detekován dvěma odlišnými analyzátory ze dvou různých implementací. Přestože algoritmy použité pro detekci útoku mohou být v každém analyzátoru naprosto odlišné, oba by měly ohlásit manažeru stejnou událost.

Obsah zprávy IDEF musí umožnit sdělení odkazu na bezpečnostní doporučení vztažené k ohlašované události. Taková doporučení jsou vytvářena řadou organizací jako CERT (Computer Emergency Response Team), výrobci, dodavateli nebo výzkumnými týmy. Například je detekován již známý způsob útoku; součástí příslušné IDEF zprávy bude odkaz na doporučení CERT, které operátor použije k zahájení nápravných kroků. IDEF zpráva musí být také schopna poskytnout odkaz na detailní data týkající se dané události, tato informace ovšem nemusí být příjemcem použita.

IDEF zpráva musí obsahovat identifikace zdroje událostí a identifikátor cílové komponenty, jsou-li známy; například IP adresy. Identita zdroje a cíle bude záležet i na typech událostí, např. na tom, zda byly detekovány na úrovni operačního systému nebo aplikačního programu. Narušitel například zaútočí proti DNS serveru a pokusí se přeplnit vyrovnávací paměť (buffer overflow attack). Výstražná IDEF zpráva bude indikovat jako cíl DNS server a bude také obsahovat zdrojovou IP adresu, ze které byl útok veden.

IDEF zpráva musí podporovat různé typy adres, neboť zařízení, kterého se útok dotkne, nemusí být nutně součástí sítě s IP protokolem. Většina zařízení má více adres podle vrstev síťové architektury (obvykle na druhé nebo třetí vrstvě). Je vhodné je uvádět všechny, neboť to může zpřesnit identifikaci.

IDEF zprávy musí obsahovat standardizovanou specifikaci možného dopadu události na cíl, což poskytne operátorovi informaci o možném záměru narušitele a ohodnotí případný rozsah narušení. Ne všechny systémy budou tohoto schopny v náležité míře. Například je registrován útok typu přeplnění vyrovnávací paměti. Příslušná IDEF zpráva bude obsahovat informaci, že následkem tohoto útoku může být získání práv administrátora cílového systému. Operátor pak může na tuto událost urychleně reagovat.

Jestliže je odezva na událost vyvolána automaticky, musí být o tomto zaslána IDEF zpráva operátorovi. Toto pomůže rozhodnout o následující akci, pokud je potřeba. Detektor průniku například zaregistruje opakovaný neúspěšný pokus o přihlášení se, což vyhodnotí jako potenciální útok a zareaguje zablokováním příslušného uživatelského účtu.Toto zablokování bude trvat deset minut, což je doba postačující k tomu, aby operátor přezkoumal chování daného uživatele.

IDEF zpráva musí obsahovat údaj, který umožní pozdější identifikaci a vypátrání místa, kde se nalézá analyzátor, který zprávu oznámil. Toto pomůže rozhodnout o způsobu reakce na událost a lze sledovat postup narušení. Jestliže je stejná událost hlášena různými analyzátory, jejich identifikace může poskytnout cenné informace pro vlastní obranu i pro odhalení útočníka. K identifikaci může posloužit například IP adresa. IDEF zpráva musí být také schopna přenést údaj o tom, kdo implementoval detektor průniku a o prostředku, který událost detekoval.

IDEF zpráva musí počítat s požadavkem na klasifikaci stupeň své spolehlivosti (aniž by ovšem analyzátor musel tento údaj brát v úvahu). Mnohé detektory průniku mají nastavenu prahovou hodnotu, při jejímž překročení se generuje výstražná zpráva. Při těsném překročení prahu je vyšší pravděpodobnost falešného poplachu.

Každá IDEF zpráva musí být jednoznačně identifikovatelná a musí být odlišitelná od jiných IDEF zpráv. Unikátní identifikátor se může skládat z unikátního původního označení (např. IP adresy) spojeného s jednoznačným pořadovým číslem generovaným původcem zprávy. Při typické organizaci systému pro detekci průniku může analyzátor událostí na nízké úrovni zaznamenávat informace pocházející od příslušného senzoru do databáze, zatímco výsledky analýzy a zprávy bude předávat vyšším vrstvám. V tomto případě může být jednoznačný identifikátor zprávy na nízké úrovni použit jako součást výsledné zprávy předávané ke zpracování vyšším vrstvám. Analyzátory na vyšších vrstvách mohou v případě potřeby později tento identifikátor použít k přístupu k datům zprávy na nízké úrovni.

IDEF musí umožňovat záznam data a času, kdy byla zpráva o události vytvořena, což umožňuje například nalezení korelace s jinými údaji. IDEF může také umožnit záznam o datu a čase, kdy byla událost detekována. Čas detekce události se může lišit od času, kdy byla zpráva vytvořena, neboť vyhodnocení události a generování zprávy může jistou dobu trvat. Jestliže detekující element je schopen přesně určit čas, kdy se událost vyskytla, je velice důležité uložit i tuto informaci do výstražné zprávy. Údaje o čase budou vždy místní, s doplněním o údaj o časovém posunu. Formát pro předávání času musí vyhovovat platným standardům, včetně respektování přelomu století a obdobných datumů.

Časové rozlišení (přesnost, granularita), které se použije v konkrétní zprávě o události, nebude specifikováno. Jeden analyzátor může pracovat s granularitou svých hodin jedna milisekunda, zatímco jiný udává čas po jedné sekundě. Oba analyzátory musí být schopny odeslat vyhovující zprávu.

Identifikátory výstrahy a definiční proces identifikátoru výstrahy

Předpokládá se vytvoření standardního seznamu identifikátorů IDEF výstrah. Tento seznam musí být rozšiřitelný jak těmi, kdo detektory průniku implementují, tak i administrátory. IDEF musí být schopen akceptovat definici nové události nebo nové metody detekce.

Proces pro definici nového identifikátoru výstrahy nesmí preferovat některou implementaci detektoru průniku před jinou. Mohla by nastat situace, že se některá specifická implementace detektoru průniku rozhodne utajit některou informaci z obavy negativního dopadu na ni samotnou.

Závěr

Pro přijetí správných a včasných opatření pro zajištění bezpečnosti našich informačních systémů je třeba zajistit neustálé mapování potencionálních slabin a hrozeb v počítačové síti. Z tohoto hlediska nám hackeři svým způsobem pomáhají, protože jejich cílem není destrukce našich výpočetních systémů, nýbrž upozornění na jejich chyby a nedostatky. Velkým nebezpečím jsou hackerovské nástroje v rukou crackerů, jejichž motivace i schopnost odhadu následků bývá obvykle diametrálně odlišná.

Tak jako si hackeři mapují činnost uživatelů, je z druhou strany třeba si z druhé strany mapovat činnost hackerů a znát jejich standardní postupy. Rovněž je třeba efektivně nasazovat celou škálu bezpečnostních nástrojů, v poslední době vystupuje do popředí použití detektorů průniku. Významným krokem v jejich vývoji se stal návrh protokolu pro vzájemnou výměnu zpráv mezi jednotlivými detektory, a proto byla tato problematika také zahrnuta do našeho vystoupení na této konferenci.

Použitá literatura

[Anon99] Anonymous: Maximum Linux Security. SAMS 1999.

[Asse99] Assets, Threats and Vulnerabilities: Discovery and Analysis. Symantec 1999.

[Dock00] Dočkal, J.: DDoS – Distribuovaný útok v Internetu. DSM 2/2000, str. 14-17.

[Knig00] Knight E.: Computer Vulnerabilities. Security Paradigm 2000.

[McCl99] McClure, S. – Scambray, J. – Kurtz, G.: Hacking Exposed. Osborne 1999.

VIRY A PRÁVO

Petr J. Drahovzal
AEC, spol. s r.o., DATA SECURITY COMPANY

S rozvojem počítačových technologií dochází ve světě k rozvoji „gangsterských“ útoků na tyto technologie, které se ve velké míře rekrutují z počítačových virů. Důvody k napsání programu, který poškozuje počítače mohou být různé, nicméně se však v každém případě jedná o činnost nezákonnou, která bývá přísně postihována lokálními autoritami stejně tak, jako každý jiný trestný čin.

Viry totiž vážným způsobem poškozují počítačové systémy a škody, které jsou každoročně za jejich „přispění“ způsobeny se pohybují v řádech miliard dolarů.

Do nedávné doby byla závažným problémem postihování autorů počítačových virů absence příslušné legislativy, v dnešní době, když jsou někteří z těchto lidí za mřížemi se zdá být tento problém vyřešen.

Pronásledováním aktivit počítačových škůdců se zabývají například i experti z FBI a i když se dá tvrdit, že tento boj nikdy neustane, jedno je jisté – bude čím dál tím víc intenzivnější a kvalitnější.

Přednáška se bude zaměřovat na:

- škody způsobené autory virů
- jak vypadá svět autorů těchto programů
- postižitelnost těchto lidí
- úspěchy při hledání autorů virů
- situace ve vyspělém světě
- proč se viry píšou
- legislativa

KOMPLEXNÍ BEZPEČNOSTNÍ ŘEŠENÍ

Tomáš Vobruba
AEC, spol. s r.o.

Každá firma, či společnost, chtějící v dnešní době uspět ve světe obchodu, využívá ke své cestě za úspěchem Internetu. Společnosti zde prezentují své výrobky, shání informace, komunikují s klienty a obchodními partnery pomocí e-mailu, resp. využívají jiných služeb. K tomu, aby takové podniky mohly Internetu využívat ale potřebují mít vybudovanou vlastní vnitropodnikovou síť (LAN) s jistými parametry a pravidly a přípojkou přes některé z četných poskytovatelů připojení k Internetu. Co k takové síti patří?

Především počítače :-). Počítače jako servery, souborové, e-mailové servery, firewally či webové servery. No a samozřejmě klientské stanice zaměstnanců. Aby taková síť fungovala, je potřeba několika věcí:

1) Správně fungující hardware a software.
2) Šikovného správce s dobrými znalostmi problematiky IT, popřípadě externí firmy tyto znalosti vlastnící.
3) A souboru pravidel, který určí, co všechno je dovoleno, co není a jak takové sítě využívat.
4) Ukáznění uživatelé, dodržující předepsaná pravidla (každý systém je tak silný, jak silný je jeho nejslabší článek – a lidská faktor je bohužel největší slabinou současných informačních technologií).

Myslím, že není potřeba tyto vcelku základní věci nějak podrobněji rozebírat. Každému je určitě jasné, že nejdůležitější částí tohoto krátkého výčtu je bod 2). Především je třeba mít znalosti v IT, aby taková síť fungovala. Protože jenom správce sítě, nebo externí firma jsou schopny poskytnou dostatečné „HOWTO“ k tomu, aby byl splněn bod 1) a bod 3). Z bodu 3) zase dodržováním těchto pravidel časem mohou vzniknout vychovaní a ukáznění uživatelé.

Je samozřejmostí, že taková firma, která chce využívat Internetu, musí myslet také na bezpečnost v její nejobecnější rovině.

Internet je totiž zcela veřejné médium bez jakékoliv kontroly, které se velmi živelně rozvíjí. Na Internetu se nepohybují jenom obchodní společnosti, nebo univerzitní kluby, pohybují se zde především lidé s různým stupněm znalostí informačních technologií. Díky dostupnosti Internetu se může dneska za pár korun připojit kdokoliv. Od uživatelů hledajících jenom informace, přejících si třeba jenom popovídat s přáteli, nebo si domluvit schůzku, až po lidi Internetu zneužívajících k páchání trestné činnosti, která se navíc na takto otevřeném médiu velice těžko dokazuje (zvlášť pokud je uživatel dostatečně schopný). Ale i méně pokročilí uživatelé se mohou právě díky dostupnosti všech možných informací na Internetu stát hrozbou pro ostatní komunity.

Mluvme třeba o hospodářské kriminalitě na Internetu, nebo psaní zlomyslných programů s cílem něco zničit, nebo zahltit. S rozvojem Internetu a rozšiřováním moderních operačních systémů Windows, které (přiznejme si to) nejsou zrovna bezpečné a bez chyb, se také začaly velmi rychle šířit viry, protože co může být pro takový virus lepší než otevřená síť se stovkami tisíc nezkušených a nechráněných uživatelů či firem.

Je třeba začít antivirovou ochranou. Co si můžeme představit pod pojmem „antivirová ochrana“? Určitě je to nějaký program, který brání jiným programům působit na Vašem počítači bez vašeho vědomí.

Určitě je to také jistá, alespoň základní znalost o tom, co je to vir, jak se nejčastěji šíří, jak obsluhovat antivirový program a kde hledat informace v případě, že si uživatel neví rady.

Každý se už určitě s viry setkal, a tak ví, co od nich může čekat a proto se shání po nových a dokonalejších prostředcích na ochranu jejich počítačů. Je samozřejmostí, že ochránit samostatný doma stojící počítač proti útoku virů není tak složité (nemáte-li zrovna doma pubescentní ratolesti toužící vyzkoušet každou počítačovou hru pochybného původu, která se ocitla ve vzdálenosti bližší než sto světelných let) jako zabezpečit velkou podnikovou síť o mnoha uživatelích. Nechci tím samozřejmě nijak podceňovat možnosti virů na jednotlivém počítači. Důsledky a účinky virů jsou v podstatě stejné, jenomže na větší síti je to více viditelné a také podnik má vlivem působení viru co ztratit. Od času technika IT až po mnohamilionové finanční ztráty způsobené výpadkem serverů a stanic (určitě si každý vzpomene na nedávný útok emailového červa ILOVEYOU). Protože se v poslední době viry šíří hlavně přes Internet, je tedy nutné zabezpečit takovou síť hlavně na vstupech do Internetu, na serverech - a ani koncové stanice nesmí zůstat bez ochrany.

Existuje spousta antivirových řešení jež jsou schopna se vám postarat o jednotlivý počítač stejně dobře jako o celou síť. Síťovým řešením se obvykle říká Enterprise nebo Corporate solution (česky „podniková řešení“). Obvykle v sobě zahrnují ochranu firewallů, souborových serverů, poštovních serverů, e-mailových bran a proxy serverů a samozřejmě klientských počítačů. Bývají podporovány obvyklé serverové operační systémy jako jsou UNIX systémy Solaris či Linux, Novell, Windows NT, Windows 2000, OS/2 nebo operační systémy klientských stanic Windows 95 a 98, Windows NT, Linux nebo i MacOS, nezapomíná se ani na starý dobrý MS DOS a Windows 3.11 (i když většina antivirových firem již odkládá tyto dva posledně jmenované systémy do pozadí zájmu). V dnešní době je veškeré úsilí věnováno právě Windows 95 a 98 a Windows NT kde je nárůst virů nejdramatičtější, a to především makrovirům. (Poděkujme vývojářům Microsoft za skvělý, silný a velmi jednoduchý jazyk VisualBasic :-), ve kterém je většina „moderních“ virů psaná.)

Je tedy jasné, jaké budou požadavky firem na antivirové společnosti. Budou požadovat ochranu v celé šíři lokální sítě LAN. Např. AEC jako jedna z firem poskytujících takováto řešení šitá na míru jednotlivých společností je schopna provést nejprve analýzu topologie LAN sítě zákazníka a poté mu navrhnout (a samozřejmě i prodat :-) plně funkční řešení.

Obvykle se začíná právě od ochrany serverů. Přece jenom je jednodušší nainstalovat antivirový program na pár serverů umístěných obvykle v jedné místnosti, než začít tím, že se bude vymýšlet, jak zabezpečit stovky počítačů, což je samozřejmě časově náročnější.

Pokud mohu mluvit ze svých praktických zkušeností, začínám od firewallu. To je tedy od samotného připojení k Internetu. Existuje totiž krásně jednoduché a navíc bezpečné řešení, jež mají všechny moderní firewally. Tím řešením je CVP (Content Vectoring Protocol). V podstatě všechny antivirové programy pro firewally, které jsou v dnešní době dostupné, využívají tohoto protokolu.

Jak antivirový program pro firewally pracuje? Úplně jednoduše, na chráněné vnitřní síti se na funkční počítač nainstaluje příslušný antivirový program, který již se samotným firewallem komunikuje pomocí právě směrového protokolu CVP. Takováto antivirová ochrana Vám potom poskytuje ochranu před viry na úrovni samotných internetových protokolů HTTP, SMTP a FTP.

Řeklo by se, že toto by mohlo stačit na ochranu podnikové sítě proti virům příchozím z Internetu. Ale není tomu tak. Existuje spousta jiných cest, jak se Vám mohou viry dostat do počítače, a proto je třeba přistoupit k druhému stupni ochrany - a tou je ochrana samotných poštovních a souborových serverů.

Ochrana na souborových serverech je v podstatě vždy bez problémů a nároky na provozování takového antiviru jsou téměř stejné jako na stanice. Výjimkou jsou unixové servery a servery s operačním systémem Novell, které mají natolik odlišné operační systémy, že ani integrace antivirové ochrany není vždy snadnou záležitostí.

Výrobci antivirových programů v případě ochran na servery kladou důraz hlavně na ochranu síťových služeb serverů a funkčnost spolehlivost a nenáročnost na procesorový výkon rezidentních ochranných prostředků.

Poněkud složitější je to s ochranou poštovních serverů. Je třeba brát na zřetel, že dopisy nejsou servery pouze doručovány, ale i skladovány. Tedy program musí mít dva stupně ochrany. Prvním stupněm je rezidentní ochrana, neboli skenování příchozí a odchozí pošty v reálném čase, druhým pak skenování na požádání, reprezentované třeba naplánovaným skenováním mailboxů a veřejných složek. Většina výrobců antivirových programů se bohužel zaměřila na vývoj programů pro Microsoft Exchange nebo Lotus Notes. Je to velká škoda, neboť dnes jsou pro svoji nenáročnost a jednoduchost hojně rozšířené hlavně poštovní servery postavené na linuxových systémem. Třeba poštovní programy sendmail nebo qmail. Pro ně v podstatě není ochrany... Ale pokud je využíváte a už už se poohlížíte po konopném laně a nejbližší vhodné větvi, přece jen chvíli posečkejte. Není to totiž pravda tak docela. Například společnost Kaspersky Lab se svým produktem AVP zabrousila i do této problematiky a vyvinula program, který splňuje všechny požadavky na ochranu mail serverů. Bohužel je tento program zatím osamoceným pěšákem v poli.

Teď už by se i dalo říci, že je firma s antivirovou ochranou na firewallu, poštovním serveru a souborovém serveru ochráněna před útokem virů. Dalo by se to říci, to ano, ale jenom v případě, že má firma zaměstnance, kteří si nenosí do práce na své počítače hry, aplikace či dokumenty na disketách nebo CD-ROM, neboť tyto mohou obsahovat viry... Je pravdou, že pokud by společnost dodržovala všechna bezpečnostní pravidla přenosu a skladování dat na síti, asi by se virus z CD-ROMu nebo diskety nerozšířil dále. Ale tento stav je takřka i s ukázněnými uživateli utopií. Proto je posledním (třetím) stupněm antivirové ochrany právě ochrana klientských stanic.

V dnešní době Vám jakýkoliv prodejce antivirových programů nabídne minimálně pět různých antivirových programů na stanice. Vzhled a funkčnost, či úroveň těchto programů bývá na různém stupni kvality, ale funkce programů bývají stejné. Reportování, karanténa, plánované úkoly, kontrola pošty v poštovním klientovi nebo i automatické aktualizace. Stačí si jenom vybrat. Namátkou vyjmenuji ty, které nabízí naše firma: AVP, VirusScan, F-Secure Anti-Virus, Norman Virus Control a Norton Antivirus. Tedy stačí si jenom vybrat buď na základě doporučení zkušených techniků a obchodníků takové firmy a nebo na základě recenzí a srovnávacích testů renomovaných časopisů s tématikou IT.

V případě podnikových řešení je třeba brát na zřetel také komunikaci v síti a jednoduchost správy z jednoho místa bez nutnosti počítač navštívit, pokud se vyskytne problém.

Co říci závěrem?

Stoprocentně dokonalé komplexní bezpečnostní řešení je ve své podstatě utopií. To ovšem neznamená, že by nemělo být součástí každé firmy, které jen trochu záleží na ochraně svých dat, informací a především dobré pověsti. Komplexní bezpečnostní řešení totiž může předejít spoustě bezpečnostním incidentům. A pokud stále váháte, pak vězte, že v roce 1999 působily počítačové viry spolu s ostatními druhy kybernetických útoků celosvětově škody za 20 miliard dolarů. (Přepočítáno kursem platným dne 19. května je to 819,22 mld. korun českých… To je více než roční rozpočet mimořádně štědrého současného vládního kabinetu.)

STÁTNÍ KONCEPCE ROZVOJE INFORMAČNÍ SPOLEČNOSTI

RNDr. Alexander Kratochvíl, CSc.
Úřad pro státní informační systém

Vychází z programového prohlášení, schválené usnesením vlády České republiky ze dne 31.5.1999, pod názvem Státní informační politika – Cesta k informační společnosti. Její realizace se bude uskutečňovat prostřednictvím Akčního plánu. Jeho popis je obsahem první částí příspěvku.

Protože naše země nemůže svůj program koncipovat osamoceně, ale měla by usilovat o jeho sladění s aktivitami Evropské unie, budou ve druhé části příspěvku srovnány naše aktivity s iniciativou Evropské unie, známé jako Prodiho výzva e-Europe, kde pod 10 body jsou uvedeny nejdůležitější záměry na cestě k vyššímu rozvoji evropské společnosti.

A.

Akční plán

Akční plán je odpovědí vlády na to, jak naplnit vizi informační společnosti. Stanoví bezprostřední odpovědnost ústředních orgánů státní správy za:

- informační gramotnost,
- rozvoj elektronického obchodu, a
- vybudování elektronické veřejné správy.

Současně definuje aktivity samosprávy a podnikatelské veřejnosti, které mají hlavní vliv na úspěšný rozvoj informační společnosti. Vláda může rozvoji informační společnosti napomoci, ale nemůže ji zařídit.

Dosavadní výsledky realizace Státní informační politiky:

Jako první jsou plněny cíle, které se týkají hlavní úlohy vlády – legislativní iniciativy. K tomu bude zmínka později.

Jsou již připraveny přímé akce ústředních orgánů státní správy. Ty však již vyžadují finanční zdroje a proto je nezbytné prosadit realizaci státní informační politiky do návrhu státního rozpočtu. Konkrétní aktivity jsou především zaměřené na zavedení elektronických služeb veřejné správy, a v horizontu do roku 2002 je to především realizace koncepce ISVS, vytvoření rovnocenných komunikačních kanálů ve vztahu občan a veřejná správa, s využitím Internetu. Akční plán obsahuje podrobný popis priorit.

Jaké jsou věcné a časové priority:

Pro informační gramotnost:

1. vybudovat nejprve kvalifikační a technické způsobilosti vzdělávacích institucí,

2. v návaznosti na tyto způsobilosti rozvinout funkce informatizovaného školství (vzdělávací techniky a nástroje, řízení vzdělávacího procesu).

Pro elektronický obchod:

1. realizovat opatření na podporu elektronického obchodu,
2. zahájit přípravu nového zadání aktivit v oblasti e-obchodu.

Pro elektronickou veřejnou správu:

1. Přednostně zajistit veřejné informační služby (umožnit svobodný přístup k informacím podle zákona č. 106/99 Sb.) prostřednictvím dalších komunikačních kanálů (Internet, kiosky, kontaktní místa veřejné správy atd.) a realizovat koncepci budování informačních systémů veřejné správy,
2. v návaznosti na ISVS vyvinout elektronické služby veřejné správy (daňová přiznání, změny osobních údajů občanů atd.) a vyřešit problém identifikace osob.

Co to bude stát:

Realizace státní informační politiky bude v příštích letech stát okolo 6 mld. Kč ročně.

Vyhodnocení efektivity:

Značné investice do této politiky vyváží přínosy, pokud uvážíme, že povedou k podstatnému zkrácení doby strávené na úřadech, umožní přístup občana v relacích 24/7/365 k informacím a službám, a proto uspoří náklady na jeho straně. Spojení s procesním řízením také umožní sledovat efektivitu jednotlivých úkonů, jejich nákladovost a cenu, kterou by občan platil, kdyby nebyla hrazena z daní.

Proto, mít takto řízenou a efektivní veřejnou správu za iniciační náklady na úrovni 6 mld. Kč, je velmi přijatelný obchod.

Otázka, zda přeci jen není na takový „obchod“ příliš brzo, souvisí s pohledem, jak jsme na tom ve srovnání s Evropou.

B.

Srovnání s iniciativou e-Europe, projednávanou v Lisabonu ve dnech 23.-24. března 2000

1. Evropská mládež do digitálního věku

Vláda schválila Koncepci státní informační politiky ve vzdělávání v dubnu 2000. Obsahuje následující programy:

Vzdělávání:

- Koordinační centrum pro informační gramotnost
- Informační gramotnost učitelů
- Připojení k Internetu a vybavení multimediálními počítači
- Připojení škol a knihoven s multimediální kvalitou
- Multimediální nástroje a programy
- Zavádění ICT do výuky
- Informační zdroje pro vzdělávání
- Další vzdělávání učitelů

- Informační gramotnost občanů

Veřejné informační služby knihoven (VISK)

- Vybudování a provoz Koordinačního centra pro rozvoj VISK v ČR (KC VISK)
- Mimoškolní vzdělávání pracovníků knihoven
- Program vytváření informačních center veřejných knihoven - ICEKNI (etapy)
- Digitální knihovna a archiv pro informační služby knihoven
- Národní program retrospektivní konverze katalogů knihoven v ČR
- Národní program digitálního zpřístupnění vzácných dokumentů
- Národní program mikrofilmování a digitálního zpřístupnění dokumentů ohrožených degradací kyselého papíru - Kramerius
- Elektronické informační zdroje - periodika (nákup licencí)
- Souborný katalog ČR - provoz

Programy budou zahájeny ještě v roce 2000 a převážně jsou plánovány do roku 2005.

2. Levnější přístup na Internet

Současné akce jsou v ČR vedeny ve třech směrech

A) Internet 2000

Monopolní provozovatel Český Telecom, a.s. zvýhodnil využití nejmasovějšího připojení zavedením cenového sazebníku s názvem Tarif Internet 2000. Ten lze považovat za znatelný posun k levnějším službám v porovnání s obdobným tarifem Internet 99. Došlo k významným snížením, především v době slabého provozu (kde se cena snížila až na úroveň cca 12 Kč za 1 hod.) a byl zrušen tzv. sestavovací poplatek, a ČESKÝ TELECOM, a.s. se s poskytovateli Internetu dělí o výnosy z této služby.

B) Zákon o telekomunikacích

Od 1. 7. 2003 dojde, v souladu se záměry telekomunikační politiky MDS, k plné liberalizaci podnikání v telekomunikacích. Regulační rámec liberalizace je nastaven novým zákonem o telekomunikacích. Takto pojatá plná liberalizace podnikání v telekomunikacích zcela jistě bude mít, tak jako ve všech ekonomicky vyspělých zemích, za následek snížení telekomunikačních poplatků včetně poplatků za používání Internetu.

C) Smlouva se třetím operátorem sítě GSM

Mezi Ministerstvem dopravy a spojů ČR a společností Český Mobil a.s. byla v říjnu 1999 uzavřena smlouva, ve které jsou zakotveny další závazky společnosti Český Mobil, a.s. zhruba na období tří let. Smlouva byla zveřejněna na internetové stránce MDS: www.mdcr.cz.

Závazky Českého Mobilu, a.s. jsou uvedeny ve 4. části Smlouvy, a o jejich plnění Český Mobil, a.s. informuje ministerstvo vždy jednou za 6 měsíců.

Podle příslušné smlouvy musí firma Český Mobil, a.s. zabezpečit přístup k Internetu ve více než 13 000 školách a knihovnách ČR do konce tříletého období, a financovat přístupovou infrastrukturu.

3. Urychlení rozvoje internetového obchodování

Jsou připravena opatření vlády v samostatném dokumentu, který zahrnuje jak analýzy právního řádu, tak i konkrétní legislativní změny k ochraně spotřebitelů, regulace platebních systémů atd. Klíčovým bude zákon o elektronickém podpisu, který právě nyní prošel druhým čtením v Poslanecké sněmovně Parlamentu ČR, a jeho definitivní schválení se očekává do poloviny roku 2000.

4. Rychlý Internet pro vědce a studenty

ČR se doposud účastnila všech evropských iniciativ v rámci TEN a je připravena tak činit i do budoucna. Tato problematika je řešena prostřednictvím MŠMT spíše v rámci vědní politiky, nikoliv v rámci informační politiky.

5. Smart cards (programovatelné karty) pro bezpečný elektronický přístup

Je připravován projekt s názvem *Využití elektronických identifikátorů ve veřejné správě*, s cílem vytvořit datové, právní, standardizační a organizační předpoklady pro vydávání elektronických identifikátorů obyvatelům a organizacím, v návaznosti na zákon o elektronickém podpisu.

Indikátory cílového stavu:

- Vytvořit certifikační autoritu veřejné správy a právního rámce pro výdej a využití elektronických identifikátorů.
- Registr obyvatel, registr ekonomických subjektů a registr zdravotních pojištěnců budou připraveny jako datové zdroje pro vydávání elektronických identifikátorů.
- Informační kiosky na kontaktních místech veřejné správy a zdravotních pojišťoven budou vybaveny pro využití elektronických identifikátorů.
- Připravit a uvést do provozu programové vybavení pro bezpečný přístup ke službám veřejné správy prostřednictvím Internetu.
- Upravit pro využití elektronických identifikátorů vybranou oblast vybrané aplikační programové systémy (sociální služby, sociální a zdravotní pojištění, vybranou oblast zdravotnictví).
- Elektronické identifikátory budou vydány 20% obyvatel a statutárním zástupcům velkých organizací.

Termín: do roku 2002

6. Rizikový kapitál pro střední a malé podniky v oblasti nových technologií (high-tech)

V současné době nejsou v ČR vyvíjeny žádné paralelní aktivity.

7. Zapojení zdravotně postižených občanů do všech oblastí společnosti pomocí elektronických prostředků („eParticipation“)

Je nutno zmínit České fórum pro informační společnost, které vyvíjí aktivity na úrovni diskuse. Jeho význam bude neustále narůstat.

8. Zdravotní péče online

Je připravován projekt *Zdravotnictví on-line* s cílem: vytvořit zákonné, technologické, standardizační a bezpečnostní podmínky pro zavedení elektronického zdravotního záznamu, vedení národních lékařských oborových registrů a využívání telemedicíny pro konziliární účely ve zdravotnictví ČR.

Mělo by být dosaženo následujícího cílového stavu:

- Převzetí norem EU pro elektronickou zdravotnickou dokumentaci (EHCR) českou národní legislativou.
- Vytvoření standardů pro jednotlivé oblasti využití EHCR (zdravotnická dokumentace, ochrana dat, lékařské předpisy, konziliární zprávy, vyúčtování léčebných výkonů, záznam na elektronickém identifikátoru aj.).
- Elektronická komunikace na úrovni pacient – lékař (zdravotnické zařízení) – zdravotní pojišťovna – lékárna, a to s cílem optimalizovat zdravotní péči a související peněžní toky.

Termín: do roku 2002

9. Inteligentní doprava

Na základě Prodiho iniciativy byla zahájena práce skupiny odpovědné za tuto oblast a do Akčního plánu byl zařazen projekt Inteligentní doprava, prozatím na úrovni studií.

10. Státní správa on-line

Je připravován program Elektronická veřejná správa, s cílem zahájit do roku 2002 provoz vybraných elektronických služeb veřejné správy.

Předpokládá se dosažení následujícího cílového stavu:

- Nejméně 10% kontaktů veřejné správy bude již na konci roku 2002 realizováno elektronicky.
- Kontakt občana s veřejnou správou bude umožněn nepřetržitě 24 hodin denně a 7 dní v týdnu (jde o přímý přístup občanů do elektronických databází orgánů veřejné správy).
- Přístup ke službám bude umožněn na celém území ČR.
- Projekty k naplnění tohoto cíle budou zaměřeny na realizaci schválené Koncepce budování ISVS a na přijetí obecných principů označovaných jako e-Government (elektronická veřejná správa).

Těmito principy jsou zejména:

- běžné využívání informačních kiosků a prezentačních stránek na Internetu, jako dalších forem, jimiž lze plnohodnotně kontaktovat veřejnou správu (vedle osobních kontaktů „na přepážce“, poštovní korespondence, telefonem),
- služby veřejné správy, jako je poskytování informací, ale zejména vyřizování záležitostí občanů a podnikatelů, jsou dosažitelné 24 hodin denně a 7 dní v týdnu,
- realizace procesních změn ve způsobu práce úřadů, díky využití informačních a komunikačních technologií,
- výrazná „zákaznická“ orientace v přístupu pracovníků úřadů k jejich roli a k práci ve veřejné správě.

O FENOMÉNU VÝVOJE TECHNOLOGIÍ

Jiří Donát
Deloitte&Touche

V našem životě existují zážitky, na které se nezapomíná. Pro mě nastal takový okamžik letos v květnu, kdy jsem poprvé v životě navštívil legendární město Pompeje. Toto město mělo to „štěstí“, že bylo v sedmém desetiletí našeho letopočtu po výbuchu nedaleké sopky Vesuv během tří dnů zaživa pohřbeno a díky tomu zakonzervováno. Tato tragédie se z našeho pohledu dá přirovnat k zmrazení času. Jako by se někdo před 2000 lety rozhodl zachovat tehdejší město pro další generace. Jenom díky této tragické události nebyly Pompeje vystaveny neodvratným letitým vývojovým změnám – přestavbám, válkám, požárům.

Existuje jen málo tak silných zážitků, jako procházka městem, kde se před dvěma tisíci lety zastavil čas. Široké dlážděné ulice s chodníky, výstavními domy s attrii, dvě divadla (jedno přírodní a jedno zastřešené, používané též pro koncerty), aréna pro býčí zápasy, troje veřejné lázně, řada restaurací nabízejících teplé jídlo. Zejména procházka zachovalou lázeňskou budovou a pohled do mramorového bazénu evokují mrazení v zádech. Kdybychom se tak dokázali přenést do chvil, kdy byla tato místnost plná páry a koupajících se lidí. Kdybychom tak dokázali prohlédnout tímto nepředstavitelným oparem dávného času!

V takové souvislosti si člověk neodpustí zamyšlení. Zamyšlení o tom, jaká nová hodnota vlastně během těch dvou tisíc let naší novodobé civilizace vznikla. Čím (a zda vůbec) se naše vyspělá civilizace významně liší od civilizací dávno minulých, které již zhynuly v moři času.

A skutečně, existuje jen několik málo oblastí, které v antických městech nenalezneme. Výrazný pokrok je vidět snad pouze v oblasti dopravy (včetně letecké dopravy a kosmických letů), ve vzniku a v aplikacích elektrické energie a samozřejmě v oblasti informačních technologií, počínaje knihtiskem a konče technologiemi internetu.

Pojďme se tedy pokusit prodloužit pohled ze zmrazeného antického města přes naši dobu do budoucna.

Existují různé představy. Podle společnosti IBM bude průměrná domácnost budoucnosti obsahovat 15 počítačových systémů a za jediný den v ní proběhne průměrně 115 transakcí. Mezi připojenými zařízeními bude domácí systém, tedy nástupce dnešní televize, systém zásobování, včetně funkce automatického objednávání potravin a zboží denní potřeby, systém vytápění, který nám umožní optimalizovat spotřebu a přitom zajistit tepelný komfort již v okamžiku příchodu domů a samozřejmě i systém automatické ochrany. Možnosti závisí pouze na představivosti uživatelů.

Pojďme se nyní o jednu takovou představu pokusit.

Silvestrovská oslava

Dveře Integrovaného dopravního systému se s tichým akordem otevřely a Zdeněk vstoupil do svátečně ustrojeného bytu. Ve stejnou chvíli se obývacím pokojem rozezněly tóny Rybovy České mše vánoční. Tato skladba byla sice poněkud archaická, ale Zdeněk si ji hned při prvních tónech docela oblíbil. A to si ji zvolil spíše náhodou. Když se cestou domů probíral zprávami, Česká mše vánoční ho zaujala jako Doporučená skladba dekády ve speciální silvestrovské nabídce Integrovaného dopravního systému.

Zdeněk si nemusel odkládat kabát do šatníku; Integrovaný dopravní systém jej dopravil přímo z kanceláře, tak, jak byl Zdeněk ustrojen po celý den. A rozhodně to nebyl nezajímavý pohled. Zdeněk měl na sobě pohodlný vytahaný svetr, kalhoty, které ze všeho nejvíce připomínaly tepláky neurčité

barvy. Celkový obraz Zdeňka dokreslovaly široké velké trepky s vestavěným automatickým vyhříváním. Tento oděv se stal Zdeňkovým obvyklým kancelářským úborem již před několika lety a vlastně se tak oblékal od chvíle, kdy bylo konečně dořešeno komerčně dostupné retušování videotelefonních přenosů. Pokud tedy Zdeněk hovořil se zákazníkem své firmy, jeho skutečný oděv elektronickou cestou zmizel. A nejen oděv. Zmizely i Zdeňkovy prohlubující se vrásky a tmavé tukové váčky pod očima. Místo nich se na displeji videotelefonu objevila svěží tvář mladého sportujícího muže, jehož profesionální dojem ještě dále dokresloval dokonale padnoucí tmavý oblek, zářivě bílá košile a sametová kravata.

Výběr virtuálního kancelářského oděvu, tedy oděvu, do kterého je Zdeněk oblečen jen zdánlivě na displeji konferenčních zařízení, si Zdeněk původně nechával na cestu do práce; poslední dobou ale přišel trend přizpůsobovat virtuální oděv zcela dynamicky podle účastníků, typu a nálady rozhovoru. Zdeněk se tedy v IDS oddával už jen lenošení podmalovaném tichou hudbou a nechal všechny rutinní starosti na svém osobním systému. Nakonec, Zdeňkův systém věděl lépe než Zdeněk, jaké módní trendy se v současné době nosí, a navíc si i – na rozdíl od Zdeňka - pamatoval i vkus jednotlivých obchodních partnerů. V očích svého bankéře se tedy Zdeněk jevil velmi konzervativně: proužkovaný oblek ještě podkreslovaly úzké půlměsíčkové brýle; oproti tomu při rozhovorech s kamarády měl na sobě sportovní oděv a lehkou koženou bundu.

Mezitím ale Zdeněk pokročil dále do bytu. V kuchyni právě cinkla mikrovlnná trouba, jejíž činnost byla přesně koordinovaná s dopravním systémem a zároveň se vysunula Zdeňkova oblíbená vepřová pečeně. Aspoň v jídelníčku si Zdeněk do dnešních dní vybíral manuálně. Byla sice možnost používat výběr z doporučených týdenních jídelníčků, které respektovaly jeho aktuální zdravotní potřeby a hmotnost, a které se mu vtíravě nabízely vždy začátkem týdne. S obrovskou chutí ale Zdeněk tyto sestavy porušoval. Většinou k tomu došlo pozdě večer, kdy podlehl okamžitému popudu a objednal si to, co by v jídelníčku nikdy nenašel. Většinou se jednalo o co nejostřejší minutku, a ta byla vzápětí promptně dopravena do bytu Integrovaným dopravním systémem.

Zdeněk došel až k troubě a vyjmul čerstvě připravený pokrm. Právě jej chtěl navyklým pohybem posunout na stůl, když tu se zarazil. Z vedlejšího pokoje totiž zazníval podivný šramot, který občas doprovázely tlumené údery.

„Ty jsi už doma, Petře?“, zeptal se Zdeněk nahlas. Otázka však zůstala nezodpovězena. Zdeněk odložil talíř a ve zlé předtuše zamířil k pokoji svého syna. Až nyní si uvědomil, proč mu na volání nikdo neodpovídá. Jeho sedmiletý syn Petr byl totiž plně zabrán novou virtuální hrou Zabij a uteč. Co naplat, že ji měl od obou rodičů zakázánou. Vypadalo to, že využil příležitosti, kdy nebyl nikdo doma, a hbitě vlezl do zařízení virtuální reality. Vyhledání hry a její spuštění bylo záležitostí několika minut i pro předškolní děti, natož pro Petra..

Po pravdě řečeno, Petr ani nebyl v zařízení vidět. Celou hlavu mu zakrývala velká helma obsahující dva miniaturní displeje pro stereoskopické vidění, dvojici vysoce kvalitních odhlučněných sluchátek zajišťujících prostorový vjem, a především to nejdůležitější: přesný bezdrátový snímač pohybu. Každé pootočení Petrovy hlavy i každý pohyb jeho končetin byl ihned přenesen do počítače, a ten věrně upravil herní scénu.

Teď sebou Petr trhl: bylo vidět, že ve své virtuální skutečnosti právě bojuje nejméně s dvanáctihlavým drakem. Nebo to byl mimozemšťan? Kdo ví, zvenčí to nebylo vidět a hra Zabij a uteč nabízela mnoho variant. Petrova pravá ruka jako by třímala meč, ve skutečnosti však držela jen jeden z ovladačů vybaveným silovou zpětnou vazbou, tzv. feedbackem. Pokud tedy Petrův meč narazil do virtuální příšery, Petr tento náraz také skutečně cítil. Zuřivé nekoordinované pohyby a Petrova zpocená tvář dokonale dokreslovaly realitu hry. Občas se Petr neovládl a celý nadskočil – odtud se tedy ozývaly ty rány!

Zdeněk rázně přistoupil k ovladači a přístroj vypnul. Petr sebou nejprve silně cukl, několikrát škubl celým tělem, a až po dalších dlouhých vteřinách se jeho dětské tělíčko sesunulo na zem. I na zemi sebou Petr ještě chvíli zmítal, a teprve po chvíli zůstal bezvládně ležet. Tento klid ale netrval dlouho. Najednou se Petr zvedl, prudkým pohybem strhl helmu ze své hlavy, a hystericky se rozječel: „Tos mi musel udělat zrovna teď? Když už jsem ho skoro měl? Vždyť stačila už jen chvilka a mohl jsem se dostat do další...“

„Tak moment mladej“, vložil se do toho Zdeněk. „Tak především, kdo ti povolil tu hru pustit?“

Petr se konečně začal zklidňovat, stále však nebyl schopen slova.

„Dobře, to si teda ještě vyřešíme“, dodal přísně Zdeněk. „Za druhý, proč nejsi ve škole?“

„Protože, protože“, špitl Petr, který se již konečně vrátil do reality a začal si uvědomovat vážnost situace. „Protože nás paní učitelka dnes pustila dřív. Když je ten Silvestr,“ špitl.

„Doufám, že si nevymýšlíš,“ zaburácel Zdeněk. „Víš, že lež má krátké nohy a já si to mohu snadno ověřit,“ dodat výchovně a sáhl do kapsy pro svého osobního digitálního asistenta. V okamžiku se jeho přístroj spojil s informačním systémem školy. „Máš štěstí“, dodal již smířlivěji. „skutečně na nástěnce vaší třídy oznamují rodičům zkrácení výuky. Jak to ale vyřešíme s tou nepovolenou hrou?“

„Já už budu hodnej,“ navrhl Petr.

„No nevím, když jsou teda ty svátky,“ začal váhat Zdeněk. „Už jsi něco jedl?“, zeptal se věcně, čímž naznačil, že je nebezpečí zažehnáno.

„Vlastně jsem ještě neměl čas“, zkroušeně připustil Petr.

„Že tady ještě není maminka“, podivil se Zdeněk. „No nic, zvládneme to i bez ní“, dodal a přistoupil k hlavnímu ovládacímu panelu kuchyně. Na panelu začaly naskakovat nabídky jídel, která by se dala připravit ze stávajících zásob v kuchyni. Nabídky byly navíc seřazeny podle doby přípravy pokrmu. „Dáš si kaši? Tu můžeš mít za pět minut. Dobře,“ nečekal na odpověď a zvýšil hlas: „Dá si kaši!“ oznámil do mikrofonu kuchyňského systému.

Vtom zazněl gong Integrovaného dopravního systému a do bytu vplula Lenka. Její ladná štíhlá postava kontrastovala s postavou Zdeňka, téměř to vypadalo, jako by se ti dva poznali v retušované videokonferenci. A vlastně to bylo docela možné. „Promiň, zdržela jsem se v práci,“ zahlaholila. „Zrovna jsem zkoušela na dálku jednoho žáka, bohužel se ta zkouška protáhla. Nezlobil?“ obrátila hlavu k Petrovi.

„Maminko, to jsem rád, že už jsi doma“, snažil se Péťa včas otázku zamluvit. „Já už tu hru hrát nebudu, slíbil jsem to tátovi“, dodal rychle.

„Jakou hru?“, otázala se Lenka.

„Dobře, pro dnešek to tedy smažeme,“ zasáhl do hovoru Zdeněk, který si evidentně nechtěl kazit sváteční den.

Petrova kaše se vysunula z kuchyňského systému téměř současně s jídlem Lenky. „Čím ho to krmíš?“, podivila se Lenka. „To mu nemůžeš dát pořádné jídlo?“

„Já mám kaši rád,“ přispěchal na obranu svého otce Péťa.

„Pojďme už radši jíst“, uzavřel diskusi Zdeněk. Všichni tři se odebrali ke kulatému stolu v rohu místnosti. Z jedné strany stolu bylo velké okno, z druhé neméně veliký displej. Pokud byl kdokoliv doma, displej byl neustále plný nejnovějších zpráv. V přítomnosti Zdeňka bylo nastaveno promítání technických novinek, politiky a sportu, pokud byla doma Lenka, displej byl plný módních modelů,

kulturních senzací a drbů doslova z celého světa. Pokud byli u stolu oba, displej se automaticky vypnul: byl tak totiž nastaven. Předpokládalo se totiž, že je čas na rozhovor. A tento okamžik nastal i nyní.

„Tak co, jaký jsi měla den?“, začal Zdeněk.

„Ale, ani se neptej. Představ si, že nás v práci drželi ještě o půl hodiny déle než normálně. A to je svátek. Jsem zvědava, jak vůbec stihneme tu oslavu připravit. V kolik tady mají být Kubátovi?“

„Říkali, že mezi půl sedmou a sedmou. Neboj se, na všechno je ještě dost času“, uklidnil Lenku Zdeněk. „A kromě toho, jaká příprava. Když to nestihneme, prostě si pohoštění objednáme.“

„To chci vidět, jak o svátcích a na poslední chvíli ještě něco dostaneme,“odvětila Lenka pragmaticky, ale již vlídněji.

„Stejně je mi ale divné, že ve škole pracujete i na Silvestra. Pokud si dobře vzpomínám, dokonce i já jsem ještě jako dítě míval o Vánocích prázdniny.“

„Nevím, čemu se diviš. Dnes to snad ani jinak nejde. Vždyť děti si samy stanovují své osnovy od páté třídy, a jejich rodiče do osnov mají co mluvit vlastně už od první třídy. Dovedeš si vůbec představit, jak by se ozvali ti rodiče, kteří Vánoce prostě neslaví? Snad jsi to měl jako dítě lepší, to nevím. Ale určitě to měl lepší tvůj učitel,“ povzdychla si Lenka smutně. „Ještě že nás rodiče nenutí sloužit ve škole i v noci. To naštěstí musí děti spát. Doufám, že aspoň tohle se hned tak nezmění...“ zamyslela se.

„Bohužel, na rozdíl od letních prázdnin. Ty nám zrušili před třemi lety.“

„Kolik dětí vlastně přes léto studuje?“, zeptal se Zdeněk.

„Stále ještě zanedbatelné množství. Necelých deset procent. Ty si potom vybírají hlavní prázdniny přes zimu nebo na jaře. Takže nějak se s kolegyněmi na léto nakonec stejně vystřídáme. Pořád ještě budeme moci vyrazit v létě na rodinnou dovolenou,“ usmála se Lenka vlídně. „Už jsi něco naplánoval?“

„Mám už jeden nápad. Ale bude to pro tebe opravdové překvapení“.

„Tak mě přece nenapínej, Zdeněčku!“

Tichý akord IDS jako by nechtěl narušovat příjemný rozhovor. Ale stalo se. Zdeněk jen s nechutí povolil otevření dveří nečekané návštěvě. Vzápětí do pokoje vstoupili Kubátovi: vytáhlý Standa, drobnější Jana i jejich osmiletý syn Míša.

„Ahoj Kubátovi, co tak brzy?“, přivítal příchozí Zdeněk. Ještě jsme vás ani nečekali – není ani šest hodin...“

„Tak to je pro změnu naše překvapení“, ujal se slova Standa. „Všimli jsme si, jak jsme vám při naší poslední návštěvě přidělali práci...“

„Před rokem jsme chlebíčky připravovali až do jedenácti – na oslavu pomalu ani nezbyl čas“, doplnila ho Jana.

„Náhodou jsme to nakonec oslavili až moc dobře“, oponoval Zdeněk.

„To je pravda,“ připustil Standa, „do rána zbylo ještě dost času. To ale neznamená, že to letos nemůže být lepší! Už to prozraď, Jani.“

„Právě před týdnem totiž otevřeli dvě stě metrů od naší chalupy terminál IDS“, pochlubila se Jana. „Měl být hotov až na jaře, ale nějak si pospíšili. Zelená lhota je tedy snad úplně první vesnicí v jižních Čechách, kam se už dá takhle pohodlně jezdit“.

„No to je skvělé!“, rozzářila se Lenka

„Máme už na chalupě pro vás všechno připravené. A takový kulatý letopočet, ten si přece zaslouží pořádnou oslavu na venkově“, dodal Standa vesele.

„Takže nasedat. Za dvacet minut budeme na místě,“ pobídla přítomné Jana.

„To je tak akorát na vypití jedné uvítací skleničky“, usoudil Zdeněk a sáhl do ledničky pro láhev.

„Nezapomeňte si obléci něco na sebe“, upozornila Jana. „To víte, vesnice. Bude ještě nejmíň půl roku trvat, než rozvedou IDS až do chalup“.

„Ale aspoň se projdeme a bude nám pak o to víc chutnat,“ usmál se Zdeněk a zamířil ke dveřím.

„Počkej ještě, kam jsem vlastně dala tvůj kabát? Dobře rok jsem ho neviděla“, namítla Lenka.

„Nebude na půdě?“, vzpomněl si Zdeněk. „Moment, hned to zařídím“, sundal ze stropu schůdky a za chvíli zmizel. „Mám ho. Je tady dokonce i Péťův, beru oba“.

„Jen aby mezitím nebyl Péťovi malý,“ obávala se Lenka. „Ukaž, vyzkoušíme ho,“ zavolala Petra k sobě. „No, jen tak tak,“ zhodnotila. „Příští zimu musí mít nový,“ oznámila nesmlouvavě. To se už ale celá skupina přesunula do kabinky dopravního systému.

„Takže na oslavu vašeho nového terminálu IDS,“ navrhl přípitek Zdeněk hned poté, co se kabinka nehlučně rozjela.

„Ale to snad ne“, oponovala Jana.

„Tak na co tedy?“, otázal se Standa.

„No přece - na zdraví!“, usmála se Lenka. „Kdo je pro?“

Nikdo se neozval. Místo toho zaznělo malou místností dopravního systému cinknutí skleniček vyrobených ze speciálního znělého skla.

Na obloze vyšly první hvězdy. Ve stěně bývalého transformátoru na návsi Zelené lhoty se otevřely nenápadné automatické dveře. Vyšly z nich dvě dvojice šťastných lidí v povznesené náladě. A děti byly spokojené, že ještě nemusejí spát.

Naštěstí existují věci, které nezmění ani technika.

RIZIKA ŽIVOTA V KYBERNETICKÉM PROSTORU

Ing. Tomáš Přibyl
AEC, spol. s r.o., tomas.pribyl@aec.cz

Reálný svět má své podsvětí. Stejně tak kybernetický prostor má i svůj „podprostor"- a „žít" (tedy pohybovat se) v něm představuje velké riziko. Samozřejmě tu vyvstává dětská otázka: Proč?

V reálném světě jsou rizika celkem snadno představitelnou záležitostí (čerstvě natřené zábradlí, špatně označený výkop, pes Baskervillský v ulicích noční Prahy…), v kybernetickém prostoru je to horší. Alespoň pro většinu uživatelů – největší hrozbu pro ně představuje poškození, zničení či odcizení hardware. Ani si přitom neuvědomují, že tyto hrozby patří do reálného světa. Kybernetický prostor je totiž o něčem úplně jiném. Uvědomíte si to asi nejlépe v okamžiku, kdy se s některou z výše uvedených hardwarových „katastrof" setkáte – smutek nad ztrátou notebooku po týdnu přebolí, ale obsah jeho pevného disku vás bude strašit ještě dlouho. Komu se asi dostanou do ruky kontakty na vaše obchodní či soukromé partnery (a partnerky), kdo se teď jistě ne z dlouhé chvíle věnuje studiu vašich smluv či účetnictví?

Na následujících řádcích se pokusíme vyjmenovat některá rizika, která s sebou život v kyberprostoru přináší. V žádném případě si nenárokujeme patent na jejich úplný výčet, ale pouze na stručný přehled těch nejmarkantnějších. Rizika života v kyberprostoru jsou následující:

Odcizení dat

Používat v kyberprostoru slovo „krádež" je poněkud ošemetné a správnou formulaci bych raději nechal právníkům. Pokud si někdo stáhne data někoho jiného, tak je sice „ukradne", ale na původním nosiči dat nic nechybí (pokud je ovšem neštípne i s médiem). O to je ale zcizení dat nebezpečnější – poškozená strana ani nemusí tušit, že se stala obětí útoku. Naopak, útočník má všechny trumfy na své straně, neboť si může vybrat čas, místo a způsob útoku. Když vám někdo v reálné světě uzme např. osobní doklady, tušíte, že je může zneužít a začnete připravovat protiopatření. Při odcizení informací o bankovní kartě v digitálním světě ovšem netušíte dlouho nic a zhrozíte se až jednoho krásného dne při pohledu na svůj bankovní účet po důkladné odtučňovací kůře. Zpravidla nejprve podezříváte (většinou neoprávněně) svůj bankovní ústav.

Zneužití informací

Problém úzce související s výše uvedenou oblastí. Přímo čítankový příklad zneužití informací je neoprávněné použití údajů o cizí bankovní kartě (viz. výše). Ovšem zneužít lze i jiná data – například obyčejnou e-mailovou poštu. Vzhledem k tomu, že drtivá většina zpráv prochází po Internetu ve formě otevřeného textu (těch pár šílenců, kteří pochopili nutnost šifrování a digitálního podepisování se setkává se všeobecným opovržením a obviňováním ze „zpomalování a komplikování internetového provozu"), není problém je na kterémkoliv počítači na cestě přečíst. Představte si, že s přítelkyní (resp. přítelem) domlouváte schůzku na večer. Kdo o tomto diskrétním setkání v příšeří parku může vědět? Minimálně správci obou vašich poštovních serverů plus všichni správci počítačů, kteří se nacházejí na cestě mezi Vámi a Vaší milou (resp. milým). Pokud šifrujete a digitálně podepisujete, správci si ani neškrtnou a vy máte jistotu, že se večer pod lampou nestanete obětí sabotážní akce „přejícího" kamaráda.

Manipulace s informacemi

Pokud někdo získá přístup k citlivým informacím, je jen krůček k tomu, aby je modifikoval. Představte si, že se někdo čirou náhodou dostane dokumentům s cenovými nabídkami, které činíte možnému zákazníkovi v klíčovém kontraktu. Není pak pro něj problém buď nabídnout cenu lepší (to se ovšem

týká bodu vyššího – zneužití informací) anebo (proč by se připravoval o svůj zisk, že?) zvýšit vaši nabídku do nadoblačných výšin. Kdo pak z konkursu vyjde vítězně, nechť si laskavý čtenář dovtípí sám.

Monitorování komunikace

Všechno souvisí se vším, neboť jednotlivá popisovaná rizika se navzájem úzce prolínají. Data nemusíte ani odcizovat (tedy schraňovat pro svou či cizí potřebu), ani zneužívat, ani s nimi manipulovat, docela postačí, když je monitorujete. Jak se říká – chytrému napověz… Pouhé vysledování skupiny zákazníků, kterou se prostřednictvím vaší společnosti snažíte oslovit může někomu ušetřit mnoho námahy. Ne nadarmo se praví „řekni mi, co čteš a já ti řeknu, kdo jsi“.

Tolik tedy k základním kategoriím rizik života v kyberprostoru. A nyní ještě několik spíše obecnějších poznámek. Všeobecně platí, že jakmile se připojím byť i prostřednictvím modemu do Internetu, otevírám olbřímí bránu, kterou mohou proudit informace nejen dovnitř, ale i ven. A nemám teď na mysli pouze e-mailovou poštu – informace o sobě prozrazujete každou chvíli někde na Internetu prostřednictvím různých dotazníků (jejich vyplněním je dnes podmíněno stažení mnoha nejrůznějších programků utilitek či informací). Uživatel pak v dobré víře, že je to „zadarmo“ dotazníček vyplní a pak se diví, že se mu v e-mailové schránce po čase objevuje obrovské množství nevyžádané pošty (mimochodem, jedna z nejhorších forem reklamy – vzhledem k cenám za využívání Internetu si spočítejte, kolik stojí uživatele stahování nevyžádané pošty). Pojem „zadarmo“ po vyplnění dotazníku na Internetu se rovná ceně ztráty části soukromí – ostatně, jak by se vám v praxi líbilo, kdyby v vašich dveří zazvonil mladík v černých brýlích a otrhaných džínách a nabídl vám „zadarmo“ nějaký (byť zajímavý) produkt zdarma výměnou za to, že si prohlédne a nafotografuje váš byt? Vypustili byste jej dál? Vidíte – a na Internetu to děláte dnes a denně…

Všeobecně platí, že čím více toho povolím, tím většímu riziku se vystavuji. Z tohoto hlediska jsou nebezpeční především tzv. běžní uživatelé, kteří se rozhodnout využít nějaké nabídky Internetu zdarma, koupí si modem a vůbec netuší, co dělají. Pokud si navíc nainstalují nějaký „bezpečnostní“ program, přidává se k neznalosti ještě falešný pocit bezpečí (třeba takový špatně používaný antivirový program a ledově klidný uživatel je horší než žádný antivirový program a opatrný uživatel).

Nebezpečí představují též různé programky hojně posílané elektronickou poštou nebo stahované z nejrůznějších „zákoutí“ Internetu. Nemusí sice pokaždé obsahovat přímo virus, škodlivý kód může mít i podobu trojského koně. Tzv. trojský kůň je kus programového kódu, který se (obrazně řečeno) „přilepí“ k nějakému jinému programu (např. soubor na testování výkonu procesoru či tančící africká kráska) a zatímco se uživatel věnuje jeho sledování, trojský kůň na pozadí např. zjišťuje přístupová hesla k Internetu či e-mailem vesele odesílá nahodilé dokumenty do světa (že přitom nedělá rozdíl mezi dokumenty veřejnými a citlivými, jistě není třeba zdůrazňovat). Bohužel si většina uživatelů PC stále ještě neuvědomuje, že: Ne vše, co se děje v počítači, vidíte na obrazovce!

Takže pozor, mimo různých více či méně pochybných individuí, je Vaším největším nepřítelem NEZNALOST!

OCHRANA ŽIVOTA V KYBERNETICKÉM PROSTORU

Ing. Jiří Mrnuštík
AEC, spol. s r.o.

Fenoménem, společným jmenovatelem a nejčasteji používaným slovem posledních let a měsíců je slovo GLOBALIZACE. Je naprosto neoddělitelně spjato s největší heterogenní světovou počítačovou sítí INTERNETEM.

V rámci společností se spojováním groupwareového prostředí a webovských technologií vytváří Intranet. Spojování Intranetů do Internetu a propojování obrovského množství heterogenních sítí dochází k vyvtáření nového fenoménu – elektonického prostoru. Prostředí elektronického prostoru se zdá konečně předurčeno k tomu, aby se stalo nepostradatelnou výpočetní technologií tím, že poskytuje nastavitelnou komunikaci, spolupráci a koordinaci mezi službami a lidmi. Stejně jako word processor a tabulky se elektronický prostor stává hlavním produktem velkých i malých organizací, a to především díky ziskům v produktivitě, které neustále představuje. Ale technologie skrytá za tímto dokonalým prostředím a umožňující jeho fungování vytvoří vážný virový problém pro ty organizace, které na něj spoléhají.

Účelem tohoto článku je jak osvětlit nebezpečí spojené s počítačovými viry v prostředí elektronického prostoru, tak prověřit strategie obrany proti této hrozbě. Ukážeme si, jak prostředí elektronického prostoru obnovilo aktuální virový problém, zvláště problém makrovirů, a jak poskytlo nutné prvky pro rozšíření zcela nových a mnohem více devastujících typů.

Co to vlastně znamená elektronický prostor?

Celý efekt je dán jedinou skutečnost, kterou je KONEKTIVITA. Každý je a nebo bude dříve či později spojený s každým. Každý den se desetitisíce jednotlivců či firem připojí jako noví uživatelé INTERNETU, což sebou přináší zajímavou situaci, že na žádný konec světa není elektronicky daleko a požadované, či nabízené informace se mohou předávat a přenášet takřka okamžitě (DATOVÁ GLOBALIZACE). Nikoho z Vás ani nenapadne se podivovat, proč a jak je možné okamžitě číst informace z WWW stránky na opačné straně Globu, stejnětak se nepodivujete, proč odeslaný e-mail dosáhne adresáta za pár okamžiků. Naopak se podivujete, když po pár minutách ještě nemáte odpověď. On-line chatting a videokonference dávají výměně informací nový rozměr. Nový elektronický prostor přináší nové rozměry pro týmovou práci, kterými je Konektivita, Kooperace, Spolupráce.

Všechny webovské servery, FTP servery, e-mailové servery a jejich uživatelé vytvářejí dohromady (hardware, software, informace a uživatelé) vytvářejí novou kategorii, kterou je možno bez nadsázky nazvat novým postorem, jehož dimenze jsou tvořeny již zmínenými čtyřmi prvky – hardwarem, softwarem, informacemi a uživately. Tak jako se matematické prostory (například prostor komplexních čísel, či prostor eliptických křivek na Galoisových polích, nebo jiné) řídí jistými axiomatickými pravidly a z nich odvozenými zákonitostmi, tak se i tento prostor řídí jistými zákonitostmi položenými na a odvozenými z jistých axiomů. Předpokládám, že Nobelova cena čeká na toho, kdo tyto axiomy definuje a soubor zákonů z nich odvodí a dokáže. Pracovní název „Kybernetický prostor“, zkrácene Kyberprostor není originální, jistě bude vyhovovat příznivcům S-F a pro označení je vyhovující.

Technologie použité a používané v Kyberprostoru

Nové prostředí je umožněno kombinací pokročilývch technologií převzatých z mnoha oblastí. Některé z klíčových umožňujících technologií, zahrnutých do prostředí Kyberprostoru, jsou následující:

Systém zpráv	Systém zpráv je klíčovou službou, kterou musí mít všechny pužité produkty.
Depozitář dokumentů	Podsystém ukládání orientovaný na dokumenty je navržen tak, aby ošetřil nestrukturovaná data a bohatý typ médií spojených s dokumenty prostředí Kyberprostoru.
Replikace dokumentů	Replikace překonává nevýhodu geograficky odděleného týmu tím, že vytváří přesně stejné kopie dokumentů na několika serverech, které jsou uloženy na pracovním místě každého z uživatelů.
Přístup na dálku	Úspěšná integrace požadavků na mobilní využívání výpočetní techniky vyžaduje dostupnost této technologie.
Digitální podpisy	Autentizuje původce dokumentu nebo zprávy.
Silné šifrování	Umožňuje zajištění nutného soukromí vyžadovaného pro citlivá data.
Workflow agenti	Umožňuje agentům (makrům) být vloženy do dokumentů a zpráv za účelem provedení předdefinovaných kroků.
Makrojazyk	Mocné makrojazyky jsou k dispozici pro vytvoření aplikací a komplexní workflows v rámci prostředí Kyberprostoru.
Internetová integrace	Podpora inregrovaného internetovského protokolu pro HTTP, FTP, NNTPm GOPHER, SMTP a POP3, Java apod.

Výhody nové virtuální reality Kyberprostoru

- Konektivita mnoha různými prostředky umožňuje téměř každému najít svůj způsob jak předávat a přijímat informace, i když různorodost je na úkor standardizaci.
- V internetovském Kyberprostoru je možno najít téměř jakoukoliv informaci, nebo se na ni zeptat takového množství jedinců (lidí), že alespoň jeden ji bude znát, nebo ji koupit.
- Svoje myšlenky, ideály a nápady lze současně, či ve velmi krátkém čase sdělit takovému množství entit (lidí, serverů Webovských stránek) že propagační efekt je ohromující a naprosto nesrovnatelný s jakýmkoliv médiem v minulosti i současnost, snad kromě televize, která však postrádá interoperabilitu.
- Konkrétněji formulované výhody jsou, například okamžitý přenos operačních dat potřebných pro řízení procesů, on-line onformační databáze pro okamžité rozhodování na základě znalostních bází a mnohé další.
- Bezhotovostní platební styk a elektronický obchod je to co Internetovských Kyberprostorem hýbe kupředu. Peníze jsou nazacím olejem a elektronický obchod motorem.

Nevýhody

- Kdo si ještě neuvědomil, že informace znamenají moc a peníze? Asi hloupá otázka, nejspíš každý. Kdo by si nepřál vědět, že na pozemku, který zdědil po babičce a kde jen jen zplanělá zahrádka, povede za dva roky dálnice. Prodat?/neprodat? A za kolik? Kdo by nechtěl vědět, že v Jižní Americe byla objevena nová měděná ložiska s povrchovou těžbou alespoň v takovém předstihu, aby mohl prodat svoje akcije, než padnou na kolena?
- Nezapomeňte, za Internetovským prostoru nejsou vidět jen data, která tam chcete uveřejnit. Kanál, kterým do Internetu vstupujete je OBOUSMĚRNÝ. Vaše internetovská brána vede do Vaší firemní sítě, to je i potenciální dálnice pro lovce informací. Myslíte si, že nikdo nechce vědět jakou obchodní strategii na trhu IT Security zaujme Vaše firma v příštím roce? Já ano!
- Nakupujete elektronicky? Maličkosti za babku? Stačí jednou zjistit číslo Vaší kreditní karty a někdo jiný bude nakupovat na Váš účet.
- Jste si jisti, že v poště, kterou čtete a rozesíláte denně na desítky a možná stovky míst není virus, a jste si jisti, že nikdo jiný, než Vy a Váš komunikační partner nečte tuto poštu?

Kybernetický prostor vytváří obrovské možnosti a to jak pro jeho positivní použití, tak i k jeho zneužití. Svého soukromí si všichni vážíme a je chráněno zákony a chartami. Soukromí v prostoru informací je něco zcela jiného. Přistihnout zde pachatele, který Vám ukradl informace, strategické plány a podobně lze jen velmi obtížně. Postižený často ani nepozná, že k něčemu takovému došlo a jen se diví jakou ta konkurence má intuici. Ukradená data totiž nezmizí a nelze ani říct, kolikrát byla okopírována.

Další nová rizika plynoucí z technologií v Kyberprostoru

Groupwareové prostředky, které jsou součástí těchto tecnologií datové globalizace, podporují vnořené a připojené soubory, jak u zpráv, tak u dokumentů (attachmenty). Funkce připojování souborů umožňuje uživatelům posílat si navzájem binární data a proveditelné soubory tím, že je připojí k mailové zprávě nebo k dokumentu. Známým rizikem je skutečnost, že připojený soubor může být infikován virem specifickým pro danou platformu. Avšak, aby bylo možno aktivovat tento virus, potřebuje uživatel připojený soubor a otevřít/spustit jej. Výjimkou jsou případy, kdy se trojské koně aktivují nezávisle a spustí připojený soubor. V prostředí Lotus Notes je velmi obvyklé, zahrnout tlačítková makra, která provedou odpojení souboru a jeho spuštění ve zprávě. S velmi malým úsilím může být tato technika přeměněna na vypouštěč virů, který může rovněž zahrnovat logiku, schopnou vypnout lokální antivirový skener.

Větším problémem je však rychlost, s níž replikace a zprávy mohou šířit infikovaný připojený soubor v prostředí groupware. Charakteristiky šíření mohou potenciálně zahrnovat velké množství uživatelů infikovaných jediným virem v poměrně krátkém časovém období. Virus I love you je toho nedávným zářným příkladem.

Prostředí Kyberprostor jako celek zahrnuje také řadu technologií, které spektrum virů pro takové prostředí velmi rozšiřuje. Kombinace workflow agentů s mocnými makrojazyky a konektivita je ideálním prostředím pro podporu makrovirů a kombinovaných makro/binárních virů.

Jeden z aspektů virů specifických pro prostředí groupware a Kyberprostoru je, že se mohou šířit velmi rychle. Je-li dokument nebo zpráva čtena, takový virus se může aktivovat a může snadno sám sebe poslat náhodné sadě platných příjemců a/nebo může sám sebe zkopírovat do nových databází. Následující tabulka ilustruje poměrně konzervativní model organizace o 1000 uživatelích, kteří kontrolují svoji poštu v průměru dvakrát denně.

	Celk. počet infekcí	Odeslaných infikovaných pošt	Odeslané nové cílové pošty	Nové infekce	Procento infekcí
Den 1 - 13.00	1	10	10	10	1%
Den 1 - 17.00	11	100	100	93	10 %
Den 2 - 13.00	104	1000	930	359	46 %
Den 2 - 17.00	463	9300	3590	70	53 %
Den 3 - 13.00	533	35900	700	38	57 %
Den 3 - 17.00	571	7000	380	39	61 %
Den 4 - 13.00	610	3800	390	30	64 %
Den 4 - 17.00	640	3900	300	23	66 %
Den 5 - 13.00	663	3000	230	17	68 %
Den 5 - 17.00	680	2300	170	13	69 %

Jak každý může vidět, během 36 hodin je infikována téměř polovina organizace. Jestliže je tato organizace napojena na jiné firmy, je velmi pravděpodobné, že virus bude také infikovat tyto cizí systémy. Navíc dojde po čase k zahlcení poštovního serveru a totálnímu kolapsu kominikace.

A co jinak?

Nejde samozřejmě jen o virovou nákazu. Kybernetický prostor se svými technologiemi umožňuje velmi dobře sledovat pohyb osob pomocí monitorování použití jejich kreditních karet, mobilních telefonů, připojení jejich mobilních počítačů, pomocí odposlouchávání hovorů, čtení elektronické pošty a podobně. To dává prostor k vydírání, únosů a terorismu.

Definujme nyní základní kategorie problémů

1. Virová nákaza
    - Přenášená v e-mailech a to ve všech typech souborů, které jsou kompatibilní a používají MS Visual Basic for Applications (Dokumenty, XLS, PPT a jiné)
    - Přenášená v aktivních prvcích WWW stránek, jako například Java Applety, OCX a podobně.
    - Viry přenášené ve vykonatelných souborech, které jsou tak snadno dostupné v Internetu
    - Viry šířené s použitím těchto moderních technologií
2. Hackeři a jejich činnost s průniky spojená
    - Ukradení dat, špionáž a průmyslová špionáž
    - Vydírání, ať již na základě průniku k informacím, nebo na základě průniku do sítí, jejich zašifrovaní či jiná destruktivní infekce a následná vydírání pod hrozbou destrukce dat. Dokonce je pro některé prestižní firmy nebezpečné vydírání již jen samotných faktem možnosti průniku, který hrozí ztrátou klientů.
    - Poškozování práce a ztráta kredibility, například zničením či modifikací Web stránky. Toto je asi nejmírnější forma poškození.

- Únosy, způsobené získáním citlivých informací o osobách z elektronické sítě, které jsou pak k únosu použity. Dobrým příkladem je například sledování použití elektronické platební karty, místa použití, utracené částky, denní doba použití, periodicita. Tak je možno poměrně snadno vytvořit kompletní profil člověka.
- Teroristické akce, například průnikem do letišťního či bankovního systému a jeho zničení, či dočasné vyřazení z provozu. Toto může způsobit obrovské ztráty jak finanční, tak i ztrátu kredibility, tak I ztráty na životech. Viz, příklad s nemocničním informačním systémem.

3. Úniky zpusobené Sniffingem, a to jak e-mailů, tak například sledovaním toku paketů v síti.
   - Ztráta osobního tajemství a ztráta informací, či jejich zneužití, pokud jsou posílány e-mailem. E-mail může číst každý administrátor sítě či serveru, přes který e-maily prohází.
   - Odezíraní hesel nebo čísel platebních karet v elektronickém obchodní a platebním styku
   - Špionáž v souborech procházejících sítí a jiné podobné typu útoků, jako například podstrčení matoucích dat a podobně.

V každém prostoru je třeba a možno žít, definujme proto protiopatření

Kybernetický prostor, jako nové datové Universum, se pro nás stává realitou denního života a je nezbytné se něm naučit žít a přežít. Základním protiopatření je odpojit počítač od sítě, vymontovat disketové mechaniky, zamknout jej do ocelové bedny a odpojit síťový kabel. Takto chráněný počítač je opravdu bezpečný a data mohou být těžko zneužita.

Jaká základní bezpečnostní opatření je třeba přijmout?

Modely některých řešení:

1. Zabezpečení webovských stránek proti virům

Největší nebezpečí při použití Webovských stránek pro vyhledávání informací je virová nákaza, a to jak z hlediska makrovirů, tak i škodlivých a destruktivních aktivních prvků. Jejich vlivem může dojít k infikování počítače uživatele či celé počítačové sítě. Takový zavlečený virus může způsobit nenahraditelné finační ztráty, nebo totální destrukci dat. Je tedy třeba být, při používání Webovských stránek velmi obezřetný. Antivirové programy současné generace poskytují v této oblasti silnou ochranu, ale jsou vždy krok za tvůrci virů. Taková ochrana je tedy nezbytná, avšak není dostatečná. Kryptografie v této oblasti pomáhá tak, že autentizuje jak server, tak i jeho uživatele pomocí asymetrické kryptografie a certifikátů serveru a uživatele. Každý objekt na WWW serveru je autentizován a digitálně podepsán soukromým klíčem serveru a klient je schopen tento podpis ověřit ještě před tím, než jej použije či spustí na svém počítači. Toto není přímá ochrana proti virům, ale nepřímo, metodou neobejitelného digitálního podpisu, ověřuje, že použitá data jsou z důvěryhodného zdroje. Tato ochranná metoda není závislá na průzkumu a rychlé reakci na tvorbu nových virů. Metoda je založena na důvěryhodnosti certifikátu a současně i na důvěryhodnosti třetí strany, která data poskytuje.

2. Zabezpečení webovského elektronického obchodu

U elektronického obchodu na Internetu je největším nebezpečím odposlechnutí a následné zneužití dat vyměňovaných mezi serverem a klientem. Zde již pouze autentizace obou komunikačních partnerů

nestačí. V nebezpečí jsou jak přístupová hesla do účtů jednotlivých uživatelů webovského obchodního domu, například chránící čerpání předplacených služeb, nebo čísla kreditních karet putujících nechráněnou sítí při elektronickém nákupu ve virtuálním obchodním domě. Samozřejmě autentifikace serveru zůstává, ale informace putující například Internetem musí být navíc šifrované. Zde nastupují tzv. Šifrované tunely, které se pomocí kommbinace symetrické a asymetrické kryptografie vytvářejí mezi serverem auživatelem, přičemž asymetrická kryptografie, používající certifikáty serveru a klienta je naprosto nenahraditelná. Vzájemná autentizace serveru a klienta proběhne pomocí výměny certifikátů a určitých informací podle mezinárodního standardu X.509, potéi se mezi serverem a klientem vymění bezpečnou cestou symetrický šifrovací klíč probíhající session a další komunikace je již šifrovaná a tedy bezpečná. Hesla k účtů ztrácejí smysl, protože identifikace klienta serveru probíhá na podstatně bezpečnější, kryptografiké úrovni a všechny další informace probíhají pak veřejnou sítí šifrovaně, včetně například čísel kreditních karet. Základní roli tu opět hraje asymetrická kryptografie a certifikáty klíčů.

3. Zabezpečení e-mailů

Kdo by si přál, aby jeho e-maily byly veřejně čteny a navíc pokud obsahují soukromé a citlivé informace? E-maily je možné chránit šifrováním, tak, že pouze adresát je schopen takový mail přečíst. Navíc kryptografie dovoluje nejen informace utajit, ale také zabezpečit kontrolu jejich nepoškozenosti a soušasně taková mail nezpochybnitelně přiřadit jeho odesilateli pomocí digitálního podpisu. Pak si můžete být jistí, že informace v e-mailu obsažené nepřečte nikdo jiný než adresát, že na každý pokus o jejich změnění či poškození budete okamžitě upozorněni a že digitální podpis spolehlivě identifikuje odesilatele. Taková ochrana je opět nemožná bez asymetrické kruptografie a bez certifikátů klíčů.

4. Ochrana dat na lokálních serverech proti hackerům

Používáte-li Firewall, nikdo nemůže poskytnout positivní důkaz, že Váš Firewall je ten bezpečný a nikdo nemůže poskytnout důkaz, že ten Váš Firewall je správně nastavený. Poskytnuté důkazy v této oblasti jsou vždy důkazy sporem, tj. předpokládáte je že všechno OK, dokud někdo jiný, například hackerským průnikem, nedokáže opak. Jediná spolehlivá ochrana informací na Vačich PC a serverech je jejich šifování. Šifra poskytuje jistotu, že nikdo nebude číst Vaše data a ochrana tajemství se redukuje na ochrany nepříliš velkého šifrovacího klíče.

5. Nezapomínejme však na data, která chcete smazat tak, aby je nikdo jiný nemohl číst

Každý smazaný soubor je možno poměrně snadno obnovit příkazem undelete, či jednoduchým použitím Recycle Bin. V složitějších případech přichází ke slovu nízkoúrovňové programátorské prostředky. Při obnovování opravdu cenných či zajímavých dat je možno použít prostředků elektronických, které obnoví spolehlivě i několikrát přepsaná data na disky či disketě.
V nezáviděnihodné pozici se například ocitne úřad sociálního zabezpečení, či zdravotní pojišťovna, která nakoupí nové počítače, na starých smaže disky a prodá je do bazaru. Jediný šikovný a nezodpovědný programátor tak získá například kompletní přehled o zdravotním stavu, či sociálních dávkách celé jedné oblasti Britanie. Bezpečné skatrování dat je neopominutelnou součástí datové ochrany, i když z Internetem není až tak spojené.

Řešením se jeví být PKI

PKI samo není spasitelné, ale dobře postavené a dobře zvolené aplikace a PKI, použité v režimu prevence by mohly zabránít průniků virů a zabránit navíc i ukradení dat a jejich zneužití.

Pro ochranu informací, které sice chceme sdílet, ale zase ne s každým, a které jsou pro nás důležité v nepoškozené formě, je třeba definovat několik cílů, a ty pak je třeba dosáhnout, a to PKI dovoluje:

- Autentizace poskytovatele a příjemce
- Neodmítnutelnost zodpovědnosti tvůrce informace
- Zaručení, že informace nebyla po cestě mezi poskytovatelem a příjemcem změněna
- Ukrytí informace před nepovolanými zraky (šifra).

Výše vyjmenované požadavky jsou nezbytné pro uchování integrity a soukromí v elektronickém prostoru. Samozřejmě existují prostředky, kterými toho lze dosáhnout. Tyto prostředky však nezbytně potřebují ke své činnosti podporu, kterou jim poskytuje PKI (public key infrastructure), protože jejich jádro leží v kryptografii s veřejnými klíči.

Díky šifrování poskytuje technologie veřejných klíčů **spolehlivost** a **kontrolu přístupu**.

Díky digitálním podpisům dává tato technologie následující možnosti:

- **spolehlivá autentizace**. Spolehlivá autentizace znamená, že uživatelé a servery v síti se mohou bezpečně navzájem identifikovat bez posílání tajných informací (např. hesel) po síti, a to v otevřeném tvaru.
- **integrita dat**. Integrita dat znamená, že osoba, která prověřuje digitální podpis, může snadno určit, zda digitálně podepsaná data byla či nebyla pozměněna od okamžiku jejich podepsání.
- **podpora pro nepopiratelnost**. Podpora pro nepopiratelnost znamená, že uživatel, který data podepsal, nemůže později úspěšně popřít podepsání těchto dat.
- **podpora pro časovou značku**. Podpora pro časovou značku znamená, že uživatel, který data podepsal, stvrzuje pomocí třetí strany i dobu, kdy byl podpis proveden.

Závěr

Zabezpečení informačních systémů proti potenciálním nebezpečím, z nichž viry jsou jen jednou (byť velmi důležitou a nebezpečnou) částí je orientováno spíše na prevenci, administrativní opatření, zaručení autenticity osoby, od které data přicházejí, na kontrolní kryptografické mechanismy, které zaručují nepoškozenost a také neinfikovanost dat a podobně. Antivirové programy izolovaného charakteru ztrácejí smysl a jsou orientovány převážně na síťové a groupwarové technologie.

Bezpečnost dat v současnosti již není otázka jednotlivých izolovaných utilit, ale pouze a jenom sofistikovaných řešení na bázi centrálně řízeného PKI, s centralizovanou správou klíčů.

Úkol bezpečnostních firem je vytvářet rovnováhu nezi výhodami a nebezpečími stále se rozvíjející datové sítě Internet a celého Kyberprostoru. Rovnováha stálého boje o znalosti, technologie a infomace vytvoří současnou křehkou denní realitu.

EVROPSKÁ STANDARDIZAČNÍ ČINNOST V OBLASTI IT

(VEDOUCÍ NAKONEC I K ZÁKONNÉ ÚPRAVĚ ELEKTRONICKÉHO PODPISU V ČR)

Doc. Ing. Jan Staudek, CSc.
Fakulta informatiky, Masarykova universita Brno, staudek@fi.muni.cz

Cílem příspěvku je podat čtenářům přehlednou informaci o normotvorné činnosti související s bezpečností informačních technologií (dále jen IT) se zvláštním zaměřením na iniciativy vedoucí právnímu uznání elektronického podpisu.

Proč se zabývat právním uznáním elektronického podpisu. Důvodem je především skutečnost, že soudobé IT vytvářejí podmínky pro postupnou náhradu papírové komunikace elektronickou, pro elektronickou formu obchodování, pro elektronický styk občana s úřady apod. Nedostatečná legislativa a nezaručená bezpečnost elektronické komunikace ale klade těmto aplikacím mnohé překážky. Právní systém není dosud připraven na nové IT. Především chybí základní právní norma definující podpis elektronického dokumentu, a přitom v českém právním řádu neexistuje jednotná právní úprava, která by jednoznačně připouštěla nebo jednoznačně zakazovala elektronickou formu dokumentace ve všech případech lidského konání. Cílem snah o zakotvení elektronického podpisu v standardním českém právním řádu je učinit dokumenty a podpisy na papíře a elektronické rovnoprávnými.

O konkrétní formě a obsahu českého zákona o elektronickém podpisu se v posledních měsících hodně hovoří i jedná. Nutným předpokladem pochopení proč se řešení problému zákona o elektronickém podpisu mající za cíl, aby se elektronický podpis stal účinným a výkonným nástrojem, nerodí snadno, je porozumění procesům standardizace v oblasti IT. Pro české prostředí musí být standardizační základem pochopitelně evropský standardizační proces. Jako příklady mezinárodních snah o řešení legalizace podpisu elektronických dokumentů lze uvést např. vzorový zákon o elektronickém obchodu komise OSN pro mezinárodní obchodní právo (United Nations Commission on International Trade Law – UNCITRAL nebo i směrnici Evropského parlamentu a Rady z prosince 1999 o zásadách společenství pro elektronické podpisy. V českém návrhu zákona o elektronickém obchodu se říká, že definuje pojmy, postupy a subjekty práva účastnící se na vytváření, používání a ověřování elektronických podpisů, jako prostředků umožňujících používání elektronických dokumentů způsobem, který je v souladu s obecně závaznými právními normami. Návrh zákona se především zabývá tím, jak zajistit jak právně a správně zajistit důvěryhodnost elektronického podpisu. Technická a technologická omezení jsou v návrhu zaváděna spíše nepřímou formou – specifikací požadovaných vlastností podepisovacích nástrojů. Tento přístup umožňuje dlouhodobě udržet krok s rozvojem IT.

V omezeném prostoru pro tento příspěvek považuji za vhodnější poukázat spíše na obecnější trendy tvorby standardů v oblasti IT, než na detailní specifikace konkrétních norem různých forem elektronického podpisu. Znalost těchto trendů a reálií především v kontextu EU tvorbu českých zákonných norem v oblasti informačních a komunikačních technologií kompatibilních s ostatním světem usnadní. Státy Evropské Unie pochopily nezbytnost jednotného přístupu k řešení elektronického podpisu (zejména v návaznosti na elektronický obchod na společném trhu). Základním dokumentem EU v této oblasti je *Direktiva EU k elektronickému podpisu*. Zhruba dva roky byly velice pečlivě diskutovány její principy, zaměření a konkrétní pojmy v ní obsažené. Konečně 30. 11. 1999 byla Direktiva EU k elektronickému podpisu schválena Evropskou komisí. Vlády jednotlivých členských

zemí EU mají za úkol uvést tuto Direktivu do svého zákonodárství do poloviny roku 2001. Sama Direktiva se zabývá elektronickými podpisy používanými pro autentizační účely jak z hlediska obecného přístupu, tak i z hlediska speciálního typu tzv. zaručených elektronických podpisů, které mají být právně ekvivalentní klasickým vlastnoručním podpisům. Jejím cílem tedy není pokrýt všechny oblasti, ve kterých se používá autentizace, ale zaměřuje se na právní platnost elektronického podpisu, který je připojen k elektronickému dokumentu. Direktiva rovněž stanoví požadavky, které mají být splněny poskytovateli služeb, kteří podporují elektronické podpisy a další požadavky vztahující se k podepisující a ověřující straně. Tyto požadavky nutně vyžadují podporu v detailních normách a veřejných specifikacích, které rovněž splní požadavky evropských obchodních organizací.

EU se přirozeně snaží stát se „supervelmocí". Na této cestě se nemůže vyhnout standardizaci svých informačních a komunikačních aktivit a nutně musí prosazovat tyto standardy jako standardy uznávané celosvětově. Koncem 90. let proto jednak zakládá nový *standardizační systém informační společnosti, ISSS* (www.cenorm.be/isss) a jednak zavádí velmi pružný princip přijímání pracovních (de facto) standardů formou výsledných dokumentů standardizačních workshopů. Motivem těchto snah EU je stát se konkurenceschopným partnerem různým iniciativám pružně a účinně vydávajícím „de facto" standardy. Na evropské úrovni působí tři oficiální normalizační organizace.

- *Comité Européen de Normalisation* (CEN) – odpovídá svojí působností celosvětové univerzální normalizační organizaci ISO (*International Organization for Standardization*) – www.cenorm.be
- *Comité Européen de Normalisation Eléctrotechnique* (CENELEC) – odpovídá svojí působností působností celosvětové normalizační organizaci IEC (*International Electrotechnical Commission*) – www.cenelec.be
- *European Telecommunications Standards Institute* (ETSI) – odpovídá svojí působností ITU (*International Telecommunications Union*) – www.etsi.org.

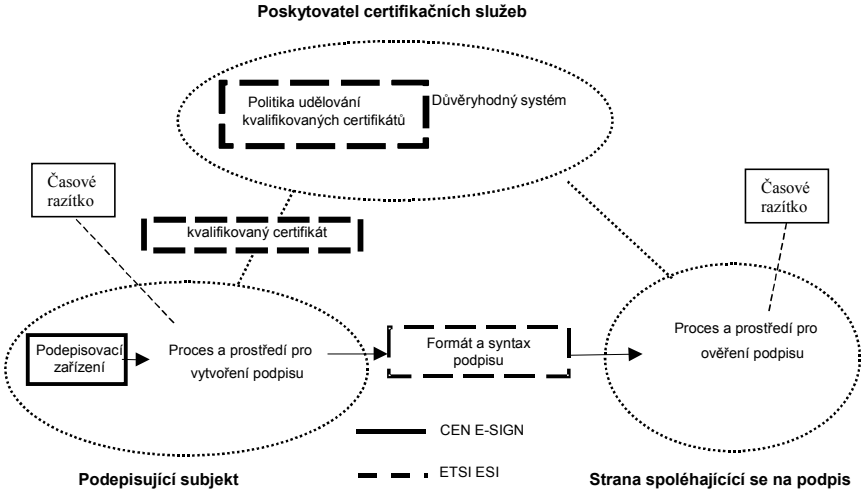
Posláním těchto organizací je podpora dobrovolné technické harmonizace v Evropě plně respektující nutnost spolupráce s odpovídajícími celosvětovými normalizačními institucemi. Cílem je odstranit technické bariéry. Přirozenou snahou budování ISSS je na „de jure" straně vytvořit partnera mnoha konsorciím působícími v oblasti IT a komunikací, které se zabývají vydáváním „de facto" norem. Jejich standardy se vesměs prosazují díky technologické propracovanosti, potřebami a tlakem z výrobních a uživatelských sfér, silně podporovaným těmito sférami i finančně.

Typickým příkladem „de facto" standardů jsou standardy sítě Internet. Tyto standardy jsou známé pod označením *RFC* (Request for Comment). Síť Internet vznikla jako výsledek úzké spolupráce vlády, průmyslu a vysokých škol, propojuje jejich počítačové sítě a privátní počítačové sítě. Projekt Internet vznikal za podpory vlády USA a rozšířil se především díky iniciativám akademických a výzkumných institucí. V posledních letech síť Internet propojuje stále více i sítě mnohých privátních organizací, pro které jsou komunikační služby poskytované touto sítí zajímavé. Chod Internetu je řízen vesměs nepřímo, především prosazováním internetovských „de facto" standardů. Internet je manažersky spravován a provozován radou pro internetovské činnosti, *Internet Activities Board* (IAB), která deleguje hlavní odpovědnost za vývoj a posuzování svých standardů na komisi *Internet Engineering Task Force* (IETF). Konečné rozhodnutí o vydání internetovských standardů pochopitelně dělá IAB. Podobným „de facto" partnerem je i *Institute of Electrical and Electronics Engineers* (IEEE) – profesionální orgán inženýrů v oblasti elektroniky a elektrotechniky, který se výrazně zaměřuje na i normy bezpečnosti, lokálních sítí (IEEE 802.x) a operačních systémů (POSIX); normy IEEE vesměs mají mezinárodní význam a dopad.

Předností konsorcií pečujících o „de facto" standardy je především fakt, že jsou schopny identifikovat potřebu nové normy, její vypracování a zveřejnění i v průběhu jednoho roku. Standardní periodou

vývoje nové normy v rámci ISO je proti tomu pětileté období. To je v oblasti moderních IT neúnosně dlouhá doba. Zkrácení této periody bylo hlavním motivem založení ISSS. Účinným nástrojem pro rychlé dosažení shody názorů v rámci normalizační činnosti ISSS jsou „CEN/ISSS workshopy“. ISSS workshop může uspořádat kdokoliv, kdo sekretariátu ISSS předloží jeho plán a získá od sekretariátu ISSS garanci jeho uspořádání. Výsledkem činnosti workshopu, která se realizuje především komunikací via Internet, je dokument – Workshop Agreement, který má charakter „de facto“ standardu a který je publikován a šířen s podporou sekretariátu ISSS. Finančně ISSS podporuje částečně CEN, částečně je ISSS finančně podporován členskými organizacemi.

Jedním z právě běžících workshopů ISSS (od prosince 1999) je workshop *Electronics Signatures* (http://www.cenorm.be/isss/Workshop/e-sign/Default.htm). Je realizován i v rámci implementační fáze *European Electronic Signature Standardization Initiative* (EESSI) podporované ETSI. Workshop *Electronics Signatures* (E-SIGN) je zřízen v rámci iniciativy CEN. Na řešení problematiky elektronického podpisu se takto podílejí obě evropské standardizační organizace. Dělbu jejich práce a současně základní strukturu podepisovacího schématu pro oblast informačních a telekomunikačních technologií ilustruje následující obrázek.



Mezi cíle workshopu patří stanovení bezpečnostních požadavků na důvěryhodné systémy a produkty, stanovení bezpečnostních požadavků na bezpečné prostředky pro vytváření a ověřování podpisů, vytvoření prostředí pro tvorbu a ověřování podpisů a stanovení hodnotících kritérií produktů a služeb pro elektronické podpisování. Dále se řeší politiky poskytovatelů certifikačních služeb potřebných pro ustanovení důvěryhodnosti elektronických podpisů, formáty elektronických podpisů, profily kvalifikovaných podpisů (splňujících předem daná přísnější kritéria), profily a formáty časového razítkování apod. Pracovní plán workshopu byl definován v lednu 2000. Výsledné dokumenty tohoto workshopu jsou plánovány k publikaci ve druhé polovině r. 2000. Podrobné informace o řešení problematiky elektronického podpisu v rámci iniciativ CEN-ETSI lze naleznout např. na URL www.ict.etsi.org/eessi/eessi-homepage.htm , www.etsi.org/sec/el-sign.htm a na www.cenorm.be/isss/workshop/e-sign .

Existující mezinárodní normy pro oblast elektronických podpisů lze v zásadě roztřídit do více základních okruhů: použití hashovacích funkcí, podpisové algoritmy, činnost v oblasti služeb tzv. třetích důvěryhodných stran – poskytovatelů certifikačních služeb apod. Práce v rámci tohoto workshopu plně respektují stav vývoje normalizační činnosti v oblasti IT, cílem je např. adekvátní vyhovění normě ISO 15408 (Common Criteria for Information Technology Security Evaluation). Mezi plánované výsledky workshopu patří dokumenty typu Workshop Agreement:

- Security requirements for trustworthy systems used in issuing qualified certificates for electronic signatures
- Security requirements for secure signature creation devices
- User interface and operating environment for electronic signature creation
- Procedures for electronic signature verification
- Guidelines for conformity assessment of electronic signature products and services
- Security Management and Certificate Policy for CSPs issuing qualified certificates

Výchozí stav prací mj. vymezují i výsledky normalizační činnosti v rámci ISO související se zaváděním digitálních podpisů, které charakterizují následující odstavce.

ISO normy digitálních podpisů. Mechanismus digitálního podpisování sestává ze dvou komponent, z podepisovacího mechanismu (má soukromý, důvěrný charakter) a z ověřovacího mechanismu (má veřejný charakter). Digitální podpisy implementují bezpečnostní funkce nepopiratelnosti, autentizace původu, integrity dat a tvoří bázi některých autentizačních mechanismů a mechanismů správy klíčů. Rozeznávají se dva typy digitálního podepisování:

- digitální podpis s obnovou zprávy
- digitální podpis v dodatku zprávy.

Digitální podpis s obnovou zprávy zavádí norma ISO/IEC 9796: 1991. Je vhodný jen pro krátké zprávy. Norma ISO/IEC 9796-2: 1997 umožňuje podepisování bez omezení délky zprávy, pro velmi dlouhé zprávy však pouze s jejich částečnou obnovitelností. Další část této normy, ISO/IEC 9796-4 zabývající se mechanismy na bázi diskrétních logaritmů je stále ještě ve vývoji. Specifické mechanismy pro podpis libovolně dlouhých zpráv jsou předmětem vznikající normy ISO/IEC 14888. Podstatnou částí výpočtu digitálních podpisů v dodatku zprávy jsou jednocestné hašovací funkce. Tyto funkce připravované normy digitálních podpisů nepokrývají, jsou předmětem samostatné normy ISO/IEC 10118. Norma ISO/IEC 10118-1:1994 zavádí základní pojmy, norma ISO/IEC 10118-2:1994 obsahuje definice dvou metod pro budování hašovací funkce na bázi blokového šifrovače, norma ISO/IEC 10118-3:1998 specifikuje tři dedikované hašovací funkce (funkci zavedenou NIST pod názvem SHS – Secure Hash Standard a dvě funkce evropského původu vzniklé v rámci iniciativy RIPE – Réseaux IP Européans, RIPEMD-160 a RIPEMD-128). Konečně norma ISO/IEC 10118-4:1998 specifikuje další dvě hašovací funkce pro digitální podepisování založené na aplikaci modulární aritmetiky.

ISO normy integritních mechanismů. Integritní mechanismy jsou určeny pro implementaci ochrany proti neautorizované modifikaci dat, implementují integritní služby a služby autentizace původu a tvoří bázi některých autentizačních mechanismů a mechanismů správy klíčů. Jsou normalizovány ve dvou typech – zabezpečení integrity jednotky dat (MAC, kryptografický součet) a zabezpečení integrity plné posloupnosti dat (k mechanismům prvého typu přidávají pořadové číslování a časové razítkování). Normou integritního mechanismu je norma ISO/IEC 9797: 1994, která specifikuje použití blokového šifrovače v režimu CBC. Vychází z předchozí bankovní normy ISO 8731-1: 1987, dříve americké bankovní normy ANSI X9.9 a X.9.19.

ISO normy mechanismů výměny autentizačních dat. Mechanismy výměny autentizačních dat implementují služby autentizace entity a tvoří bázi některých autentizačních mechanismů a mechanismů správy klíčů. Jsou součástí mnohých autentizačních protokolů. Jedná se o specifikace posloupnosti výměn kryptograficky chráněných zpráv vyměňovaných mezi komunikujícími entitami a pravidla pro zpracování těchto zpráv. Norma ISO/IEC 9798 poskytuje ve svých pěti částech pestrý výběr takových mechanismů na bázi různých kryptografických technik:

- ISO/IEC 9798-1: 1997 (2. vydání) – obsahuje obecný model autentizace entity
- ISO/IEC 9798-2: 1994 – obsahuje specifikaci mechanismů výměny autentizačních dat založené na bázi symetrické kryptografie
- ISO/IEC 9798-3: 1998 (2. vydání) – specifikuje autentizační mechanismy založené na bázi digitálních podpisů
- ISO/IEC 9798-4: 1995 – specifikuje autentizační mechanismy založené na bázi kryptografických kontrolních součtů (integritní mechanismy)
- ISO/IEC 9798-5: 1999 – specifikuje autentizační mechanismy založené na technikách nulové počáteční znalosti (zero knowledge techniques).

ISO normy mechanismů notarizace. Mechanismy notarizace pomocí třetí důvěryhodné strany (notáře) dávají záruku za integritu, původ a cíl přenosu dat. Typicky se jedná o kryptografické transformace dat. Mechanismy notarizace pomocí třetí důvěryhodné strany mohou podporovat nepopiratelnost. Mezi normy mechanismů notarizace lze zařadit normy:

- ISO/IEC 13888 – specifikuje mechanismy pro podporu služeb nepopiratelnosti, z nichž některé zahrnují notarizační techniky
- ISO/IEC 13888-1: 1997 – specifikuje obecný model nepopiratelnosti
- ISO/IEC 13888-2: 1998 – specifikuje mechanismy nepopiratelnosti založené na kryptografických kontrolních součtech (MAC, Message Authentication Code) a použití notarizačních služeb
- ISO/IEC 13888-3: 1997 – specifikuje, jak lze mechanismus digitálního podpisu použít pro služby nepopiratelnosti.

Kromě již zmíněné *Direktivy EU k elektronickému podpisu* je pro řešení problémů souvisejících s praktickými aplikacemi elektronických podpisů v zemích EU velice důležitým dokumentem závěrečná zpráva iniciativy EESSI (červenec 1999, *Final Report of the EESSI Expert Team*). Základním cílem tohoto dokumentu je analýza budoucích potřeb v oblasti standardizace na podporu Evropské Direktivy pro elektronický podpis. Mezi důležité závěry tohoto dokumentu patří:

- převzetí resp. vývoj průmyslových norem by mělo maximálně zmenšit potřebu detailizace zákonů a vyhlášek v dané oblasti
- normy jsou nezbytně nutné a všude, kde je to možné, je třeba preferovat odkazy na existující mezinárodní normy před vývojem nových norem
- požadavky v oblasti norem jsou dvojího druhu: kvalitativní a procedurální normy týkající se informační bezpečnosti a technické normy vzhledem k interoperabilitě produktů
- podepisovací prostředky (produkty), pokud vyhovují požadavkům Direktivy, musí projít příslušným hodnocením (shoda produktu) a certifikací akreditovanou institucí

- je třeba vytvořit společný referenční bod na základě definice výchozí množiny technologických komponent, který bude tvořit technický rámec pro ověřování kvalifikovaných elektronických podpisů využívajících asymetrickou kryptografii a digitální certifikáty
- je nezbytná koordinace jednotlivých aktivit v oblasti norem.

Informace o autorovi

Doc. Ing. Jan Staudek, CSc., docent Fakulty informatiky Masarykovy university v Brně, vedoucí katedry programových systémů a komunikací. Zabývá se bezpečností informačních systémů, budováním bezpečnostních politik IS v organizacích typu spořitelen, vysokých škol a státní správy, analýzou rizik a aplikovanou kryptografií. Pracuje jako nezávislý konzultant v těchto oblastech, přednáší o bezpečnosti informačních systémů v Bankovní akademii Praha. Mimo to se zabývá výukou v oblasti operačních systémů a počítačových sítí.

CERTIFIKACE VEŘEJNÝCH KLÍČŮ A CERTIFIKAČNÍ AUTORITY

Dr. Ing. Petr Hanáček
Ústav informatiky a výpočetní techniky, Vysoké učení technické v Brně
Božetěchova 2, 612 66 Brno
tel. 41141 216
e-mail: hanacek@dcse.fee.vutbr.cz

Abstrakt

S masovým rozvojem využívání kryptografie veřejným klíčem v prostředí internetu a zejména s plánovaným rozvojem používání elektronického podpisu ve všech oblastech lidské činnosti stoupá do popředí otázka nutnosti zajištění důvěry ve veřejné klíče jednotlivých účastníků. Základním stavebním kamenem, který musí zajistit důvěru ve veřejné klíče, je certifikační autorita. Ačkoli při prvním pohledu je certifikační autorita poměrně jednoduchá služba, při jejím skutečném používání vyjde najevo, že jde o poměrně složité svázání procesů technických, administrativních a právních, které musí zajistit bezpečné navázání "důvěry v elektronickém světě" na "důvěru ve světě papírových dokumentů". Příspěvek se proto zabývá jak technickými, tak i netechnickými problémy činnosti certifikačních autorit. Vysvětluje jak jednotlivé technické procesy, tak i jejich navázání na systém potřebných dokumentů (jako je Certifikační politika) a administrativních úkonů.

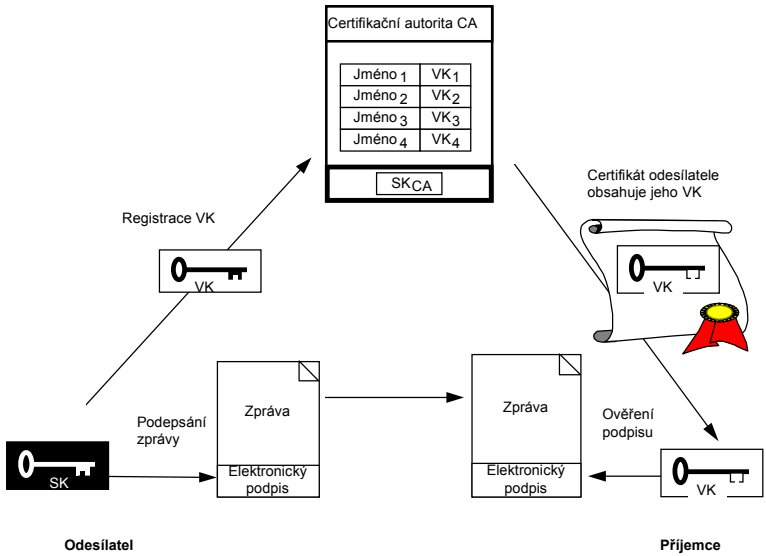
Úvod

Základním problémem, který se projevuje v otevřených prostředích s velkým počtem navzájem neznámých partnerů, je otázka autenticity veřejných klíčů. V okamžiku ověřování elektronického podpisu si musí být ověřovatel jistý, že veřejný klíč, který používá k ověřování daného podpisu, je veřejným klíčem autora zprávy, tzn. potřebuje spolehlivou vazbu mezi klíčem a jménem. Bez dalších opatření by každý uživatel musel nějakým jiným způsobem provést ověření autenticity veřejného klíče každého partnera před tím, než by se na něj mohl spolehnout. Složitost tohoto problému může být zmenšena *certifikací* veřejných klíčů prostřednictvím někoho jiného, komu jak zprávu podepisující tak ten zprávu ověřující důvěřují. Tento prostředník, takzvaná *certifikační autorita* (CA), podepíše veřejný klíč uživatele a jeho jméno (a také další údaje jako například doba platnosti) svým vlastním soukromým klíčem. Tyto údaje, podepsané certifikační autoritou, se nazývají *certifikát*. Tento certifikát může být ověřen veřejným klíčem certifikační autority. Potom jsou partneři schopni navzájem se autentizovat tím, že nejprve ověří elektronický podpis veřejným klíčem partnera a potom ověří autenticitu veřejného klíče partnera ověřením elektronického podpisu certifikátu pomocí veřejného klíče certifikační autority. Jediný klíč, kterému musí oba partneři věřit, je veřejný klíč certifikační autority, čímž se snižuje počet veřejných klíčů, kterým musí každý jednotlivý uživatel důvěřovat.

Ve velkých skupinách uživatelů, které zahrnujících třeba milióny partnerů, však nestačí jediná certifikační autorita. Veřejné klíče certifikačních autorit mohou být opět certifikovány jinými certifikačními autoritami. Je možné představit si stromové struktury certifikačních autorit nebo síťové struktury, ve kterých se certifikační autority náležící do různých stromů navzájem křížově certifikují, což vytváří cesty certifikace nebo řetězce důvěry mezi jednotlivými partnery.

Řetěz certifikací však nemůže být nekonečný a veřejný klíč posledního certifikátu potom zůstává necertifikovaný. To je *kořenový veřejný klíč* a uživateli nezbývá, než mu věřit. Autenticita a

neporušenost tohoto klíče musí být zajištěna nějakým jiným způsobem. Klíč může být zveřejněn, například v čitelné podobě, a daný software může uživateli umožňovat porovnání s klíčem uloženým v počítači. Od okamžiku zadání kořenového veřejného klíče do lokálního počítačového systému musí být jeho celistvost chráněna lokálními prostředky (například využitím čipových karet). Kořenový veřejný klíč, přestože je veřejný, je stejně citlivý na bezpečnost jako soukromý klíč.



Obr. 1 Příklad použití certifikátů a certifikační autority

Certifikační strom

Z algoritmického hlediska není certifikát veřejného klíče nutnou součástí elektronického podpisu. Elektronický podpis může být ověřen i bez certifikátu, pokud je veřejný klíč dostupný z jiného zdroje, například ve veřejném adresáři nebo na čipové kartě. Pro ověření podpisu je třeba důvěryhodný řetězec certifikátů. To v praxi znamená, že první certifikát v řetězci certifikuje veřejný klíč podpisu a každý další certifikát v řetězci certifikuje veřejný klíč certifikátu, jež jej předcházel. Veřejný klíč posledního certifikátu náleží certifikační autoritě, které ověřovatel důvěřuje. Důvěryhodný řetězec mezi tvůrcem podpisu a ověřovatelem se nazývá certifikační cesta. Složitost struktury všech certifikačních cest mezi kterýmikoli dvěma uživateli je srovnatelná s topologií směrování v systémech elektronické pošty.

Zrušení certifikátu

Certifikační autorita musí být schopna zrušit vydaný certifikát před skončením doby jeho platnosti. Pro zrušení certifikátu certifikační autoritou mohou být rozličné důvody:

- Předpokládá se, že tajný klíč uživatele byl prozrazen, čím je neplatné také daný certifikát.

- Změnil se zaměstnavatel uživatele (příslušnost uživatele), čímž je neplatné jméno obsažené v certifikátu.
- Uživatel již nemá být certifikován danou CA.
- Předpokládá se, že certifikát CA byl kompromitován.
- Uživatel porušil bezpečnostní pravidla CA.

Certifikační autorita může jako neplatný označit certifikát, který vydala, jeho přidáním na seznam zrušených certifikátů.

Informace týkající se zrušení certifikátu musí být šířeny prostřednictvím seznamů zrušených certifikátů, takzvaných "černých listin". Tyto seznamy musí být veřejně dostupné, například umístěny ve veřejném adresáři X.500.

Formát certifikátu X.509

Struktura certifikátu je v doporučení CCITT *Authentification Framework* X.509 definována následovně:

```
Certificate ::= SIGNED SEQUENCE {
        version[0]                  Version Default 0,
        serialNumber                CertificateSerialNumber,
        signature                   AlgorithmIdentifier,
        issuer                      Name,
        validity                    Validity,
        subject                     Name,
        subjectPublicKeyInfo        SubjectPublicKeyInfo}
```

Obr. 2 Struktura certifikátu podle X.509

Version a *CertificateSerialNumber* (viz dále) jsou celočíselného typu, *issuer* je vydávající certifikační autorita a *subject* je vlastník certifikátu. *Validity* je dvojice položek typu datum a čas, *notBefore* a *notAfter* (viz dále). *SubjectPublicKeyInfo* obsahuje veřejný klíč subjektu identifikovaného v *subject*, certifikát (*certificate)* samotný je podepsán svým vydavatelem (*issuer*). V X.509 není určeno, ke kterému podpisu se vztahuje část *AlgorithmIdentifier* položky *signature*. Obvykle se vztahuje k podpisu vydavatele (*issuer*) certifikátu, ten se tedy vyskytuje dvakrát: uvnitř a vně podepisovaného certifikátu.

NBÚ A BEZPEČNOST DAT VE STÁTNÍ SPRÁVĚ

Ing. Jan Šmíd
Národní bezpečnostní úřad

Postavení Národního bezpečnostního úřadu (NBÚ), jehož jsem zaměstnancem, je upraveno zákonem 148/1998 Sb. Tento zákon byl přijat v červnu roku 1998 a účinnosti nabyl 1. listopadu téhož roku. NBÚ je ústřední správní orgán a jeho ředitel je přímo podřízen předsedovi vlády. Postupným přibližováním naší republiky k členství ve společenstvích jako je NATO, Evropská unie atd. bylo nutno přizpůsobit i pravidla na ochranu informací. Tato potřeba se netýkala jen informací zpracovávaných v informačních systémech (IS), ale obecně informací ve všech podobách. Zákon 102/1971 Sb. o ochraně státního tajemství ani ve znění pozdějších předpisů nevyhovoval požadavkům na ochranu informací, které je nutno v zájmu České republiky utajovat. Nový zákon, způsobem obvyklým v členských státech NATO i Evropské unie, upravuje způsob ochrany a nakládání s utajovanými skutečnostmi. Zákon kromě jiného definuje novým způsobem stupně utajení informací, oblasti utajovaných skutečností, personální, administrativní, objektovou, technickou a průmyslovou bezpečnost, definuje stupně bezpečnostních prověrek osob, kryptografickou ochranu a zavádí pojem bezpečnost IS a certifikace. Zákon, jehož celý název zní: „ o ochraně utajovaných skutečností a o změně některých zákonů“ stanovuje, že informační systémy používané k nakládání s utajovanými skutečnostmi této republiky (případně skutečností k jejichž ochraně se Česká republika zavázala) by měly být povinně certifikovány.

Žijeme na prahu třetího tisíciletí, pro které bude charakteristický neustálý nárůst objemu výměny informací nejen mezi podnikatelskými subjekty ale i mezi státy využíváním spolehlivých komunikačních a informačních technologií. Naše republika se na přechod do globální informační společnosti připravuje současně se svým začleňováním do mezinárodních politických, hospodářských i vojenských struktur. Mezi důležité počiny v tomto směru je kromě zmiňovaného zákona o ochraně utajovaných skutečností i přijetí Státní informační politiky, která ve svých osmi prioritách nezapomíná ani na důvěryhodnost a bezpečnost IS a ochranu osobních údajů. Zabezpečení informací v IS je bohužel často chápáno jako jakési nutné břemeno zatěžující pořizovací a provozní náklady IS. Přestože popisovaná právní úprava hovoří o IS nakládajících s utajovanými skutečnostmi, neznamená to, že se týká pouze IS státních institucí. Například firmy usilující o speciální státní zakázky, nebo (což je již dnes možné) o řešení projektů zadávaných NATO budou muset kromě kvalifikačních předpokladů doložit, že mají potvrzení o bezpečnostní spolehlivosti a v případě, kdy budou utajované skutečnosti zpracovávat v IS budou předkládat i certifikát IS. NBÚ ze zákona vykonává také státní dozor v oblasti ochrany utajovaných skutečností včetně kontroly certifikovaných IS. Je třeba si uvědomit, že řešení ochrany utajovaných informací a IS určených k jejich zpracování není jen otázka financí a technického zabezpečení, ale také otázka změny myšlení v této oblasti. Podcenění zabezpečení ochrany utajovaných informací by mohlo mít nepříjemné následky zejména v případech, kdy náš stát ručí za ochranu informací třetích stran a selhání v této oblasti by vedlo ke ztrátě prestiže a důvěryhodnosti České republiky v zahraničí. Ta části komerčních organizací, která nebude nakládat s utajovanými skutečnostmi bude zřejmě využívat standardů a metodologií doporučených NBÚ při ochraně svých privátních informací a při tvorbě interních předpisů na jejich ochranu. Zákon č. 148/98 Sb. netvoří ani se svými souvisejícími vyhláškami ucelený návod jak řešit problematiku ochrany utajovaných skutečností a IS v daném konkrétním případě, ale doufáme, že pozitivním způsobem ovlivňuje myšlení lidí odpovědných za bezpečnost informací a dává jim do rukou nástroj, kterým mohou přesvědčit management svých organizací, aby investoval do vytváření důvěryhodného prostředí pro nakládání s utajovanými nebo jinak cennými informacemi.

NBÚ svou vyhláškou z 19. března 1999 ***o zajištění bezpečnosti IS nakládajících s utajovanými skutečnostmi, provádění jejich certifikace a náležitostech certifikátu*** stanovil požadavky na

bezpečnost IS nakládajících s utajovanými skutečnostmi, minimální požadavky v oblasti počítačové bezpečnosti, jakož i postupy a způsoby certifikačního procesu IS a náležitosti certifikátu. Tato právní norma vymezuje pojmy a požadavky v oblasti bezpečnost IS. Základní požadavky, které jsou kladeny na IS nakládající s utajovanými skutečnostmi jsou obecně uznávané potřeby zajištění integrity, dostupnosti a důvěrnosti informací. Z těchto požadavků se odvíjejí další ve vyhlášce rozpracované požadavky jako např. požadavky přístupu k utajované informaci, odpovědnosti za činnost v IS, označení stupně utajení, zpracování bezpečnostní politiky, provozování IS v určeném provozním módu, na bezpečnost v počítačových sítích, na fyzické zabezpečení, na ochranu proti úniku informací prostřednictvím parazitního elektromagnetického vyzařování, na bezpečnost nosičů utajovaných informací, na testování bezpečnosti IS, na personální bezpečnost atd. Vyhláška definuje postup a způsob certifikace IS od podání žádosti o provedení certifikace až po vydání certifikátu včetně certifikační zprávy, která tvoří jeho přílohu. Postup pro provozované IS je popsán v přechodných ustanoveních.

Novelizace zákona č.148/1998 Sb. o ochraně utajovaných skutečností a změně některých zákonů.

V současné době je připravována novelizace zákona č.148/1998 Sb. o ochraně utajovaných skutečností. Návrh znění novely byl vládou předán k projadnání do parlamentu.

Je připraven věcný záměr nového zákona o ochraně utajovaných skutečností jehož zpracování uložila vláda NBÚ v září roku 1999. Tento záměr byl vládě ke schválení předložen koncem loňského roku. Zákon je připravován jako nový a cílem jeho přípravy je vytvořit nový právní předpis, který by plně vyhovoval vnitřním podmínkám a potřebám České republiky a zároveň byl aplikovatelný i v rámci mezinárodní spolupráce.

Hlavním cílem tohoto řešení (proti současnému stavu) je zjednodušení certifikačního procesu, zkvalitnění celého systému ochrany utajovaných skutečností a především jeho přizpůsobení požadavkům NATO a EU např. zavedením nových institutů. Jedná se zejména o:

- Středisko komunikační bezpečnosti
- Středisko pro distribuci kryptografických materiálů
- Středisko TEMPEST – problematika kompromitujícího parazitního vyzařování

Dalším cílem je snížit finanční náročnost při realizaci jednotlivých opatření pro ochranu utajovaných skutečností.

Zjednodušení by se mělo týkat:

1. Personální bezpečnosti

- zjednodušení postupů při prověrkách má za cíl snížit jejich časovou i finanční náročnost
- aby před vznikem pracovně právního vztahu nebo jmenováním nebo volbou do funkce byla příslušná osoba již držitelem platného osvědčení pro požadovaný stupeň utajení
- psychologické vyšetření požadovat vždy pouze pro stupně Tajné a Přísně tajné
- zkrátit počet zkoumaných roků, D – 5let, T,PT – 10let, u PT možno i déle
- bezpečnostní dotazník diferencovat podle stupně bezpečnostní prověrky

2. Objektové bezpečnosti

- realizace objektové bezpečnosti fyzickou ostrahou objektu, použitím technických prostředků, režimovými opatřeními nebo jejich vzájemnou kombinací
- konkrétní bezpečnostní opatření realizovat na základě analýzy rizik, ohrožení utajovaných skutečností
- kategorizace objektů podle výskytu utajovaných skutečností

tyto změny již obsahují vyhlášky NBÚ vydané v prosinci 1999

- vyhláška NBÚ č. 339/1999 platná od 28. prosince 1999 nahrazuje vyhlášku NBÚ č.258/1998 Sb. o objektové bezpečnosti
- vyhláška NBÚ č. 337/1999 Sb. platná od 28. prosince 1999 nahrazuje vyhlášku NBÚ č. 12/1999 Sb. o technické bezpečnosti
- vyhláška NBÚ o administrativní bezpečnosti č. 244/1998 Sb., byla zrušena a nahrazena vyhláškou č. 338/1999 Sb., platnou od 28. prosince 1999

3. Certifikace

- žadatel o certifikaci bude hradit náklady spojené s certifikací
- budou přesněji stanoveny podmínky uznávání certifikátů vydaných cizí mocí

4. Bezpečnostní standardy Úřadu

- Úřad stanoví postupy, technická řešení, bezpečnostní parametry a organizační opatření pro zajištění nejnižší dovolené úrovně ochrany utajovaných skutečností
- tyto standardy bude Úřad zpracovávat sám nebo přebírat. Vydávány budou ve Věstníku Úřadu.

5. Průmyslové bezpečnosti

- rozdělení na organizace kde vznikají utajované skutečnosti (materiální podoba) a které se pouze s nimi seznamují v nemateriální podobě
- podle toho budou zjednodušeny prověrky organizací
- diferenciace podle stupňů utajení

Doporučený postup při certifikaci IS nakládajících s utajovanými skutečnostmi

- při žádosti o certifikaci postupovat přesně podle vyhlášky, tj. podle §24.

V žádosti je potřeba uvést všechny 4 body, tj.

1. stručně popsat rozsah a účel IS, včetně stanovení jeho běžných a minimálních funkcí
2. stanovit stupeň utajení zpracovávaných utajovaných informací v IS
3. vybrat jeden ze tří bezpečnostních provozních módů (vyhrazený, s nejvyšší úrovní, víceúrovňový)
4. uvést dodavatele IS, (popsat použitý HW a SW)

- žádost musí být podepsána statutárním zástupcem organizace
- je nutno vždy zpracovat bezpečnostní dokumentaci ve smyslu vyhlášky NBÚ č.56/1999 Sb. tj.
  - bezpečnostní politiku informačního systému a stručný výčet a zhodnocení rizik, kterým je vystavena utajovaná informace v něm zpracovávaná
  - návrh bezpečnosti informačního systému
  - bezpečnostní provozní směrnice pro tento informační systém (pro každou skupinu uživatelů zvlášť, tj. pro bezpečnostního správce, administrátora a uživatele IS, případně skupiny uživatelů, pokud jsou stanoveny, z důvodu dodržovat pravidlo „Need to know = potřebu znát“)
  - sadu testů bezpečnosti IS, jejich popis a popis výsledku testování
- je důležité, aby požadované dokumenty popsaly celkové zabezpečení informačního systému, a to z hlediska personální, fyzické, administrativní a počítačové bezpečnosti a organizačních opatření. Jednotlivým požadavkům bezpečnostní politiky pak mají odpovídat realizační opatření v návrhu bezpečnosti a v provozních bezpečnostních směrnicích. Jednotlivé části požadované bezpečnostní dokumentace lze posílat jednotlivě, pokud možno ve výše uvedeném pořadí. Při zpracování požadovaných materiálů je nezbytné vycházet z příslušných ustanovení vyhlášky NBÚ č.56/1999 Sb.
- **dobře ohodnotit své potřeby a snažit se najít co nejjednodušší a nejlevnější řešení.** Z praxe vyplývá, že většinou postačí samostatné PC, s výměnným HDD, operačním systémem Windows NT, v zabezpečené místnosti s trezorem.

  V zájmu snadnějšího zajištění ochrany utajovaných skutečností na pevném disku, často doporučujeme používat výměnný disk např. s operačním systémem Windows NT, který bude jediným HDD v počítači.
- V bezpečnostní dokumentaci je nutno mimo jiné uvést:
  1. popis účelu a rozsahu IS (jaké informace jsou zpracovávány, druh, četnost, rozsah, periodicita, seznam oprávněných osob se stupněm určení, topologie IS, konfiguraci PC, operační systém atd.)
  2. přesně specifikovat HW a SW, dodavatele, kdo provádí údržbu, instalaci ….

3. zajištění informační bezpečnosti v organizaci
4. kontrolní činnost - provádění, vyhodnocení a přijetí nápravných opatření
5. zásady přístupu k utajované informaci
6. personální, fyzickou, administrativní a počítačovou bezpečnost
7. popis a zabezpečení používaných prostor pro zpracovávání a uchovávání utajovaných informací
8. povinnosti vyplývající ze zvoleného bezpečnostního provozního módu
9. ochranu proti parazitnímu vyzařování pokud je vyžadována)
10. popsat jak bude vlastní zpracování probíhat, fyzické umístění VT, provozní režim
11. jak je zabezpečen přenos dat a jejich ochrana (výměnná média, komunikační kanály,…)
12. bezpečnostní incident – vznik, řešení, závěry
13. ochranu SW před modifikací, správnost používaných verzí, doložení použití legálního SW
14. povinnosti bezpečnostního správce, administrátora a uživatelů IS
15. bezpečnostní provozní směrnice pro jednotlivé typy uživatelů
16. řešení krizových situací, likvidace IS

Z bezpečnostní dokumentace musí jednoznačně vyplývat osobní odpovědnost za prováděnou činnost a osobní odpovědnost za kontrolu této činnosti.

Pověření k výkonu činnosti musí být vždy písemné s uvedením patřičných náležitostí (datum, jména a funkce osob, podpisy) a musí být bezpečně ukládáno a archivováno.

U provozních deníků je potřeba uvést minimální rozsah vedených skutečností (např. datum, čas, jméno, podpis, činnost, výsledek, …). Zápisy je nutno pravidelně kontrolovat a vyhodnocovat.

Požadavky NBÚ na rozsah a způsob testování bezpečnosti budou upřesněny v průběhu certifikačního řízení. Ověřeno musí být zejména nastavení zabezpečení operačního systému a správný tok utajovaných informací mezi vnitřní pamětí počítače a diskovými pamětmi během zpracování informací pomocí aplikačního SW (např. textového editoru), vypracování příslušné provozní dokumentace pro uživatele a pro bezpečnostního správce, mechanizmus přihlašování do systému a nastavení příslušných kontrolních a bezpečnostních parametrů, zkoumání a vyhodnocování práce uživatele v systému, mechanizmus zálohování, archivace a obnovení požadované funkčnosti systému po havárii, havarijní plán, ověření bezpečnostních mechanismů personální, fyzické, administrativní a počítačové bezpečnosti, atd. Z testů je nutno dodat protokoly, z nichž bude patrné, co bylo testováno, jakým způsobem a s jakým výsledkem. NBÚ provede následně ověření testů na místě.

- stanovit odpovědnou kontaktní osobu pro styk s NBÚ v procesu certifikace informačního systému, je dobré již v žádosti, neboť v případě nejasností je rychlejší komunikace
- podmínky úspěšné certifikace IS:
    1. organizace musí být prověřena na požadovaný stupeň utajení, z hlediska průmyslové bezpečnosti

2. osoby přicházející do styku s IS musí být prověřeny na požadovaný stupeň utajení a být určeny k nakládání s utajovanými informacemi (personální bezpečnost)
3. každý prostor, kde bude provozován IS s utajovanými informacemi musí mít schválení pro provoz na daný stupeň od objektové a technické bezpečnosti NBÚ
4. použitá výpočetní technika musí vyhovovat z hlediska parazitního vyzařování je-li to vyžadováno s ohledem na stupeň utajení zpracovávané informace

- Na internetové stránce NBÚ (http://www.nbu.cz) je uveřejněn **Metodický pokyn k certifikaci informačních systémů a Věstník NBÚ.**

Doporučená literatura se vztahem k bezpečnosti IS

- Zákon č.148/1998 Sb. o ochraně utajovaných skutečností a o změně některých zákonů,

  účinnost od 1.11.1998

  zákon č.164/1999 Sb., *účinnost od 28.7.1999*

- Vyhláška NBÚ č.56/1999 S. o zajištění bezpečnosti informačních systémů nakládajících s utajovanými skutečnostmi, provádění jejich certifikace a náležitostech certifikátu, *účinnost od 30.3.1999*
- Certifikace informačních systémů, Metodický pokyn NBÚ, Věstník NBÚ č.1, 1999
- Internetová stránka NBÚ, informace III. odboru, informace NBÚ
- Common Criteria v. 2.1 / ISO IS 15408
- Kritéria hodnocení bezpečnosti IS, (Information technology security evaluation criteria - ITSEC), Ministerstvo Hospodářství České republiky, Praha 1993
- Kritéria hodnocení zabezpečených počítačových systémů, (Trusted computer systém evaluation criteria – TCSEC), tzv. Orange book, nakladatelství BEN, Praha 1993
- Návrh pro hodnocení bezpečnosti v informačních technoligiích (Information technology security evaluation manual - ITSEM), European Communities, Národní informační středisko České republiky, 1994
- Vyhláška NBÚ č.244/1998 Sb. o podrobnostech stanovení a označení stupně utajení a o postupech při tvorbě, evidenci, přenášení, přepravě, zapůjčování, ukládání, jiné manipulaci a skartaci utajovaných písemností , *účinnost od 1.11.1998*

  Vyhláška NBÚ č.338/1999 Sb., *účinnost od 28.12.1999*

- Vyhláška NBÚ č. 245/1998 Sb. o osobnostní způsobilosti a o vzorech tiskopisů používaných v oblasti personální bezpečnosti, účinnost od 1.11.1998
- Nařízení vlády č. 246/1998 Sb., kterým se stanoví seznamy utajovaných skutečností, *účinnost od 1.11.1998*

  nařízení vlády č. 89/1999 Sb., *účinnost od 18.5.1999*

  nařízení vlády č.152/1999 Sb., *účinnost od června 1999*

- Vyhláška NBÚ č.339/1999 Sb. o objektové bezpečnosti, *účinnost od 28.12.1999 (nahradila zrušenou vyhlášku NBÚ č, 258/1998, účinnost od 10.11.1998)*

- Vyhláška NBÚ č.263/1998 Sb., kterou se stanoví způsob a postup ověřování bezpečnostní spolehlivosti organizace, *účinnost od 17.11.1998*
- Vyhláška NBÚ č.12/1999 Sb. o zajištění technické bezpečnosti utajovaných skutečností a certifikaci technických prostředků, *účinnost od 21.1.1999*

  vyhláška NBÚ č.337/1999 Sb., *účinnost od 28.12.1999*
- Vyhláška NBÚ č.76/1999 Sb. o zajištění kryptografické ochrany utajovaných skutečností, provádění certifikace kryptografických prostředků a náležitostech certifikátu, *účinnost od 27.4.1999*

  vyhláška NBÚ č.109/1999 Sb., *účinnost od 10.6.1999*

ÚSIS A „DIGITÁLNÍ KOMPATIBILITA“ PŘI ZAČLEŇOVÁNÍ DO EU

Dagmar Bosáková
ÚSIS

Anotace: Úřad pro státní informační systém se podílí na realizaci „státní správy on-line“. Strategické dokumenty „Státní informační politika“ a navazující „Koncepce budování informačních systémů státní správy“ stanovily úkoly pro vytvoření integrovaného informačního systému zahrnujícího informační systémy veřejné správy. Tento informační systém bude sloužit jak pro veřejnou správu, tak k poskytování veřejně přístupných služeb. Zajištění informační bezpečnosti, adekvátní té, která je požadována v EU, je předpokladem spolehlivého fungování takového systému. Součástí příspěvku jsou informace o zákonu o ochraně osobních údajů a návrhu zákona o informačních systémech veřejné správy.

Státní správa on-line

Z pohledu cílů, které si při rozvoji informační společnosti vytýčila Evropská unie, spočívá úloha ÚSIS především v participaci na „státní správě on-linë“, tj. na přiblížení celé státní správy občanovi, na zpřístupnění informací ze státní sféry a na umožnění dialogu mezi státní sférou a občany. K tomu přistupuje úkol, pro který sice nenacházíme v dokumentech EU přímou oporu, ale který je z hlediska státní informační politiky prioritní a je předpokladem pro přiblížení státní správy veřejnosti, tj. vytvoření integrovaného informačního systému zahrnujícího informační systémy veřejné správy, resp. informační systémy sloužící pro výkon veřejné správy. Ten by měl vést k celkové racionalizaci činnosti státní správy a rozhodovacích procesů v jejím rámci. Cílem provázání jednotlivých informačních systémů veřejné správy (ISVS) do neveřejné sítě státního informačního systému je dosáhnout stavu, kde stejná data budou do systému zaváděna pouze jednou a následně budou pouze opravována a doplňována. Tento integrovaný informační systém přitom musí poskytovat služby i budovaným informačním systémům samosprávy a definovaným způsobem s nimi komunikovat. Následně se předpokládá zřízení integrované sítě kontaktních míst veřejné správy k vyřízení správních agend. Na tento integrovaný informační systém veřejné správy budou přes příslušná rozhraní navázány veřejně přístupné služby, které umožní prostřednictvím počítačových sítí kontaktovat veřejnou správu, získávat od ní potřebné informace a též jí informace poskytovat.

Státní informační politika a Koncepce budování ISVS

Tyto cíle, které jsou obsaženy v programovém prohlášení vlády, jsou podrobně rozvedeny v dokumentu Státní informační politika, který připravil Úřad pro státní informační systém a který vládá schválila v květnu minulého roku. Tento dokument rovněž definuje v dané oblasti přípravu na integraci České republiky do EU s akcentem na možnost přímé účasti našich odborníků na akcích a aktivitách organizovaných Evropskou komisí (dále „Komise“), pracovních týmů Komise a na přímou spolupráci s generálními direktoráty Komise.

Státní informační politika deklaruje hlavní cíle v oblasti bezpečnosti informačních systémů a ochrany osobních údajů:

- vytvořit ve veřejnosti povědomí o nutnosti chránit informace,

- zvýšit spolehlivost a zajistit bezpečnost a ochranu zpracovávaných dat pro zvýšení důvěry občanů ve státní správu a samosprávu.

Na Státní informační politiku navázala Koncepce budování informačních systémů státní správy, schválená vládou v říjnu loňského roku. Ta definovala problémy, cíle, podmínky a prostředky při realizaci koncepce, vyslovila se k obsahu a zajištění funkčnosti ISVS, vzdělávání pracovníků veřejné správy, poskytování informací veřejnosti (veřejné informační služby) a k partnerství veřejného a soukromého sektoru. Jako jedno z nejdůležitějších opatření se jeví vyřešení problematiky základních registrů, které představují páteř pro výkon státní správy, přičemž za základní registry jsou v současné době považovány registr obyvatel, registr ekonomických subjektů, registr nemovitostí a registr územní identifikace.

`(Viz: www.usiscr.cz/cz/dokumenty/domaci/index.html)`

Informační systémy veřejné správy

Návrh zákona o informačních systémech veřejné správy

Kompetence Úřadu pro státní informační systém jsou pouze rámcově vymezeny zákonem č. 272/1996 Sb., kterým přešla působnost v oblasti státního informačního systému z bývalého Ministerstva hospodářství (které tyto kompetence nemělo zvláštním zákonem vymezeno) na nově zřízený Úřad pro státní informační systém s tím, že se předpokládalo jednoznačné vymezení jeho kompetencí ve zvláštním zákoně. Vládou předložený zákon byl schválen Poslaneckou sněmovnou, Senátem byl však vrácen z důvodu neslučitelnosti kompetencí v oblasti ochrany osobních údajů a státního informačního systému.

V těchto měsících je v PSP projednáván nový návrh zákona, tentokrát s názvem „o informačních systémech veřejné správy“. Pojem "informační systémy veřejné správy" není v právním řádu České republiky definován, je tedy nutné tak učinit tímto navrhovaným zákonem. Současně je nutné respektovat skutečnost, že v rámci informačních systémů veřejné správy je nutné nalézt definovanou míru spolupráce mezi jednotlivými informačními systémy orgánů veřejné správy. Tento přístup reflektuje nejen současný, ale i cílový stav, tj. existenci jednotlivých informačních systémů orgánů veřejné správy, u kterých dochází k vzájemnému poskytování informací při definování právního rámce a organizačních a technických podmínek (včetně ochrany údajů) společných pro všechny tyto informační systémy.

Navrhovaný zákon bude mít přímý dopad do stávajícího právního řádu, a to tím, že mj. stanoví kompetence Úřadu pro státní informační systém, předpokládá zveřejňování informací o datových prvcích obsažených v informačních systémech orgánů veřejné správy, pokud zvláštní zákon nestanoví jinak, a dále stanoví závaznost standardů ISVS a systém atestací pro ověření technické způsobilosti referenčního rozhraní, produktů, služeb a informačních systémů.

Integrace ISVS, komunikace mezi jednotlivými informačními systémy, zejména pak předávání a dělení dat a služeb, jsou podmíněny dodržováním organizačních a technických pravidel, tj. standardů ISVS. Standardy musí vždy plně respektovat ustanovení českých i mezinárodních norem a jsou harmonizovány s předpisy a legislativou Evropské unie. Atestace budou zajištěny nezávislými atestačními středisky, jejichž činnost bude koordinovat a kontrolovat ÚSIS a příp. jeho poradní orgán. Atestace budou mít platnost pouze na veřejnou správu a budou postaveny na dobrovolných obchodněprávních vztazích všech zúčastněních subjektů.

Po zprovoznění veřejně přístupného informačního systému obsahujícího základní informace o dostupnosti a obsahu jednotlivých informačních systémů veřejné správy a průběžného vyhodnocování

analýz údajů tohoto systému, je možné očekávat případné návrhy na změny nebo doplnění zákonů týkajících se zřízení a provozu informačních systémů a využívání dat z těchto systémů. Tyto změny bude Úřad pro státní informační systém iniciovat ve spolupráci se správci dotčených informačních systémů.

Zásada použitá pro tvorbu informačních systémů veřejné správy, že identifikační údaje fyzických a právnických osob již jednou těmito osobami poskytnuté by neměl jiný orgán po těchto osobách opět vyžadovat, ale pouze dát si od nich odsouhlasit platnost těchto údajů, si však pravděpodobně vyžádá novelizaci řady zákonů. Některé z nich budou obsahem předpokládaného návrhu věcného záměru zákonné úpravy základních registrů.

Hlavním principem navrhovaného zákona je stanovení některých práv a povinností osob souvisejících s provozem informačních systémů veřejné správy, stanovení působnosti Úřadu pro státní informační systém, vytvoření podmínek pro zajištění kompatibility informací vedených orgány veřejné správy a stanovení systému atestací. Informační systémy veřejné správy jsou pojímány jako soubor jednotlivých informačních systémů, které slouží pro výkon veřejné správy a jsou vedeny ministerstvy, jinými správními úřady, orgány územní samosprávy v přenesené působnosti a dalšími státními orgány (souhrnné označení "orgány veřejné správy"). Východiskem je skutečnost, že jednotlivé informační systémy obsahují informace, které jsou potřebné pro jiné informační systémy, resp. pro zajištění správních činností příslušných orgánů. Cílem navrhovaného zákona je vytvoření podmínek pro zajištění kvalitních dat a bezpečné výměny informací za předem stanovených podmínek.

Skutečnost, že pravomoc a působnost Úřadu pro státní informační systém není ve stávajícím právním řádu vymezena, komplikuje jeho činnost. Nutnost jednoznačného a nezpochybnitelného vymezení působnosti Úřadu pro státní informační systém zákonem je tedy naléhavá.

Nedostatečná stávající právní úprava je také příčinou toho, že část současných resortních informačních systémů shromažďuje a zpracovává informace bez dostatečné legislativní podpory. Součástí návrhu je vytvoření veřejně přístupného informačního systému obsahujícího základní informace o dostupnosti a obsahu jednotlivých informačních systémů veřejné správy za účelem vytvoření základních podmínek pro jejich optimalizaci a zefektivnění.

Velmi významným společenským rysem využívání informačních služeb bude zvýšení komfortu občana při jednání s úřady (do budoucna možnost vyřízení jeho záležitostí z jednoho místa), omezení zbytečné byrokracie způsobené opakovaným zadáváním osobních údajů jakémukoliv úřadu, který je vyžaduje. Je tedy reálné předpokládat, kromě úspor času a starostí, také úspory výdajů právě u občana, který již nebude muset na své náklady získávat požadované údaje. Současně se zlepší podmínky pro rozhodování úředníků ve věcech předkládaných občany a zamezí se možnosti uvádět úmyslně nestejné údaje na různých úřadech. Povinností uloženou orgánům veřejné správy zveřejňovat informace o datových prvcích obsažených v jimi provozovaných informačních systémech bude umožněn přístup občanů k informacím o struktuře informačních systémů veřejné správy.

(Stav ke 4. 5. 2000, text návrhu je dostupný na www.psp.cz ve verzi pro první čtení.)

Aktivity navazující na návrh zákona o ISVS

Referenční, sdílené a bezpečné rozhraní, které definuje návrh zákona o ISVS, je klíčovým prvkem pro jejich fungování, integračním zprostředkujícím informačním systémem, soustavou společných služeb pro připojené informační systémy, včetně služeb zajišťujících bezpečnost. Samotné rozhraní je datově bezobsažné, resp. obsahuje pouze metadata, služební data a data v okamžiku zprostředkování služby.

ISVS tedy budou napojeny na společné rozhraní, které v první fázi především umožní využívat údaje ze základních registrů a následně i realizaci dalších služeb. Data budou dostupná výhradně oprávněným subjektům v rámci příslušně legislativně zarámovaného procesu.

V oblasti ISVS se předpokládá zavedení atestací referenčního rozhraní, produktů, služeb a informačních systémů. Atestacemi se rozumí stanovení jejich technické způsobilosti, jakosti a bezpečnosti. Pro referenční rozhraní, připojované ISVS a případně pro připojované IS mimo ISVS, je třeba zpracovat soustavu technických norem a standardů a případně jiných předpisů, na jejichž základě budou atestace probíhat. Z hlediska harmonizace s EU je v této oblasti žádoucí mít na zřeteli existující standardy a doporučení EU (např. oblast IDA – Interchange of Data between Administrations).

Na informační bezpečnost ISVS je nutné pohlížet i očima občanů. Jejich důvěra v procesy, kdy údaje o nich samých jsou sdíleny prostřednictvím počítačových sítí, respektování základních lidských práv, musí být podepřeny jak odpovídajícími zákony, tak důslednou aplikací opatření, která jsou obecně vyžadována v oblasti informační bezpečnosti. Bezpečnostní politika referenčního rozhraní by měla pamatovat i na tento aspekt a deklarovat i způsobem přístupným občanům své principy, způsob jejich aplikace a kontrolu jejich dodržování.

Na přijetí zákona o ISVS bezprostředně naváží dokumenty informační bezpečnostní politika a bezpečnostní standard, oba zaměřené na informační systémy státní správy a samosprávy, které nepracují s utajovanými skutečnostmi. Informační bezpečnostní politika je ve Státní informační politice definována jako „komplexní systémové řešení bezpečnosti informačních systémů a informačních a bezpečnostních technologií. Jejím cílem je stanovení oblastí, předpokladů a základních organizačních a normativních opatření pro dosažení všech požadovaných parametrů bezpečnosti informací při zajišťování informačních potřeb veřejné správy. Definuje veškerá možná ohrožení bezpečnosti a integrity dat. Proti těmto ohrožením pak navrhuje opatření, která zajistí dostatečnou ochranu“, přičemž základními atributy chápání bezpečnosti jsou důvěrnost, integrita a dostupnost. Bezpečnostní standard stanoví náležitosti při projektování, tvorbě a provozu informačních systémů veřejné správy z hlediska jejich bezpečnosti. Obsahem standardu bude soubor bezpečnostních opatření a návod pro vytvoření systému řízení bezpečnosti. Standard bude určen především pro řídící pracovníky, projektanty a ostatní pracovníky, kteří jsou odpovědni za prosazování a udržování bezpečnosti informačních systémů a pro všechny subjekty mimo veřejnou správu, které ve prospěch veřejné správy působí, např. dodavatelé informačních a bezpečnostních technologií. Předpokládá se, že standard bude vycházet především z BS 7799, ISO/IEC TR 13335 a ISO/IEC 15408. Řešení musí vycházet z platných legislativních předpisů ČR a platných standardů státního informačního systémy (SIS) ČR.

Zákon o ochraně osobních údajů

Významným počinem Úřadu pro státní informační systém je zpracování zákona o ochraně osobních údajů, jehož přijetí je předpokladem k tomu, aby Česká republika ratifikovala Úmluvu Rady Evropy č. 108 z roku 1981 na ochranu osob se zřetelem na automatizované zpracování osobních údajů a aby se naše legislativa v této oblasti stala kompatibilní s legislativou EU, tj. „vyhověla“ Směrnici Evropského Parlamentu a Rady č. 95/46/EC z roku 1995 o ochraně jednotlivců se zřetelem na zpracování osobních údajů a o volném pohybu takových údajů. Zákon vyšel ve Sbírce zákonů pod číslem 101/2000 a nahrazuje zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Zákon nabude účinnosti prvním červnem t.r., s výjimkou ustanovení věnovaných oznamovací povinnosti těch, kdo hodlají zpracovávat osobní údaje, a registrace povolených zpracování osobních údajů orgánem dohledu. Tato ustanovení nabývají účinnosti prvním prosincem t.r. Ti, kdo již zpracovávají ke dni nabytí účinnosti tohoto zákona osobní údaje, a na něž se vztahuje povinnost oznámení, jsou povinni tak učinit nejpozději do šesti měsíců ode dne nabytí účinnosti tohoto zákona.

Prvním červnem zahájí činnost Úřad pro ochranu osobních údajů, jehož přípravný útvar dosud působil v rámci ÚSIS jako samostatné pracoviště. Prozatím tento úřad najdete v budově ÚSIS, kde jeho pracovníci poskytnou zájemcům veškeré informace. V tomto směru chce být nově vzniklý Úřad velmi aktivní a hodlá poskytnout v různých přístupných formách veřejnosti co nejvíce praktických informací k aplikaci zákona. Ačkoli zákon deklaruje systém kontroly zpracování osobních údajů i sankce za porušování zákona, je záměrem Úřadu vyvinout maximální úsilí, aby se kolizím se zákonem předcházelo.

I když je nezbytné se seznámit s celým textem zákona, vyjímám to, co by nemělo uniknout pozornosti. Zákon se vztahuje na automatizované i neautomatizované zpracování osobních údajů orgány veřejné správy, fyzickými i právnickými osobami. Výjimku z některých ustanovení tvoří úzký okruh zpracování související s bezpečností státu a s bezpečností občanů. Zákon se nevztahuje na zpracování osobních údajů fyzickou osobou pro vlastní potřebu a na nahodilé shromaždování osobních údajů, pokud tyto nejsou dále zpracovávány.

Zákon neukládá žádnou povinnost občanu. Povinnosti jsou stanoveny pro správce, tedy subjekty, které určují účel a prostředky zpracování, provádějí je a odpovídají za ně, přičemž správce může zpracováním pověřit jiný subjekt, tzv. zpracovatele, jehož práva a povinnosti zákon rovněž stanoví. Správce odpovídá za zpracování osobních údajů v souladu se zákonem. Například smí shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění tohoto účelu, uchovávat osobní údaje jen po dobu nezbytnou pro účel zpracování, zpracovávat osobní údaje získané k určitému účelu a následně je zpracovávat k jinému účelu jen tehdy, pokud k tomu dal subjekt údajů souhlas, nesmí shromažďovat osobní údaje pod záminkou jiného účelu či sdružovat osobní údaje, které byly získány k rozdílným účelům. Předpokladem pro to, aby správce mohl údaje vůbec zpracovávat, je souhlas subjektu údajů. Výjimku tvoří zpracování, které se děje na základě zákona a některé další případy, které zákon přesně vymezuje. Zákon upravuje zpracování osobních údajů za účelem nabízení obchodu a služeb.

Zvláštní, přísnější „režim“ je stanoven pro kategorii „citlivých údajů“, tj. údajů vypovídajících o národnostním, rasovém nebo etnickém původu, politických postojích, členství v politických stranách či hnutích nebo odborových či zaměstnaneckých organizacích, náboženství a filozofickém přesvědčení, trestné činnosti, zdravotním stavu a sexuálním životě subjektu údajů. Po dlouhých diskusích nejsou tedy, v souladu se směrnicí EU, mezi citlivé údaje zařazeny údaje o majetkových poměrech.

K dalším povinnostem správce patří informovat subjekt údajů například o tom, že o něm shromažďuje údaje, v jakém rozsahu a pro jaký účel, komu mohou být zpřístupněny či komu jsou určeny. Správce je povinen jednou ročně bezplatně, jinak kdykoliv za přiměřenou úhradu, poskytnout subjektu údajů na základě písemné žádosti informace o osobních údajích o něm zpracovávaných. Dále jsou stanoveny povinnosti správce při zabezpečení osobních údajů a povinnost mlčenlivosti těch, kdo přicházejí do styku s osobními údaji.

Pro správce je důležité ustanovení o oznamovací povinnosti, což znamená, že ten, kdo hodlá zpracovávat osobní údaje, je povinen tuto skutečnost oznámit Úřadu před započetím zpracování. Obsah takového oznámení zákon specifikuje. Tato povinnost se nevztahuje na zpracování údajů, které jsou součástí evidencí veřejně přístupných a zpracování údajů, které je správci uloženo zákonem. Pokud oznámení obsahuje všechny náležitosti a není důvodná obava, že by došlo k porušení tohoto zákona, Úřad oznámení zaregistruje a dnem registrace může oznamovatel zahájit zpracování. Správce Úřadu oznamuje rovněž ukončení zpracování a především to, jak bude s osobními údaji naloženo. K likvidaci osobních údajů je správce povinen přistoupit po ukončení zpracování nebo na základě žádosti subjektu údajů.

Zákon dále upravuje oblast ochrany práv subjektů údajů, předávání osobních údajů do jiných států, postavení, působnost a činnost Úřadu. K jeho základním povinnostem patří vedení veřejně přístupného

registru povolených zpracování osobních údajů a provádění dozoru nad dodržováním povinností stanovených tímto zákonem při zpracování osobních údajů.

Na některá výše uvedená ustanovení jsou vázány výjimky, nebo jsou tato ustanovení detailně upravena, je tedy žádoucí prostudovat celý text zákona.

PROBLEMATIKA BEZPEČNOSTI POD ZORNÝM ÚHLEM ČLENSTVÍ V NATO

plk. gšt. Ing. Karel STREJC

Dámy a pánové,

dříve než přistoupím k vlastní přednášce mně dovolte, abych Vás co nejsrdečněji pozdravil a popřál Vám pevné zdraví, hezký a příjemný den (zbytek dne).

Tématem mého dnešního vystoupení je "Problematika bezpečnosti dat pod zorným úhlem členství v NATO".

Jistě je Vám známo, že přijetím ČR za řádného člena NATO se výrazně zvýšily nároky na ochranu utajovaných skutečností. V tom i nároky na kvalitu komunikační infrastrukturu AČR a požadavky na bezpečnost zpracovávaných a předávaných dat a informací.

Současný stav v komunikační infrastruktuře AČR je možné charakterizovat (při respektování atributů ochrany utajovaných skutečností) asi takto:

- úspěšně probíhá výstavba komunikačního prostředí, jehož nosnou částí je digitální komunikační systém ALCATEL umožňující plné využití služeb ISDN,
- jako nadstavba komunikačního systému jsou urychleně budovány informační systémy druhů vojsk a služeb, ale zejména ŠIS. Všechny systémy jsou prozatím určeny ke zpracování a přenosu neutajovaných informací,
- intenzivně se pracuje na zabezpečení celé komunikační infrastruktury tak, aby mohla být plnohodnotně využívána k přenosu utajovaných skutečností do stupně utajení Důvěrné (Tajné),
- k termínu přijetí ČR do NATO bylo péčí specialistů NATO vybudováno zabezpečené komunikační prostředí umožňující zpracování a přenos utajovaných informací do stupně TAJNÉ. Realizace tohoto úkolu probíhala ve velmi krátkém časovém období a byla hodně náročná jak technicky, tak i z hlediska nutných stavebních úprav a personálního zabezpečení. Zvýšeným úsilím se nám však všechno podařilo splnit v požadovaných parametrech a termínech,
- jako dosti závažný, i když z počátku poněkud opomíjený, se nakonec ukázal problémem, vyplývající ze změny legislativy pro ochranu utajovaných skutečností. S výstavbou komunikačního prostředí ALCATEL se započalo přibližně v roce 1993, tedy v době kdy pro OUS v ČR platil zákon číslo 102/1971 Sb. Tento pro komunikační bezpečnost nedefinoval tak náročné požadavky, jako je tomu v případě zákona č. 148 z roku 1998 Sb., a právních předpisů k němu vydaných. Realizace požadavků zákona číslo 148/98 Sb představuje mnohem vyšší nároky na rozpočet resortu obrany než jsme předpokládaly, což poněkud přibrzďuje naše snahy a záměry. To je také jeden z důvodů, proč neustále hledáme cesty a způsoby, jak vyhovět požadavkům zákona na ochranu utajovaných skutečností a současně se vtěsnat do dostupných finačních prostředků,
- velmi dobře si uvědomujeme význam a možnosti využití výpočetní techniky pro rozvoj informačních technologií, přenos dat nebo vytváření databází, ale stejně dobře si uvědomujeme i různá úskalí a nebezpečí, které tato problematika přináší.

Bezpečnost informací a dat v AČR chápeme jako souhrn dílčích opatření bezpečnosti: administrativní, personální, objektové, technické, kryptografické, průmyslové, informačních systémů (včetně antivirové problematiky), ale i certifikačních řízení. Chápeme, že tyto prostředky ochrany utajovaných skutečností se na celkové bezpečnosti informací a dat podílejí různou měrou, resp. v závislosti na okolnostech výstavby komunikační infrastruktury se mění jejich podíl, nároky a význam. Bezpečnost informací a dat chápeme proto jako progresivní, dynamicky se rozvíjející proces, u kterého musíme být neustále připraveni na řešení nových bezpečnostních situací a požadavků. Také proto mnohé zkušenosti potřebné pro bezpečnost komunikační infrastruktury přebíráme ze standardních norem NATO, kde jsou mnohem větší zkušenosti u problematiky bezpečnosti informačních systémů.

K základním požadavkům našeho členství v NATO patří i bezpečná komunikační infrastruktura (zabezpečený komunikační a informační systém) AČR. Tato musí být odolná nejen vůči atakům nepovolaných osob nebo rozvědných služeb, ale i dalších cílených nebo náhodných ataků jednotlivých osob nebo organizací, včetně teroristických. Z těchto důvodů v AČR považujeme bezpečnost informací a dat za nepřetržitý proces, při kterém jsou do systému implementovány nové a účinnější bezpečnostní prvky nebo technologie.

V bezpečnosti komunikační infrastruktury AČR se snažíme co nejvíce uplatňovat především systémový přístup. V rámci tohoto přístupu, řešíme jak zabezpečení vlastního komunikačního systému (technická zařízení přenosu, objekty, přenosové trakty, krypto-ochranu přenášených informací a dat atd.), tak i informačních sítí. Přitom zabezpečení vlastního komunikačního prostředí považujeme za základní aspekt ochrany utajovaných skutečností komunikační infrastruktury AČR.

Z hlediska požadavků na bezpečnost informačních sítí, které sdílejí budovaný komunikační systém AČR se zabýváme především možnostmi spolehlivého zabezpečení přístupu k technice určené pro zpracování a přenos informací a dat a databázím, dále pak zabezpečením objektů v nichž jsou zařízení provozována, ale také o bezpečnostními prověrkami osob, které informace zpracovávají. Nemalý důraz klademe i na tzv. "organizační opatření", tj. zavedení odpovídajícího režimu utajení na všech pracovištích, ve kterých se s utajovanými skutečnostmi na výpočetní technice pracuje. Z Vám, jistě pochopitelných důvodů, specifické místo i naši pozornost zaujímá především Štábní informační systém, který tvoří něco jako páteř celého informačního systému AČR. To proto, že jej jako podsystémy, sdílejí i jiné informační systémy součástí AČR.

Z hlediska :

- současného stavu rozpracovanosti bezpečnostní politiky v resortu obrany (AČR),
- stavu výstavby resortní komunikační infrastruktury,
- zvýšených požadavků Severoatlantické aliance na bezpečnost informací a dat,

je pro nás v AČR velmi aktuální problematika, kterou se právě dnešní konference zabývá.

Bezpečnost informačních systémů je proto i pro nás základním úkolem, kterým se denně zabýváme z důvodů vnitřní potřeby AČR, tak i potřeb vyplývajících z členství v NATO. A jak jsem již řekl v úvodu, bezpečnost informačních systémů řešíme jako komplex dílčích aspektů jednotlivých prostředků ochrany utajovaných skutečností, které se v průběhu doby různou měrou podílejí na celkové bezpečnosti informačního systému AČR.

Bezpečnost informačních systémů řešíme souběžně ve dvou rovinách: národní a koaliční v rámci NATO. Určité složitosti a problémy při jejich řešení vyplývají z rozdílných požadavků zákona 148/98 Sb. a právních předpisů k nim vydaných a aplikace standardních norem NATO. Dovolte, abych se nyní o některých problémech zmínil.

V prvé řadě je to **problém kvalifikace osob**, které se problematikou bezpečnosti informací v AČR profesionálně zabývají. V bezpečnosti informací, a tato konference to plně potvrzuje, nestačí být "jen specialistou" (vševědem), který zná kde co, ale je třeba být vysoce kvalifikovaným specialistou s hlubokými znalostmi v oboru celé řady doplňkových vědních oborů a disciplin. Ideálním řešením je samozřejmě tým erudovaných pracovníků, kteří teoretické výsledky své práce dovedou až do praktických řešení, použitelných v podmínkách života vojsk. Takový tým prozatím nemáme a také proto přejímáme řadu zkušeností, bezpečnostních technologií a postupů od odborných organizací NATO. Souběžně se snažíme o vyškolení potřebných specialistů ve školících zařízeních NATO. Bohužel se však stává, že tito vyškolení lidé nám odcházejí za lepšími platovými podmínkami mimo AČR.

V druhé řadě je to **problém dostupnosti technických prostředků** určených k zabezpečení zpracovávaných a přenášených informací a dat. Každá armáda na světě, AČR nevyjímaje, musí k tomu, aby své informace spolehlivě chránila, používat jen taková technická zařízení, která jsou pro ni jedinečná. Jinými slovy, nemůže si dovolit žádnou komerční techniku, běžně dostupnou na trhu pro kteréhokoli zákazníka. Vzhledem k možnostem ČR na vývoj, výrobu a zavedení takovéto techniky do výzbroje AČR, jsme opět nuceni hledat podporu a pomoc v rámci struktur NATO.

Další **problémy jsou spojeny s implementací techniky do komunikační infrastruktury** AČR. Těchto problémů je více, proto vzpomenu jen některé. Implementace technických prostředků a bezpečnostních technologií, nutně vyžaduje, aby se dodavatelské firmy seznamovaly s některými utajovanými skutečnostmi resortu obrany. Pokud se jedná o firmy, jejichž státy mají z ČR (resortem obrany) uzavřeny odpovídající bezpečnostní dohody, pak je to snadno řešitelný problém. Složitější je to v případech, kdy potřebné bezpečnostní dohody doposud uzavřeny nejsou.

Uvedené problémy se poněkud zvýrazňují (nabývají na složitosti) pokud se jedná o kryptografickou techniku určenou k ochraně informací a dat v komunikační infrastruktuře AČR. V problematice kryptografické bezpečnosti jsme povinni respektovat požadavky vyhlášky NBÚ číslo 76/1999 Sb.. Tato vyhláška stanovuje způsoby použití, nasazování a evidence kryptografických prostředků používaných k ochraně utajovaných skutečností, používání klíčových materiálů, zjišťování odborné způsobilosti pracovníků kryptografické ochrany utajovaných skutečností, postup a způsob certifikačního procesu kryptografických prostředků a náležitosti certifikátu.

Současný stav na tomto úseku je takový, že **kryptografické prostředky tuzemské výroby**, které by splňovaly požadavky této vyhlášky (mají certifikát NBÚ) a současně bezpečnostní, technické a technologické nároky budované komunikační infrastruktury AČR, prozatím nemáme. Necertifikované kryptografické prostředky mohou být podle § 12, této vyhlášky používány jen do 31.12.2001. Vzhledem na současné možnosti našeho výzkumu, vývoje a průmyslu není předpoklad, aby v brzké době došlo v této záležitosti k nějakému zásadnímu obratu

Řešením uvedeného problému může být např. **nákup potřebné kryptografické techniky u renomovaných zahraničních firem.** Náš zájem je zaměřen především na nákup kryptografických prostředků certifikovaných pro použití v NATO. I s tím je však spojen určitý problém. Jeho meritem jsou opět požadavky na bezpečnost informací a dat. Pro použití kryptografické techniky je příznačné, že garantem kryptografické ochrany informací je použitý šifrový algoritmus a systém jeho klíčování. V souvislosti s tímto vyvstává v případě zahraničních dodavatelů řada otázek, jako např.: máme od výrobce převzít kompletní kryptografické prostředí, tzn. techniku s jejím šifrovým algoritmem a klíčovým hospodářstvím včetně systému generování a distribuce klíčů?, to vše bez ohledu na národní zájmy? Pokud ano, tak za jakých podmínek? Máme akceptovat riziko, že naše utajované skutečnosti mohou být výrobcem "čteny"? Jiná otázka - Pro jaký stupeň utajovaných skutečností lze tento postup, tedy nákup kryptografické techniky ze zahraničí, použít? Bezpečnostní riziko vyplývající z tohoto přístupu k zabezpečení komunikační infrastruktury AČR je dost velké. Avšak vzhledem k situaci v jaké

se nyní v procesu výstavby komunikační infrastruktury AČR nacházíme musíme urychleně přijmout odpovídající rozhodnutí.

Druhý přístup, který se pro řešení tohoto problému nabízí, vychází z myšlenky předat výrobci kryptografické techniky vlastní šifrový algoritmus a odpovídající systém jeho klíčování k implementaci do nakupované kryptografické techniky. Tento přístup je možný, ale položme si otázku co to v praxi znamená? V prvé řadě je pro tyto účely potřebné mít připraveno několik takových základních šifrovacích algoritmů s odpovídajícím systém jejich klíčování. To nemáme. Použitelné jsou i klony těchto základních šifrovacích algoritmů, ale ty také nemáme. Nehledě k tomu, že ani klonování šifrovacích algoritmů, které je jinak ve světě běžné, nelze často používat, protože se tím snižuje bezpečnost a odolnost proti prolomení šifry.

Hlavním důvodem, pro který je nutné tento přístup velice pečlivě zvažovat je ten, že vybranému výrobci v každém případě musíme náš šifrový algoritmus zpřístupnit v takové míře, aby mohl provést jeho implementaci do příslušných výrobních technologií. Mimo jiné mu musí být předán i matematický model našeho šifrového algoritmu, systém klíčování a další nezbytné informace nutné k implementaci našeho kryptografického prostředí. A tady se přímo vnucuje otázka - můžeme v tomto případě a za těchto podmínek mluvit ještě o bezpečné a spolehlivé kryptografické ochraně informací na bázi národního šifrovacího algoritmu. Jsou tady však i další otázky, které vyplývají z možných bezpečnostních rizik a které nám nedovolují jednoznačně v dané záležitosti rozhodnout.

Z uvedeného je zřejmé, že kryptografická ochrana komunikační infrastruktury AČR není snadnou záležitostí. Vyžaduje promyšlený, systémový přístup, vysoce kvalifikovaný personál, dobré materiální zabezpečení a to vše dohromady hodně finačních prostředků.

Děkuji Vám za pozornost, děkuji pořadatelům konference za pozvání, kterého se mně dostalo a přeji Vám všem hodně úspěchů a zdaru v další prospěšné práci.

CO JE NOVÉHO V KRYPTOGRAFII V ROCE 2000?

Ing. Jaroslav Pinkava, CSc.
AEC, spol. s r.o., e-mail: jaroslav.pinkava@aec.cz

Úvod

Cílem předloženého materiálu je dát určitý přehled o současném dění v kryptografii. Každá takováto práce se musí nutně jednotlivými okruhy problémů zabývat pouze stručně a poukázat jen na některé základní aspekty problematik. V závěru je proto dán poměrně široký seznam zdrojů (literatura a Internet), kde zainteresovaný čtenář nalezne další podrobnosti. Pokud se týče informací pro vstupní přehled do problematiky odkazuji na práci [17], kde lze nalézt definice příslušných pojmů i popisy základních kryptografických algoritmů. Pro každého, kdo se zajímá o aktuální informace z kryptologie, doporučuji Cryptogram Bruce Schneiera [22] a Crypto-World (v českém jazyce) Pavla Vondrušky [24]. Zájemcům o hlubší studium kryptologické problematiky doporučuji knihu [13], kterou lze celou nalézt on-line na Internetu.

Další odstavce obsahují některé nové poznatky, skutečnosti, které se objevily v průběhu posledního roku. Týká se to samozřemě jak symetrické tak i asymetrické kryptografie. Středem pozornosti v posledním období je speciálně i problematika elektronických podpisů.

3-DES

Algoritmus DES již ukončil svou životnost i jako americká vládní norma. Do doby než bude schválen chystaný Avanced Encryption Standard (AES) byl vydán NIST dokument

FIPS-PUB-46-3 [4], který ustavuje jako současně platnou normu algoritmus 3-DES. Fakticky tak dochází pouze ke schválení již existujícího status-quo. Algoritmus 3-DES byl převzán z již déle platné finanční normy ANSI X9.52.Souběžně s touto normou (rovněž v říjnu 1999) byl vydán materiál NIST [11] popisující velice důkladně validaci jednotlivých operačních módů algoritmu.

Postup při zašifrování 64-bitového bloku otevřeného textu I na 64-bitový blok O šifrového textu je dán následovně:

$$O = E_{K3}(D_{K2}(E_{K1}(I))).$$

Dešifrace je pak logicky popsána vzorcem:

$$O = D_{K1}(E_{K2}(D_{K3}(I)))$$

Norma specifikuje tři varianty pro použití klíče $(K1, K2, K3)$:

1. $K1, K2$ a $K3$ jsou nezávislé klíče;
2. $K1$ a $K2$ jsou nezávislé klíče a $K3 = K1$;
3. $K1 = K2 = K3$.

Celková délka použitého klíče je tedy v jednotlivých variantách 168, 112 a 56 bitů.

AES

V roce 1996 inicioval NIST program AES – formou veřejné výzvy na vytvoření kryptografického algoritmu na principu blokové šifry. Oproti stávajícím algoritmům má tanto nový typ algoritmu zpracovávat bloky otevřeného textu v délce 128 bitů a musí umožňovat práci s klíči v délkách 128, 192 a 256 bitů. V roce 1998 bylo akceptováno celkem 15 kandidátů, přitom v roce 1999 z nich bylo vybráno 5 finalistů.

Třetí AES konference (AES3) se konala 13-14. dubna 2000 v New Yorku. Zúčastnilo se jí vice než 250 lidí z cca. 25 zemí. Obsahem konference bylo provedení druhého cyklu technické analýzy finalistů (5 algoritmů: MARS, RC6™, Rijndael,Serpent, Twofish). Je k dispozici elektronická verze konfernečních materiálů [1].

Vítěz zatím nebyl oznámen, čeká se, že příslušná informace bude zveřejněna v průběhu letošního léta.

Z komentářů Bruce Schneiera ([22], April 2000): Z kryptoanalytických útoků se zdá být nejvíce postižen algoritmus RC6 (bylo ukázáno, jak rozbít tento algoritmus při jeho redukci na 15 cyklů z celkových 20 cyklů). Z těchto útoků naopak nejlépe vyšly algoritmy Serpent a Twofish. Samozřejmě žádný z útoků není aplikovatelný na plné verze algoritmů.

Co se týká rychlosti, pak na tom jsou nejlépe Rijndael a Twofish, naopak Serpent je nejpomalejší na většině softwarových technologických platforem. V hardwaru jsou na tom nejlépe Rijndael a Serpent, Mars je velice pomalý.

Schneier doporučuje z dalšího zvažování eliminovat algoritmy Mars a RC6 (oba jsou dle jeho názoru poměrně nevhodné pro hardware a nelze je vhodně umístit na malé čipové karty).

Pozn.: Samozřejmě je třeba vzít na zřetel, že B. Schneier je autorem jednoho z návrhů (algoritmus Twofish).

P1363

Výsledky pracovní skupiny IEEE P1363 (lit.[15]) jsou v oblasti asymetrické kryptografie současným nejvýznamějším počinem. Od svého vzniku byla tato práce orientována na vytvoření základní normy pro tři rodiny kryptografických systémů s veřejným klíčem:

Jsou to algoritmy, jejichž bezpečnost je založena na složitosti úlohy faktorizace velkých čísel (známý RSA algoritmus, Rabin-Williamsův algoritmus). Dále jsou to algoritmy spočívající z hlediska bezpečnosti na složitosti úlohy diskrétního logaritmu a konečně algoritmy eliptické kryptografie, jejichž bezpečnost je obdobně opřena o složitost řešení úlohy eliptického diskrétního logaritmu. Jsou zde pokryty všechny tři základní oblasti asymetrické kryptografie: algoritmy pro výměnu klíčů, digitální podpis a šifrování.

V letošním roce byl schválen poslední (třináctý) draft zpracovaných materiálů jako norma IEEE a tato norma bude v brzké době oficiálně vydána.

Práce skupiny však tímto nekončí. Již se rozběhly práce na dokumentu: IEEE P1363a: Standard Specifications for Public-Key Cryptography: Additional Techniques, jehož obsahem bude řada doplňkových technik (v současné době je k dispozici již třetí verze). Po ukončení těchto prací by se stávající doplněk měl stát součástí hlavního materiálu.

P1363 a nové algoritmy

V současné době se rozjíždí práce na dalším významném projektu. Byla vytvořena tzv. „The Study Group for Future Public-Key Cryptography Standards" (lit. [16]), jejímž cílem je jak adekvátní popis nových aplikací asymetrické kryptografie, tak i adaptace dalších nových rodin kryptografických algoritmů. Jedná se např. o popis autentizace na bázi hesla a sím souvisejícími protokoly pro výměnu klíčů, identifikační schemata, prahové schema digitálního podpisu a jiné. Níže jsou stručně zmíněny dva z těchto nových přístupů (kryptosystémy NTRU a ACE). V letošním roce má k nim přibýt také některý ze systémů rozvíjených německými kryptology. Odpovídající citace lze nalézt v článku [25]. Tyto kryptosystémy jsou konstruovány nad imaginárními kvadratickými tělesy a mají mít určité výhodné vlastnosti a to jak z hlediska rychlosti, tak i z hlediska délky klíče. Např. systém ze zmíněného článku poskytuje stejnou bezpečnost při délce klíče 341 bitů jakou má RSA při délce klíče 1024 bitů. Přitom má umožňovat výrazně rychlejší implementace.

NTRU

Jako jeden z příspěvků pro další práce skupiny P1363 byl přijat materiál [10]. Na webovské stránce firmy NTRU Cryptosystems,Inc.[14] je tento systém inzerován dokonce jako současný nejrychlejší kryptosystém s veřejným klíčem, který je až 100 krát rychlejší než jeho konkurenti. NTRU pracuje pouze s malými čísly a proto umožňuje relativně rychlé implementace. Např. pro RSA při délce klíče N je složitost práce odpovídajícího kryptografického algoritmu popsána výrazem $O(N^3)$, zatímco pro NTRU výrazem $O(N^2)$, resp dokonce $O(N \log N)$ – dle způsobu implementace. Ovšem z hlediska kryptografické odolnosti je délka klíče kryptosystému NTRU srovnatelná se systémem RSA (resp. se systémy na bázi diskrétního logaritmu), tj. v současnosti délka klíče v mezích 1000-2000 bitů poskytuje dostatečnou bezpečnost (eliptické křivky požadují pro odpovídající bezpečnost délku klíče cca 180-200 bitů).

ACE

Velice zajímavým příspěvkem pro P1363 je článek [22], iniciovaný původními články R. Cramera a V.Shoupa [2,3]. Je zde popsán tzv. Advanced Cryptographic Engine (ACE), který specifikuje jak šifrování tak i digitální podpis pomocí algoritmu s veřejným klíčem. Schéma je přitom popsáno natolik detailně, aby byla zabezpečena interoperabilita mezi jeho jednotlivými implementacemi. Schéma má navíc jednu zásadní výhodu – tzv. prokazatelnou bezpečnost (za určitých přesně definovaných požadavků , týká se to zejména tzv. adaptivních útoků [9]).

DSS

V posledních dvou letech prošla norma Digital Signature Standard (DSS) [5].dvojí reedicí. Koncem roku 1998 (FIPS 186-1) zde byl doplněn algoritmus RSA (dle formulace z normy ANSI X9.31) a v lednu tohoto roku (FIPS 186-2) byla norma doplněna celou sadou eliptických křivek. Eliptické křivky jsou definovány pro oba typy těles (binární a prvočíslená tělesa) a byly generovány tzv. prokazatelně náhodně. Obdobnou cestou jdou i materiály SECG (aktivita firmy Certicom – lit.[26]).

Samotný původní algoritmus DSA (na bázi diskrétního logaritmu) však nedoznal změn z hlediska doporučované délky klíče. S tím polemizuje např. článek [12], ve kterém je řečeno,

že použité délky parametrů (p má délku 1024 bitů, q délku 160 bitů) budou bezpečné nejdéle do roku 2002 z hlediska velikosti použitého pole (resp. do roku 2013 z hlediska použité hashovací funkce a do roku 2026 z hlediska velikosti podgrupy).

Kryptoanalýza – výzvy Certicomu a RSA

Kryptoanalytické metody jsou samozřejmě výzvou schopnostem výpočetní techniky již sami o sobě. Protože je však i v zájmu producentů kryptografických technologií mít možnosti výpočetní techniky zmapovány velice důkladně, existují takovéto výzvy dokonce v oficiální podobě. Na webovských stránkách firem RSA a Certicom lze nalézt celou serií úloh v rámci taovýchto výzev (challenge), přitom jednotlivé úlohy (a i ceny) jsou odstupňovány dle jejich rostoucí složitosti. Kryptografickou veřejností jsou sledovány dosažené výsledky také proto, že umožňují lépe zmapovat současné možnosti výpočetní techniky a učinit tak i možné závěry o budoucím vývoji v tomto směru. V srpnu roku 1999 tak bylo poprvé rozbito RSA s klíčem v délce 512 bitů. Pro kryptosystémy na bázi eliptických křivek byly v poslední době dosaženy dva takovéto výsledky: v září 1999 byl rozbit ECC2-97 (binární těleso, obecná křivka) a v březnu 2000 ECC2K-108 (binární těleso, Koblitzova křivka). Čísla 97 a 108 značí přitom odpovídající počet bitů klíče eliptického kryptosystému. Podrobnosti a další odkazy viz [24].

Elektronický podpis – Směrnice EU

Celá řada velice zajímavých dokumentů se objevila v souvislosti s úsilím Evropské Unie o zavedení technologií elektronických podpisů. Je to především Směrnice EU pro elektronický podpis [6], která po několikaleté veřejné diskusi byla schválena v prosinci 1999. Tato směrnice vytváří základ nu pro elektronický podpis především z hlediska legislativního. Jednotlivé členské země EU mají do poloviny roku 2001 upravit své zákony pro tuto oblast tak, aby splňovaly podmínky stanovené touto směrnicí.

Základním výchozím dokumentem z hlediska přípravy evropských norem pro elektronické podpisy je materiál EESSI [7]. V květnu tohoto roku byl schválen rovněž velice důležitý dokument „Electronic Signature Formats“ (lit. [8]). Obsahuje řadu velice užitečných podnětů zejména z hlediska aplikace tzv. časových značek pro elektronické podpisy. Na základě těchto doporučení bude např. možné archivovat elektronický podpis i několik desetiletí, aniž by tento podpis ztratil svoji právní platnost. Některé úvodní poznámky k problematice norem pro oblast elektronických podpisů lze nalézt v [20].

Zákon o elektronickém podpisu v ČR

V květnu tohoto roku proběhl druhým čtením parlamentu ČR návrh zákona o elektronickém podpisu. Formulace zákona vychází již ze Směrnice EU pro elektronický podpis, jinou otázkou je však, zda se zákonodárcům podaří zformulovat i příslušná administrativní východiska tak, abychom se brzy dočkali elektronických podpisů i v praxi (elektronických podpisů v komplexní podobě, tj. včetně odpovídajících legislativních důsledků). Zájemcům doporučuji [18] a také http://www.trustcert.cz.

Délky kryptografických klíčů

Na toto velice zajímavé téma se v poslední době objevily hned dva zásadní články.

Autoři Lenstra a Verheul [12] na základě hluboce sofistikované analýzy dochází přitom k poměrně velice přísným odhadům (viz také výše poznámka k DSA). Autor dále dochází k následujícím doporučením pro rok 2020 (aby bezpečnost elektronické informace byla garantována pro období 20 let). Symetrické klíče by měly mít minimálně délku 86 bitů, modul RSA minimálně 1881 bitů,

analogicky i modul pro diskrétní logaritmus, pro eliptické křivky by měla být minimální délka klíče 161 bitů (pokud nedojde k významnému kryptoanalytickému pokroku).

S těmito odhady polemizuje R. Silverman [23], který je považuje za příliš přísné. Poukazuje zejména na to, že dnes neexistuje takový hardware s jehož pomocí by se dal uskutečnit požadovaný pokrok v kryptoanalýze. Dochází proto k závěru, že např. délka klíče 1024 bitů pro algoritmus RSA zůstává dostatečně bezpečná. Je ovšem třeba také vidět, že pan Silverman je pracovník firmy RSA, které se nepříznivé odhady Arjena Lenstry přímo dotýkají. Viz také článek [21].

Literatura

[1] AES: http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf

[2] Cramer, R.; Shoup, V.: A practical public key cryptosystem provaby secure against adaptive chosen ciphertext attack, In Advances in Cryptology – Crypto 98, pp.13-25

[3] Cramer, R.; Shoup, V.: Signature schemes based on the strong RSA assumption, In 6th ACM Conf. On Computer and Communications Security, 1999

[4] Data Encryption Standard (DES), FIPS-PUB 46-3, October 1999

[5] Digital Signature Standard (DSS), FIPS PUB 186-2, NIST, January 2000

[6] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, http://europa.eu.int/comm/dg15/en/media/sign/ind_ex.htm

[7] EESSI: Final Report of the EESSI Expert Team 20th July 1999, http://www.ict.etsi.org/eessi/Final-Report.doc

[8] ETSI ES 201 733, V1.1.3 (200-05), Electronic Signature Formats, http://www.etsi.org/sec/el-sign.htm

[9] Goldwasser, S.; Micali, S.; Rivest, R.: A digital signature scheme secure against adaptive chosen-message attacks, SIAM J. Comput., 17, pp. 281-308, 1988

[10] Hoffstein, Jeffrey, Pipher, Jill; Silverman, Joseph H.: NTRU. A Ring-Based Publi Key Cryptosystem, IEEE P1363 submission

[11] Keller, Sharon S.: Modes of Operation Validation system for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures, NIST Special Publication 800-20.

[12] Lenstra Arjen K.; Verheul Eric R. : Selecting Cryptographic Key Sisez, November 1999, (http://www.pwcglobal.com/cce.)

[13] Menezes, Alfred J.; van Oorschoot, Paul C.; Vanstone: Handbook of Applied Cryptography, 1997, http://www.cacr.math.uwaterloo.ca/hac/

[14] NTRU: http://www.ntru.com/

[15] P1363: http://grouper.ieee.org/groups/1363

[16] P1363, Study Group: http://grouper.ieee.org/groups/1363/StudyGroup/index.html

[17] Pinkava, J.: Úvod do kryptologie, http://www.aec.cz

[18] Pinkava, J.: Elektronický podpis a Evropská Unie, DSM 2/2000

[19] Pinkava, J.: Digitální a elektronický podpis ve světě a v EU. Legislativní a standardizační aspekty. Seminář AFOI, únor 2000

[20] Pinkava J.: Moderní kryptografické algoritmy pro elektronický podpis, Seminář ČAČK, duben 2000

[21] Pinkava, J.: Jak je to s bezpečností eliptických kryptosystémů, Crypto World

[22] B: Schneier: Cryptogram: http://www.counterpane.com

[22] Thomas Schweinberger; Victor Shoup: ACE: The Advanced Cryptographic Engine, March 1, 2000.

[23] Silverman, Robert D.: A Cost-Based Security Analysis of Symmetric and Asymmetric Key Length, Bulletin RSA, April 2000

[24] Vondruška, P.: Crypto World, http://www.mujweb.cz/veda/gcucmp

[25] Paulus, S.; Takagi, T.: A New Public-Key Cryptosystem over a Quadratic Order with Quadratic Decryption Time, Journal of Cryptology, Vol. 13, Number 2, Spring 2000

[26] SECG: http://www.secg.org/

BANKOVNÍ POČÍTAČOVÉ PODVODY A ÚNIK INFORMACÍ.

Ing. Jiří Nápravník

Většina bankovních podvodů je ve svém principu velmi jednoduchá, i když jsou často v mediích prezentována jako složitý propletenec ještě složitějších operací.Stačí se ohlédnout zpět a podívat se na mimořádné události v posledních dvou letech a zamyslet se nad důvody, které tyto podvody umožnily. Ve všech případech se jednalo především o chyby v řízení banky a v provádění kontroly obezřetného hospodaření se svěřenými prostředky.

Poněkud stranou těchto velkých podvodů v řádu stovek miliónů či miliard, které byly provedeny v oblasti poskytování úvěrů, obchodování s cennými papíry, dokumentárními akreditivy a při použití dalších „klasických" bankovních produktů je zde již téměř deset let oblast kudy je možné z banky odčerpat velké množství peněz. Bez násilí, malým rizikem, že Vás chytnou a s minimálním rizikem, že Vám něco dokážou. Jedná se o nekontrolovaný přístu k informačnímu systému a datům, která jsou v tomto systému uložena.

Když teď s odstupem několika let hodnotím situaci v oblasti bezpečnosti IS a obecně v oblasti bezpečnosti, byla to doba silně poznamenaná nezájmem top manažerů o tuto oblast. Jednou byl argument pro odmítnutí zabývat se touto oblastí názor, že :

- otvíráme se Evropě a světu a není tedy vhodné něco schovávat
- jsou důležitější věci
- je málo peněz na provoz a žádné na rozvoj
- používáme počítač, který užívá Pentagon, americká centrální banka, apod.
- počítač, informační systém, který používáme má certifikát bezpečnosti, např. C2

Tento pohled byl ještě umocněn názorem, že počítače jsou v organizaci jaké si nutné zlo, které je třeba mít k provozu a pokud začala ve firmě reorganizace a snižování pracovníků, týkala se tato opatření i informatiků a často i správců centrálních informačních systémů. To vedlo až k takovým extrémům, že byl v bance, pojišťovně nebo jiné organizaci, která je životně závislá na IS, jeden pracovník, který zakládal novým pracovníkům profily (jméno a heslo), udržoval v provozu centrální systémy a pokud se vedení rozhodlo zabývat se bezpečností, tak také zpracovával zprávy o incidentech a rozličné analýzy rizik. Zdá se vám to v roce 2000 bláhové, že dotyčný informatik je neomezeným vládcem a nadřízení nemají možnost jeho kontroly. Rozhodně se ale nejedná o sci-fi. I dnes se najdou organizace, které spravují citlivé informace či cizí finanční prostředky a přitom bezpečnost jejich informačního systému a tedy i bezpečnost a důvěryhodnost celé organizace je postavena na hliněných nohách.

Další brzdou v řešení bezpečnosti a také spolehlivosti informačních systémů je pohled na peníze, co jsou a co nejsou peníze společnosti. Pro mnoho uživatelů informačního systému (a to jsou právě top manažeři společností) je rozdíl pokud vidí balíček bankovek, za které si mohou okamžitě něco koupit a když vidí na monitoru v kolonce jedničku a šest nul. Samostatnou kapitolou jsou informace a firemní know-how ale to by bylo na samostatnou několikahodinovou přednášku.

Pro ilustraci jeden příklad. Přístup do trezorové místnosti má pouze omezená skupina pracovníků banky, vždy musí být alespoň dva a jejich pohyb je sledován videokamerami. Přístup k centrální databázi účtů a denních transakcí má v porovnání s přístupem do trezorové místnosti velká skupina lidí, někdy i externistů. Tito lidé mohou v informačním systému pracovat sami a jsou jen málo nebo vůbec nejsou kontrolováni a poslat elektronicky z účtu na účet několik miliónů je otázkou několika sekund.

To jej jen jedna z možností, které mohou mít za následek pokus o podvod nebo dokonaný podvod. Jak tyto problémy řešit ?

První a nejdůležitější, ostatně jako i v jiných oborech je prevence. Předcházet bankovním podvodům s použitím výpočetní techniky s pomocí :

- budování dobré podnikové kultury
- kvalitního výběru nových pracovníků a jejich trvalého proškolování
- jasné definování pracovních pozic a oddělení citlivých oprávnění (jak v oblasti IT, tak v oblasti bankovnictví)
- oddělit správu sítě a IS od provozní bezpečnosti
- vybudovat kvalitní kontrolní / auditorské mechanizmy pro rychlé odhalování mimořádných událostí – neoprávněné operace, nadlimitní operace, mazání, atd, atd
- brát na vědomí a řešit postřehy řadových pracovníků, i nováčků
- začít řešit uvnitř organizace i při komunikaci s obchodními partnery jednoznačnou identifikaci osob, např. s použitím PKI a certifikátu uloženého na čipové kartě

K tomu, aby se výše uvedené body mohly úspěšně uvést do praxe je třeba přestat strkat hlavu do písku před mimořádnými událostmi a selháním IS. Informační systémy, které používají banky mají v těch základních rysech mnoho společného, i když je ve skutečnosti dodávali různé firmy. Lidé, kteří systémy spravují a kteří je používají pochází z jednoho kulturně - sociálního prostředí a tedy i jejich sklon k chybovosti a podvodům je velmi podobný. To znamená, že i počty pokusů nebo dokonaných podvodů si budou velmi podobné. Co se ale diametrálně liší je přístup k řešení takovýchto případů. Do nedávna byla v ČR ale i v další evropských zemí taková praxe, že se podvody v bankovních informačních systémech se nezveřejňovaly s odkazem na to, že takováto skutečnost by mohla poškodit dobré jméno banky. Přitom pokud se stane přepadení bankovní pobočky a lupiči si odnesou X miliónů ví o tom z novin a televize v krátké době celý stát a všem je jasné, že takovou věc umožnila špatná ochrana dané pobočky banky.

V loňském roce se alespoň v ČR začala situace měnit. Jedna z českých soukromých bank vydala směrem ke svým zaměstnancům prohlášení, že veškeré podvody a pokusy o podvod s použitím výpočetní techniky budou předány k vyšetření Policii ČR. Podle mých informací to v loňském roce dvakrát učinila.

Podle mého názoru je to jasný posun od přístupu kdy banky prohlašovaly, že mají vše zabezpečené na 100 procent, k přístupu který je srozumitelný a pochopitelný pro každého kdo se nějaký čas pohybuje okolo informačních systémů, tedy : „Jsme si vědomi, že náš systém může mít a má slabiny ale děláme maximum pro jejich odhalení a odstranění.“

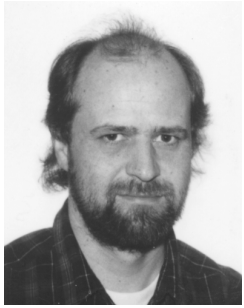
Co ale dělat, když už se nějaká mimořádná událost stane? Především začít s tvorbou pravidel pro vyšetření události a zadržení důkazů až v okamžiku, kdy někdo převedl deset miliónů je už pozdě. Stejně jako nikdo nezlehčuje nebezpečí klasického přepadení bankovní pobočky a třeba se dívat i na oblast informačních systémů a dopředu se dobře připravit. Důležité je rychlé zjištění podvodu a účinné sledování podezřelých operací uvnitř systému, protože naprosté většině podvodů předchází jejich příprava a „průzkum terénu“. Jedná se například o testování co se stane, když se zvýší hodnota povoleného debetu u některého z účtů, monitorování provozu na lokální síti s cílem získat uživatelská hesla pracovníků organizace, zkušební nahlédnutí na stav určitého účtu dále se může jednat o použití určité operace (zaúčtování bez průvodního dokladu, storno, atd.) pod cizím profilem. Tyto informace je možné vždy v systému nalézt ještě dřív než vůbec k nějaké mimořádné události dojde. Záleží vždy

na vedení organizace je takovou událost bude řešit. Zda se taková věc přejde bez povšimnutí, zda bude napomenut nebo propuštěn zjištěný pracovník nebo zda budou tyto aktivity dál sledovány a následně bude konkrétní pachatel přistižen takříkajíc s „rukama v kase“.

Rychlost rozhodnutí a reakce jsou velmi důležité mimo jiné i proto, že důkazy v podobě záznamů v auditních souborech mohou být vymazány, přepsány, upraveny, atd. V mnoha společnostech se s poukazem na to, že auditní žurnály zabírají hodně místa na discích se tyto soubory po několika dnech nebo týdnech přepisují. Rychlost s jakou interní audit zjistí mimořádnou operaci nebo se o takové operaci dozví od pracovníků ostatních odborů je velmi důležitá. Pro ilustraci uvádím jeden příklad. V bance zjistily účetní podezřelé způsoby zaúčtování položek v rozsahu několika miliónů, protože ale pracovnice pod jejímž profilem se operace provedly byla na třítýdenní dovolené mimo republiku, čekala její nadřízená na její návrat a vysvětlení. Po návratu se zjistilo, že v den provedení operace byla dotyčná první den na dovolená v inkriminovanou dobu mimo území republiky a současně se zapřísahala, že své heslo nikdy nikomu neřekla. Začalo interní vyšetřování, které mělo ale nulový výsledek protože po téměř třiceti dnech si již nikdo přesně nevzpomínal na ten konkrétní den, kdo byl příslušný den v zaměstnání, na příslušném pracovišti, atd. atd. Tím chci upozornit na další důležitou věc spojenou s úspěšným objasněním mimořádných událostí, a to na pohyb osob uvnitř organizace, příchod a odchod zaměstnanců.

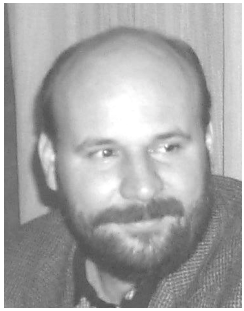
Podvody s použitím výpočetní techniky nebo útoky na důvěryhodnost informačního systému se již objevují několik let. Rozvoj Internetu, vývoj nového diagnostického programového vybavení a masivní rozšíření výpočetní techniky i mezi zdánlivě laickou veřejnost rozšíří i množinu potenciálních pachatelů. Proto by společnosti, které chtějí chránit své zisky, měly již dnes investovat do ochrany svého IS, do pravidel pro předcházení mimořádným událostem a vyšetřování počítačových podvodů. Je pravda, že investovat do ochrany informačních systémů a dat v něm uložených neukládá soukromé společnosti, až na výjimky, žádný zákon. Záleží tedy na majitelích zda budou investovat do bezpečnosti IS nebo budou riskovat, že z jejich práce bude profitovat neloajální zaměstnanec nebo dokonce konkurence.

WHO IS WHO



Ing. Pavel Baudiš

Pavel Baudiš se narodil 15. května 1960. Vystudoval VŠCHT Praha, obor ASR. Několik let pracoval ve Výzkumném ústavu matematických strojů v oblasti počítačové grafiky pro minipočítače ADT. Od roku 1988 se zabývá bezpečnosti osobních počítačů, a zejména antivirovou ochranou. Ve firmě ALWIL Software působí od jejího založení v roce 1991, v současné době se specializuje se na vývoj nových antivirových technologií pro produkty avast! a avast32.



Petr Odehnal

Petr Odehnal, narozen 26.12.1966, vystudoval VUT Brno. Pracuje jako patolog (pitvá počítačové viry) ve firmě Grisoft. Pokud náhodou zrovna nepitvá, tak sedí U Bláhovky a pokouší přijít na to, proč zrovna tam mají nejlepší Plzeň.

Ing. Jiří Mrnuštík

Ing. Jiří Mrnuštík se narodil 17.2.1958 v Brně. V letech 1973 - 1977 vystudoval přírodovědnou větev gymnázia v Boskovicích, pak pokračoval studiem v Praze na ČVUT FJFI (Fakulta jaderná a fyzikálně inženýrská), obor fyzikální elektronika. V roce 1990 založil firmu AEC. Tehdy ještě Jiří Mrnuštík netušil, že z rozjetého vlaku se vystoupit nedá.... Postupně odložil výstroj horolezce, na kterou nějak přestal zbývat čas, na nářadí v posilovně se začíná ukládat prach. Snad jen na skleničku dobré whisky se vždy najde příležitost, ale pohříchu většinou buď s kolegy nebo s přáteli z konkurenčních či spolupracujících firem.

Miloš Kuchař

Miloš Kuchař se narodil v roce 1976 v Boskovicích. Po (a při) působení na fakultě Intomatiky na VUT v Brně a Fakultě podnikatelské taktéž v Brně působí od roku 1996 ve firmě AEC, spol. s r.o. jako konzultant bezpečnosti informačních systémů. Do jeho práce patří posuzování bezpečnosti IS zákazníků a návrhy na jejich zlepšení.

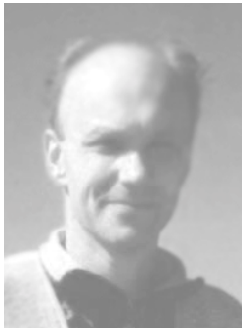
Igor Hák

Jmenuji se Igor Hák, je mi 18 let. Momentálně studuji posledním rokem na SPŠ Textilní ve Dvoře Králové nad Labem. Právě v době konání konference Security 2000 mám za sebou již první část maturitní zkoušky (alespoň doufám). Druhá část je pro změnu přede mnou.

K virové problematice mám blízko a věnuji se jí již delší dobu. Výsledkem je jedna z nejrozsáhlejších stránek o virech / antivirech na českém Internetu - "Igiho stránka o virech" - www.viry.cz.

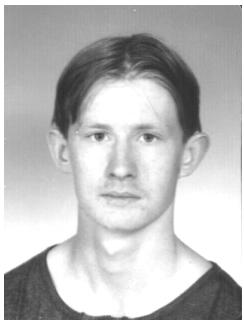
Doc.Ing. Jaroslav Dočkal, CSc.

Absolvent VDU Martin (aprobace matematika - fyzika), Vojenské akademie Brno (obor elektronické počítače), postgraduálního studia v bývalém SSSR (automatizované systémy velení) a USA (finanční management). V současné době vedoucí předmětové skupiny na katedře Automatizovaných systémů velení a informatiky Vojenské akademie Brno. Přednáší předměty Počítačové sítě a Počítačová bezpečnost. Autor řady publikací, mj. učebnice Ochrana dat (VA Brno, 1990). Člen redakční rady časopisu Data Security Management.



Ing. Josef Kaderka

Je absolventem Vojenské akademie v Brně, obor elektronické počítače, a na této škole jako odborný asistent také působí. Zabývá se problematikou operačních systémů, počítačových sítí a bezpečnosti. Má bohaté zkušenosti se správou různých unixových systémů, Novell NetWare a především pak od roku 1992 s provozem Internetu.



Tomáš Bouček

Student 3. ročníku Vojenské Akademie v Brně. Jako koníček má počítačové sítě a bezpečnost.

Petr J. Drahovzal

Petr J. Drahovzal se narodil 12. února 1972 v Brně. Má pracovní zkušenosti i z finančního oboru, neboť před svým „přestupem“ do AEC pracoval ve významné domácí investiční společnosti.
V současné době pracuje v AEC, spol. s r. o. Je členem obchodního týmu, který má v AEC na starosti certifikační autoritu TrustCert. Mezi jeho koníčky patří cestování a sport a brzy se chystá vydat svoji první knihu veršů.

Tomáš Vobruba

Tomáš Vobruba, narozen 3.12.1976, studující na Masarykově Univerzitě v Brně mezifakultní obor Matematika – Výpočetní technika. Od mládí se věnuje informatice ve všech jejich podobách. V dnešní době pracuje jako technik ve soplečnosti AEC. Ovládá UNIX, Windows. Specialista na produkty F-Secure.

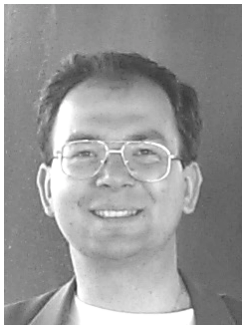
Jiří Donát

Jiří Donát se celoživotně zabývá oblastmi IT a telekomunikací; v poslední době se zaměruje na obchodní aplikace Internetu jako manažer skupiny elektronického podnikání firmy Deloitte&Touche. V této oblasti je autorem řady odborných článku a sci-fi knihy Podraz na informační dálnici (Grada 2000).

RNDr. Alexander Kratochvíl CSc.

Narodil se 16. února 1945 v Táboře. Maturoval na SVVŠ v Praze v roce 1963. Vysokoškolské studium na matematicko-fyzikální fakultě Karlovy univerzity v Praze skončil v roce 1968. Pracoval nejprve v Matematickém ústavu ČSAV, později na Úřadu prezídia ČSAV. V roce 1977 mu byl udělen titul doktora přírodních věd. V roce 1978 titul kandidáta fyzikálně-matematických věd.

V roce 1990 na vyžádání místopředsedy federální vlády a předsedy Státní komise pro vědecko-technický a investiční rozvoj (SKVTRI) ukončil působení v ČSAV a stal se jeho poradcem. Pak nastoupil jako poradce náměstka ministra na Ministerstvu pro hospodářskou politiku a rozvoj ČR. Dne 10. listopadu 1998 nastoupil v Úřadu pro státní informační systém jako vedoucí sekretariátu a 1. ledna 1999 byl jmenován ředitelem sekretariátu Rady vlády pro státní informační politiku. S účinností od 1. února byl pověřen řízením Úřadu pro státní informační systém.



Ing. Tomáš Přibyl

Tomáš Přibyl se narodil 18. března 1975. Po absolvování jeslí, mateřské a následně i základní školy (a to v uvedeném pořadí) byl přijat na brněnské gymnázium na tř. kpt. Jaroše, obor matematika-fyzika. Po jeho úspěšném ukončení pokračoval ve studiu na Fakultě podnikatelské při VUT Brno (kde získal nejprve titul „Bc." a posléze i „Ing."), přičemž již v průběhu studia nastoupil do AEC, spol. s r.o. jako pracovník Public Relations.

Od 21. června 1997 je šťastně ženatý. Svůj volný čas dělí nerovnoměrně mezi manželku, sbírku podpisů astronautů a kosmonautů, psaní článků a knih o kosmonautice a přednášení na toto téma (vystupuje na hvězdárnách a slyšet jej můžete i na některých rozhlasových stanicích).

Doc. Ing. Jan Staudek, CSc.

Doc. Ing. Jan Staudek, CSc., docent Fakulty informatiky Masarykovy university v Brně, vedoucí katedry programových systémů a komunikací. Zabývá se bezpečností informačních systémů, budováním bezpečnostních politik IS v organizacích typu spořitelen, vysokých škol a státní správy, analýzou rizik a aplikovanou kryptografií. Pracuje jako nezávislý konzultant v těchto oblastech, přednáší o bezpečnosti informačních systémů v Bankovní akademii Praha. Mimo to se zabývá výukou v oblasti operačních systémů a počítačových sítí.

Dr. Ing. Petr Hanáček

Petr Hanáček, Dr. Ing., odborný asistent na Ústavu informatiky a výpočetní techniky VUT v Brně. Zabývá se několik let bezpečností informačních systémů, analýzou rizik, aplikovanou kryptografií, elektronickými platebními systémy. Je nezávislý konzultant v této oblasti a přednáší několik kurzů o bezpečnosti informačních systémů v Bankovní akademii Praha.

Mgr. Dagmar Bosáková

Mgr. Dagmar Bosáková, nar. 3. 11. 1951, vystudovala FF UK katedru informatiky, pracovala od roku 1976 v Ústředí vědeckých, technických a ekonomických informací (ÚVTEI), od roku 1991 v Národním informačním středisku ČR. V současné době ředitelka odboru bezpečnosti informačních systémů Úřadu pro státní informační systém.

plk. gšt. Ing. Karel STREJC

Plukovník gšt. Ing. Karel STREJC, narozen 2.4.1951, vystudoval VA Brno, obor vojenská spojovací technika. V současnosti pracuje na Generálním štábu AČR, ve funkci náčelníka odboru bezpečnosti informací.

Ing. Jaroslav Pinkava, CSc.

Jaroslav Pinkava, nar. 2.5.1948, kandidát matematicko-fyzikálních věd. Začínal na katedře statistiky VŠE v Praze, od roku 1978 se věnuje profesionálně kryptologii. V současné době pracuje jako kryptolog brněnské firmy AEC spol. s r.o. Je místopředsedou kryptologické skupiny JČMF (GCUCMP), členem IACR, ICSA, ISACA. Byl členem organizačního výboru mezinárodních konferencí Pragocrypt 96, Eurocrypt´99.

BEZPEČNOST DATOVÝCH SÍTÍ - TECHNOLOGIE VPN

RNDr. Ivan Svoboda, CSc.
T-SOFT s.r.o., e-mail: svoboda@tsoft.cz

Klíčová slova: VPN, bezpečnost datových sítí, autentizační systémy, firewally, šifrovací systémy, IPSec, PKI.

Souhrn

Účelem přednášky je seznámit posluchače se současnými trendy v zajišťování bezpečnosti datových sítí, především s technologiemi pro tvorbu bezpečných VPN - bezpečných virtuálních privátních sítí. Základní komponenty při tvorbě VPN představují platformy IPSec a PKI.

Co je to VPN ?

Přínosy VPN

Pojem VPN - Virtual Private Network, neboli Virtuální Privátní Síť, je v poslední době velice frekventovaný nejen v propagačních materiálech většiny firem z oblasti IT, ale i v odborných diskusích. Během uplynulého roku se začaly bezpečné sítě budovat konečně i v České republice. Ve vyspělých zemích je již tato technologie považována za dospělou a je nasazována ve stále se zrychlujícím tempu.

Bezpečnostní manažeři všech organizací, společně s manažery zodpovědnými za informační technologie, totiž stojí velmi často před složitým úkolem: zajistit širokou a rychlou dostupnost informací pro oprávněné uživatele z nejrůznějších lokalit, při současném zajištění komplexní bezpečnosti celého informačního systému. Zároveň jsou manažeři IT nuceni snižovat náklady na rozvoj či provoz IS, ačkoliv neustále vzrůstají telekomunikační poplatky včetně nákladů na pronájem datových spojů.

Vysoký zájem o VPN vyplývá z několika skutečností:

- prudce se zvyšuje samotné využití či budování datových telekomunikací pro co nejrychlejší přenos informací mezi pobočkami či připojování z mobilních stanic,
- budování a údržba privátních či pronajatých sítí je příliš drahá,
- zvyšuje se potřeba komunikací s obchodními či jinými partnery,
- zvyšuje se využití Internetu i jako média pro obchodní styk.

Problémem Internetu a jiných veřejných, poloveřejných či pronajímaných komunikací je, že nezajišťují žádnou bezpečnost přenášených dat. Řešení tohoto problému je právě úkolem VPN.

Využití VPN, zejména společně s využitím levné veřejné sítě jako je Internet, poskytuje organizacím následující výhody:

- kvalitnější komunikace, zvýšení komunikační kapacity,
- vyšší dostupnost spojení (připojení vzdálených poboček, sítě mobilních uživatelů),
- redukce nákladů na provoz,
- zvýšení bezpečnosti bez ztráty pohodlí a rychlosti.

Typy VPN

Pojem VPN je používán v mnoha různých významech:

- virtuálně oddělené segmenty sítí (nastavením pravidel na směrovačích a dalších komunikačních uzlech);
- šifrovaná komunikace.

Je zjevné, že pouze druhý typ, který zahrnuje ochranu přenášených dat a další bezpečnostní služby (autentizaci apod. viz dále), je skutečně bezpečná. Proto se někdy pro odlišení mluví o „bezpečné VPN“ (S-VPN, neboli Secure VPN).

Technologie bezpečné VPN zahrnuje následující bezpečnostní nástroje:

- bezpečnou autentizaci všech účastníků (např. pomocí digitálních certifikátů X.509, nebo pomocí tzv. sdílených hesel),
- řízení přístupu ke zdrojům (podobně jako firewall),
- šifrování dat (tedy ochranu proti odposlechu a modifikaci přenášených dat).

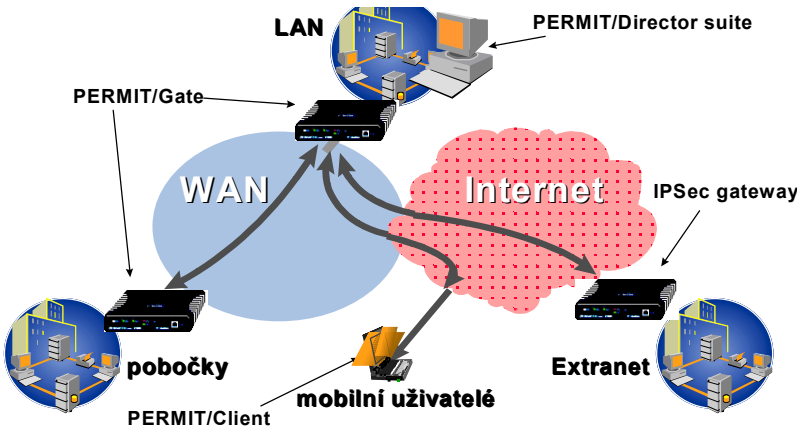
Samotné šifrování v rámci VPN může být provedeno na různých komunikačních vrstvách, pomocí různých standardizovaných technologií:

- na síťové vrstvě IP (platforma IPSec, nejobecnější použití v sítích TCP/IP),
- na transportní vrstvě (platforma SSL/TSL, pro použití především v rámci WWW),
- na jiných vrstvách (PPTP, ATM šifrování atd.).

Aplikace VPN

Technologie VPN je vyžívána pro zajištění bezpečnosti různých typů datových komunikací:

- Intranet (LAN i WAN),
- vzdálený přístup (přes modemy, ISDN, xDSL apod.),
- propojení poboček (WAN nejrůznějších typů),
- Extranet (propojení sítí nezávislých obchodních partnerů).



Obrázek 1 - Schéma aplikace systému VPN

Bezpečnostní hrozby a příslušné bezpečnostní mechanismy

Proč je vlastně důležité zajišťovat bezpečnost počítačových sítí? Co vlastně hrozí?

Několikrát již bylo veřejně prezentováno, že **naprostá většina komunikací (nejen datových, ale i ostatních) je rutinně monitorována (odposlouchávána) a dále analyzována!** K tomu je nutné ještě připomenout, že zmíněný rutinní odposlech se netýká pouze vojenské špionáže, ale i všech státních, komerčních či soukromých komunikací.

Vzhledem k uspořádání datových spojů lze uvažovat především o následujících bezpečnostních hrozbách (platí především pro sítě na platformě IP-protokolu, ale nejen pro ně):

- spoofing - útočník předstírá cizí počítač (použitím jeho IP adresy nebo modifikováním hlavičky paketů); (řešeno bezpečnou autentizací koncových šifrovacích modulů),
- sniffing - útočník odposlouchává (zachytává) cizí pakety; to je snadné zejména v sítích Ethernet; (řešeno šifrováním dat),
- session hijacking - neoprávněné převzetí spojení; útočník simuluje jednoho z účastníků již navázaného spojení s použitím obou předchozích metod; (řešeno bezpečnou autentizací komunikujících stran spojenou s autentizačním záhlavím - ochranou každého jednotlivého paketu),
- man-in-the-middle - komplikovaná metoda využívající navíc i podvrh veřejných šifrovacích klíčů (řešeno mechanismem digitálních certifikátů X.509 s využitím Certifikační autority),
- odposlech či jiné zcizení šifrovacích klíčů (řešeno šifrováním přenášených šifrovacích klíčů, jejich generováním vždy individuálně pro jednotlivá spojení, častým střídáním klíčů, bezpečnou správou),
- modifikace přenášených dat (řešeno ochranou integrity dat pomocí autentizačních algoritmů),

- odposlech interních IP adres (řešeno „tunelováním“, t.j. překladem interních IP adres),
- neoprávněný přístup do interní sítě LAN (řešeno ochranou přístupu založenou na bezpečné autentizaci oprávněných komunikujících stran).

Mezi další požadavky může patřit například zajištění ochrany počítačových sítí proti jejich výpadku a tedy nedostupnosti, zajištění ochrany celé sítě proti neoprávněnému použití, zajištění mechanismů pro důkaz odeslání nebo příjmu určitých dat atd.

Společné doplňkové požadavky na síťové bezpečnostní systémy

Mezi základní požadavky komunikační bezpečnosti patří:

- zajistit diferencovaný systém **řízení přístupu** uživatelů do sítí, k systémům a serverům, což vyžaduje také spolehlivou **autentizaci** všech oprávněných uživatelů,
- zajistit bezpečnost dat během přenosu - jejich **důvěrnost** a **integritu**.

Z praktického realizačního hlediska však nelze zapomenout na řadu dalších požadavků, které by bezpečnostní systém měl splňovat, pokud má být smysluplně nasazen v rozsáhlých informačních systémech velkých organizací:

- **Transparentnost**: systém by měl být „téměř neviditelný“ pro koncové uživatele, neměl by zasahovat do již existujících systémů a aplikací či omezovat jejich funkci, a neměl by být žádnou překážkou ani z hlediska provozní spolehlivosti a přenosové rychlosti.
- **Výkonnost a rozšiřitelnost**: systém by měl být natolik modulární, aby mohl být nasazen zároveň v obrovských centrálách stejně tak jako v malých pobočkách či na izolovaných vzdálených počítačích; centrální správa by měla být natolik pružná, aby umožnila nasazení na tisících uzlů po celé republice (nebo i po celém světě), jakož i spolupráci s bezpečnostními systémy obchodních či jiných partnerů (tvorbu bezpečného Extranetu).
- **Interoperabilita**: systém by měl díky dodržování standardů umožnit navazování bezpečných komunikací i s obchodními či jinými partnery využívajícími jiné standardní prostředky. Mezi uznávané standardy patří zejména sestava protokolů IPSec, a také certifikáty X.509 pro bezpečnou autentizaci obou partnerů; nezbytnou součástí je též možnost cross-certifikace mezi jednotlivými nezávislými certifikačními autoritami.
- **Komplexnost**: systém by v zájmu snadné a bezpečné administrace i snížení nákladů měl pokrývat co nejširší spektrum bezpečnostních potřeb; tedy nejen bezpečné propojení vzdálených poboček a vzdálené přístupy mobilních uživatelů, ale také interní komunikace uvnitř lokálních sítí. V neposlední řadě by měl umožnit perspektivní tvorbu bezpečných Extranetů. Jako velký problém se u řady systémů jeví právě skutečně komplexní pokrytí bezpečnosti uvnitř lokálních podnikových sítí LAN, kde naráží především na dva požadavky:
    - vysoká přenosová rychlost (minimálně 10 Mbps nebo lépe 100 Mbps) i při vysokém počtu paralelních spojení,
    - nezávislost na platformě koncových uzlů; tedy pokrytí nejen PC s platformou Microsoft (což je často dostatečné pro vzdálené přístupy z notebooků), ale také serverů nejrůznějších platforem.
- **Výkonná centrální správa**: vzhledem k tomu, že provozní náklady na instalace, rekonfigurace či vlastní administraci systémů se stávají nezanedbatelnou položkou především pro velké organizace, jsou nyní výkonné, bezpečné a přitom přehledné a snadno použitelné

nástroje pro kompletní vzdálenou administraci celého systému často tím jazýčkem na vahách, který rozhoduje o volbě mezi jinak srovnatelnými systémy různých výrobců.

- **Certifikace kvality**: je výhodné, pokud je kvalita a splnění uváděných parametrů produktu potvrzena některou nezávislou organizací.

Odkazy na některé nezávislé srovnávací testy bezpečnostních systémů můžete nalézt na adrese http:\\www.tsoft.cz.

Jak lze zajistit ochranu počítačových sítí

Za nejdůležitější nástroje pro dosažení bezpečnosti, pokud jde o počítačové sítě a jejich ochranu, lze považovat:

- autentizační systém,
- firewall,
- šifrovací systém.

Autentizační systémy

Základem bezpečnosti IS je nepochybně bezpečná autentizace uživatelů. Dosud je ochrana naprosté většiny systémů či sítí založena pouze na sdělení přístupového hesla, a s tím je řada problémů. Lidé používají slabá hesla, protože by si silná nezapamatovali a protože je nikdo nenutí tato hesla používat; hesla jsou používána dlouhou dobu, a není nijak zajištěna jejich ochrana. Kdokoliv je může odposlouchat během přenosu po síti, uživatelé si je navíc vzájemně prozrazují, píšou si je na monitor atd.

Jednou z možností, jak se proti tomu bránit, je doplňkový autentizační mechanismus, který zajistí, že se k danému serveru může přihlásit pouze uživatel patřící do určité skupiny. Tím nástrojem může být dedikovaný autentizační server (jednorázová dynamická hesla, autentizační kalkulátory), nebo třeba samotný šifrovací systém, nejlépe ve spojení s moderní technologií digitálních certifikátů. To jsou velice užitečné digitální „průkazy totožnosti“, které jsou založené na asymetrické šifrovací technologii. Existuje k tomu infrastruktura PKI, takzvaná **certifikační autorita** ve spojení s adresářem (LDAP, X.500), která se automatizovaně stará o obnovování průkazů, jejich skladování tak, aby si kdokoliv mohl zkontrolovat jejich platnost, rušení platnosti ukradených průkazů atd.

Firewally

Dalším známým nástrojem pro ochranu počítačových sítí je firewall. Obecně lze říci, že nástroj typu firewallu slouží především pro zabezpečení **vstupního bodu** do sítě z Internetu, nebo z jiné veřejné sítě. Firewall je především soubor opatření, která umožňují např. řízení přístupu uživatele z vnější i vnitřní sítě, nastavení přístupových práv, odfiltrování nebezpečných služeb, soustředění bezpečnosti do jednoho komunikačního uzlu, zablokování nepřátelského mapování vnitřní sítě, audit legálních a nelegálních operací atd.

Je však nutné mít na paměti, že ani pevné vstupní dveře ani inteligentní „vrátný“, provádějící kontrolu při vstupu, ještě nezajišťují bezpečnost dat při pohybu po síti. Přitom ochranu přenosu dat je žádoucí zajistit nejen ve vnější síti, ale také v síti vnitřní.

Firewally původně samy o sobě neposkytovaly žádné šifrovací služby; v posledních letech jsou sice doplňovány přídavnými šifrovacími moduly, ale ty jsou dodávány jen jako určitý doplněk; hlavní funkcí a smyslem firewallu je vždy ochrana samotného vstupního bodu.

Znamená to, že pro dosažení bezpečnosti datové sítě je nutno se ještě postarat o šifrování přenášených dat.

Šifrovací systémy

Šifrování dat, nebo obecně šifrovací systémy, poskytují následující služby:

- Ochranu **důvěrnosti** dat. To znamená, že všechna data jsou jakoby uložena do takové obálky, kterou nikdo nemůže rozlepit nebo prosvítit pod lampou a podobně.
- Ochranu **integrity** dat. To znamená, že na každé jednotlivé obálce je nějaká pečeť, a pokud by někdo změnil třeba jen jedno jediné písmenko, tak to adresát pozná, neboť pečeť přijde rozlomená.
- Zajišťují, že se lze i na dálku přesvědčit, kdo doopravdy data odeslal, dotyčná osoba to také nemůže popřít - pokud je to řešeno na aplikační úrovni. To znamená, že data jsou podepsána digitálním podpisem, který je více než plnohodnotnou náhradou skutečného fyzického podpisu.

Bezpečná VPN

Je nutné připomenout, že technologie bezpečné VPN do značné míry zahrnuje všechny tři výše zmíněné bezpečnostní nástroje:

- bezpečnou autentizaci,
- řízení přístupu ke zdrojům (firewall),
- šifrování dat.

Častou chybou je, že pojem VPN je spojován pouze s poslední ze zmíněných služeb, t.j. se šifrováním přenosu dat. Ve skutečnosti jsou však moduly VPN schopny výborně řešit nejen požadavky bezpečné autentizace založené na digitálních certifikátech X.509, ale i požadavky řízení přístupu ke zdrojům, neboli služby firewallu (i když „jen“ na úrovni filtrování paketů).

Samostatnou výhodou specializovaných systémů VPN je možnost **distribuce správcovských rolí**. To znamená, že je možné rozdělit správu minimálně takovým způsobem, aby se řadový systémový správce staral pouze o chod sítě jako takové, a o řízení bezpečnosti se staral zvláště prověřený *bezpečnostní správce.*

Kombinace VPN a firewallu

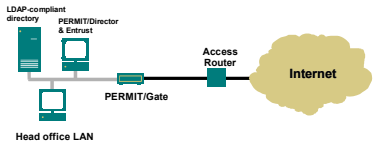
Šifrovací systém určený pro tvorbu VPN lze kombinovat s jakýmkoliv firewallem, mnoha způsoby; šifrovací modul může být umístěn:

- před firewallem,
- za firewallem,

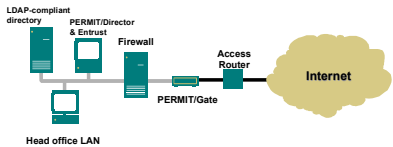
- paralelně s firewallem,
- VPN modul může sám fungovat jako „absolutní“ firewall - „dovnitř“ (k citlivým datům) jsou vpuštěni pouze určení uživatelé, podle nastavených pravidel, s platným certifikátem atd.

Optimálním uspořádáním pro *většinu* situací je **paralelní uspořádání,** neboli **VPN vedle firewallu**. Výhody tohoto paralelního uspořádání lze shrnout:

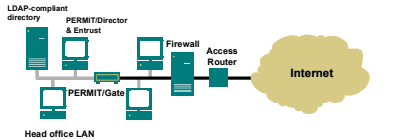
- přístup oprávněných uživatelů do vnitřní sítě (k interním zdrojům vyšší citlivosti) je chráněn systémem bezpečné VPN; t.j. - veškerý přenos citlivých dat je chráněn šifrováním, uživatelé jsou autentizováni digitálními certifikáty;
- přístup veřejnosti (cizích, neoprávněných uživatelů) do DMZ (veřejné, nechráněné informace) je chráněn firewallem: firewall řídí, zda cizí uživatelé mohou používat protokoly SMTP, HTML, atd.; není potřeba šifrovat přenos dat - data jsou veřejná;
- bezpečnostní politika je flexibilní a jednoduchá: lze výrazně rozlišit práva vlastních (oprávněných) uživatelů a cizích (neoprávněných) uživatelů;
- v provozu nejsou „úzká hrdla“ (komunikace může probíhat jednoduchým a rychlým způsobem).



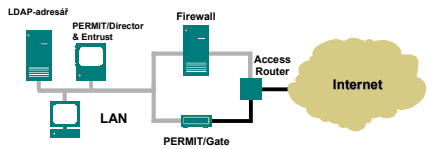
Obrázek 2 - VPN modul „místo“ firewallu



Obrázek 3 - VPN modul před firewallem



Obrázek 4 - VPN modul za firewallem



Obrázek 5 - VPN modul paralelně vedle firewallu

Odlišné uspořádání lze doporučit při využití systémů VPN pro ochranu speciálních vybraných segmentů uvnitř běžných sítí (například ochrana systémů zpracovávajících utajované skutečnosti, uvnitř sítí s „běžným“ provozem). V tom případě je vhodné kombinovat oba nástroje tím způsobem, že firewall chrání přístup do běžné sítě, a uvnitř, „za“ firewallem, je ještě druhá úroveň ochrany, představovaná speciálním systémem VPN.

Technologie bezpečné VPN

Bezpečná VPN (Virtual Private Network, neboli Virtuální privátní síť) je z technologického hlediska založena především na dvou součástech:

- IPSec - protokol zajišťující bezpečnost na síťové vrstvě,
- PKI a X.509 - nástroje zajišťující bezpečnou vzájemnou autentizaci komunikujících entit.

IPSec - šifrování na síťové vrstvě

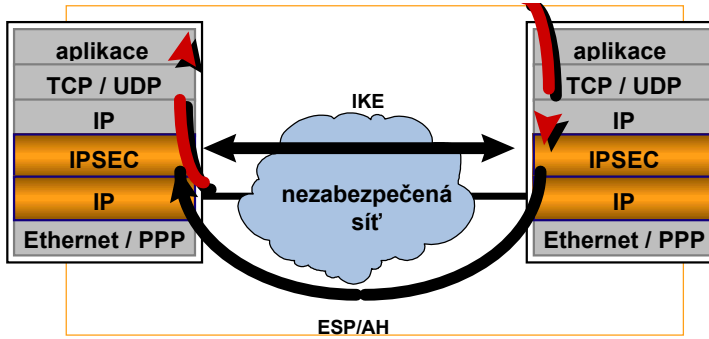
IPSec je otevřený průmyslový standard bezpečnostního protokolu, navržený skupinou IETF (*Internet Engineering Task Force*). Představuje soubor rozšíření protokolu IP, poskytujících bezpečnostní služby na síťové vrstvě. Je založen na moderních šifrovacích technologiích, poskytujících silné záruky z hlediska autentizace a důvěrnosti dat. Je kompatibilní jak se stávající verzí IP (v4), tak i s budoucí verzí IPv6.

Podrobné informace je možno nalézt v dokumentu „Understanding the IPSec protocol“ na webové adrese http:\\www.tsoft.cz.

Jak pracuje IPSec

Bezpečnostní prostředky v IPSec:

- **ESP** (Encapsulating Security Payload) - formát pro zapouzdření a zašifrování celé datové části paketu resp. i některých částí hlavičky. Šifrování poskytuje ochranu proti odposlouchávání.
- **AH** (Authentication Header) - autentizační hlavička paketu, která umožňuje kontrolu integrity a původce dat (totožnosti odesílatele).
- **IKE** (Internet Key Exchange, dříve ISAKMP/Oakley) - protokol pro navázání spojení s požadovanou úrovní zabezpečení a pro bezpečnou výměnu šifrovacích klíčů. Tento protokol umožňuje používat a spravovat šifrovací klíče i ve velmi rozsáhlých VPN (s desetitisíci uzlů).



Obrázek 6 - Technologie “Bezpečná VPN”

Obrázek 6 představuje souhrn toho, co všechno IPSec zajišťuje, pokud chcete například:

- odeslat e-mail nebo soubor,
- navázat spojení se serverem přes FTP nebo Telnet,
- pracovat v jakékoliv klient/serverové aplikaci, v serverové databázi, apod.,
- sdílet data z jiného počítače, včetně PC,
- cokoliv jiného - pokud chcete jakkoliv komunikovat.

IPSec pracuje na síťové vrstvě. Znamená to, že IPSec je zcela nezávislý na typu aplikace nebo operačního systému. Navíc je zcela nezávislý i na koncovém uživateli - uživatel nemusí dělat vůbec nic, a všechno proběhne zcela automaticky (vyjma případu, kdy se využívá autentizace metodou sdíleného hesla, přímo z koncového PC).

V rámci platformy IPSec jsou využívány následující mechanismy:

- symetrické algoritmy pro ochranu důvěrnosti přenášených dat (ESP - DES, 3-DES, CAST, RC5, atd.),
- hashovací algoritmy pro ochranu integrity přenášených dat (AH - MD5),
- asymetrické algoritmy pro ochranu přenosu jednorázových symetrických šifrovacích klíčů
  (IKE - RSA, Diffiie-Hellmann),
- digitální certifikáty X.509 pro ochranu veřejných klíčů RSA; pro bezpečnou autentizaci komunikujících entit.

Centrální správa VPN

Následující odstavce vysvětlují rozdíl mezi tím, co zajišťuje samotná platforma IPSec,
a nadstavbovými službami centrální správy: Security Policy Manager, PKI, certifikáty X.509, atd.

IPSec představuje ideální platformu pro automatické navázání bezpečného spojení podle nadefinovaných bezpečnostních pravidel.

Moduly IPSec, nebo VPN jsou nástroje, které šifrují. Tyto nástroje jsou schopny využít autentizační tokeny i jsou schopny využít (někým) nastavená pravidla, ale je nutno tyto samotné šifrovací moduly doplnit dalšími nástroji, které zajistí následující služby:

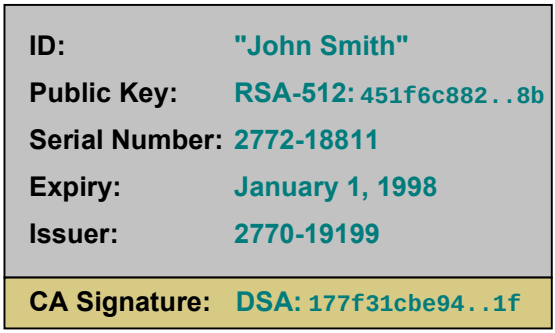
- definici bezpečnostních pravidel: určení, JAK se má šifrovat (jaké algoritmy se mají použít, s jakou délkou klíčů atd.) - **Security Policy Management**;
- výrobu autentizačních tokenů - např. digitálních certifikátů - **PKI**.

Bez certifikační autority je možno se obejít ve výjimečných případech, pokud je třeba šifrovat pouze jen mezi dvěma šifrátory. V takovém případě lze využít úspornou alternativní metodu: mechanismus sdíleného hesla - heslo se ručně zadá do obou šifrátorů, nastaví se (zase ručně) potřebná úroveň bezpečnosti pro tento jeden spoj, a je hotovo. Tento autentizační mechanismus „shared secret“ je však pro rozsáhlejší systémy vzhledem k manuální obsluze velmi **nepraktický až nebezpečný**.

Bezpečná autentizace - PKI, digitální certifikáty X.509

Jakékoliv dva komunikující uzly, dříve než spolu navážou bezpečné spojení (bezpečný tunel), si musí být zcela jisty vzájemnou identitou. Znamená to, že si musí vzájemně svojí identitu **prokázat**, neboli provést autentizaci. K tomu se nejlépe využívají **digitální certifikáty**.

Digitální certifikát si lze představit jako jakýsi občanský průkaz v elektronickém světě.



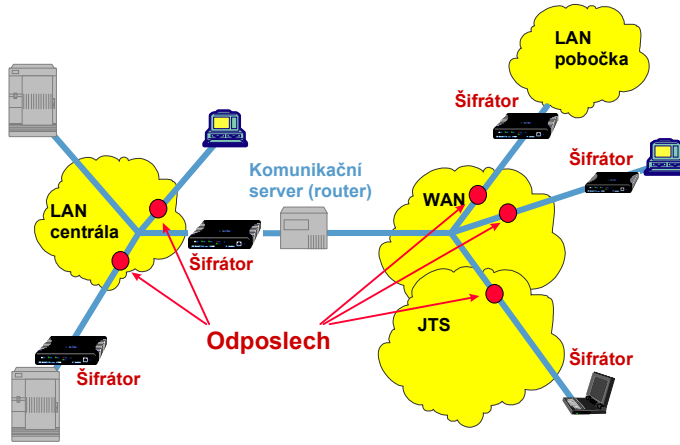
Obrázek 7 - Digitální certifikát X.509

Řízení bezpečnostních pravidel

Server bezpečnostní politiky slouží k centrální správě oprávnění - tj. řízení pravidel typu „kdo, s kým a s jakou úrovní zabezpečení“ smí komunikovat. Prvky bezpečné VPN si pak mohou ověřovat tato oprávnění vždy před vytvořením nového spojení. Informace se přenášejí bezpečným kanálem umožňujícím kontrolu integrity dat a autentizaci subjektů. Nejvhodnější metodou řízení přístupových oprávnění je využití standardu X.509, tvorbou tzv. „atributových“ certifikátů, které jsou skladovány a distribuovány jednotným způsobem, pomocí adresářů LDAP či X.500.

Při použití režimu s certifikační autoritou a s využitím modulu „VPN Group Manager“ (např. *PERMIT/Director*) lze snadno a přehledně řídit komunikaci také nadefinováním libovolného počtu skupin, neboli **virtuálních privátních sítí** (VPN). Lze vytvořit vícevrstvou strukturu z mnoha nezávislých či navzájem se překrývajících skupin VPN.

Aplikace VPN



Obrázek 8 - Hrozby odposlechu v datových sítích

Na schématu 4 je znázorněno rozhodování *které* komunikace vlastně šifrovat. Je nutné provést analýzu hrozeb, aktiv a výsledných rizik, a podle toho rozhodnout, zda aplikovat šifrovací systém na některém z uvedených typů komunikací:

- sítě WAN (od pobočky k pobočce),
- vzdálený přístup (mobilní uživatelé),
- interní sítě LAN,
- Extranet (spojení s externí organizací).

Závěr

Přednáška ukázala některé moderní trendy řešení bezpečnosti datových sítí - technologii VPN, založenou na platformách IPSec a X.509. Technologii VPN je možné snadno aplikovat pro zajištění bezpečnosti datových komunikací jakéhokoliv typu, a pro tvorbu bezpečných Intranetů i Extranetů.