Martin Zikmund

Co znamená bezpečnost a jak ji prodávat

Bezpečnost je často považována za do jisté míry abstraktní pojem. Každý chce být v bezpečí, ale ne každý ví, co pro to udělat, a jaká rizika na něj ve skutečnosti číhají.

Bezpečnostní řešení se tak na rozdíl například od tiskáren nedá prodávat jen ve formě krabic. Zákazník totiž často ani netuší, jakou „krabici" vlastně chce, a v komplexnějších případech ani neví, jak dané bezpečnostní řešení nasadit a nakonfigurovat. Velký prostor se tak zde vytváří jak pro šikovné resellery edukující své zákazníky, tak i pro VAR – prodejce s přidanou hodnotou (Value Added Reseller).

Než se pustíme do otázek nejrůznějších bezpečnostních hrozeb, tak bude dobré, podívat se na to, co by takový zákazník, poptávající bezpečnostní řešení, měl vlastně dostat. Je to podobné jako v onom pověstném případě zákazníka kupujícího vrtačku a vrtáky. Ten totiž ve skutečnosti nechce ani vrtačku, ani vrtáky, ale potřebuje někde vyvrtat díru. U bezpečnostních řešení je to podobné – zákazník nechce antivir, antispam, antispyware ani nic podobného „anticokoliv". Chce jen to, aby jeho data byla v bezpečí. Pojďme si tedy položit otázku, co to vlastně je ona bezpečnost.

Co znamená bezpečnost dat

Za zabezpečená data bychom mohli považovat taková data, u nichž mohou čtení, změnu, vymazání, tisk a zápis provádět pouze k tomu autorizované osoby, a tyto změny mohou provádět kdykoliv a odkudkoliv jsou k tomu oprávněni, přičemž všechny změny prováděné autorizovanými osobami se musejí v datech promítnout. Tato na první pohled nic neříkající definice má však dalekosáhlé důsledky. Bezpečnost totiž nespočívá pouz v aplikaci řady nástrojů proti malware (vi dále) a hackerům. Bezpečnost spočívá i v vytvoření bezpečnostní politiky ve firm v korektním nastavení práv, v důsledné odhlašování uživatelů od opuštěných p čítačů, ale třeba také ve vhodné topolog a konfiguraci lokální sítě, zálohování da řešeních storage a zajištění nepřetržitéh napájení při nejmenším pro servery. Jedin pak je možné zajistit bezpečnost ve smysl výše uvedené definice.

Jednotlivé hrozby

Malware je souhrnné označení pro ško livý kód, tj. software. Název vznikl spoj ním slov malicious (zlomyslný, konaný zlém úmyslu) a software (program). Dě se v zásadě do tří subkategorií – infikují malware (viry, červy), skrytý malware (tr ské koně, spyware) a malware vytváře pro zisk (spyware, skrytý adware).

Vnější nepřítel

První velká kategorie hrozeb by šla trefn zahrnout pod pojem vnější nepřítel. J o hrozby, které přicházejí zvenčí a bez p činění uživatele.

Spam (neobsahující malware) neboli n vyžádaná pošta patří spíše mezi nepřín bezpečnostní rizika. Zatěžuje totiž poštov servery a síťovou infrastrukturu a obtěžu koncové uživatele tím, že musí spam m zat, aby v jeho záplavě nepřehlédli skuteč e-maily, které je potřeba vyřídit. Spam n tedy stojí čas a výpočetní výkon, a tedy p níze. Navíc se odhaduje, že až 90 % vše e-mailů kolujících po internetu, je spam (dn už i v podobě příloh ve formátech pdf, jp ale i v hlasových souborech). Bránit pr spamu se lze pomocí antispamu. Jde o ap kaci instalovanou přímo na poštovním se veru. Někdy může být antispam integrov ve specializované komplexní hardwaro ochraně sítě. Antispamové filtry (filtry tří cí poštu), jsou také integrovány v některý poštovních klientech jako např. v Micros Office Outlook od verze 2003.

Viry – počítačový virus je program, jeh úkolem je zničit či pozměnit data, ane znemožnit uživateli používání jeho počítač Primárním úkolem viru však je, podobně ja v biologii, šířit se a přežít. Počítačový vir se tak obvykle neprojevuje ihned, ale až určité době či k určitému datu. Virus se š tím, že modifikuje spustitelné soubory dokumenty sady Office (tzv. makrovirus

Jako ochrana proti virům slouží antivi které by na rozdíl od antispamu měly b instalovány jak na poštovním serveru (kv

Výrobci bezpečnostního softwaru

Výrobce	Internetová adresa	Distribuce v ČR	Distribuce v SR
AEC (Cleverlance)	www.aec.cz, www.aec.sk	AEC	
Aladdin	www.aladdin.com	Atlas, Avenet, DNS	
Alwil Software	www.avast.cz	Alwil Trade	
BitDefender	www.bitdefender.com/cz	Tech Data Distribution	Tech Data Distribution
CA	www.ca.com/cz, www.ca.com/sk	eD' system Czech, SWS	eD' system Slovakia, SWS Distribution
Citrix	www.citrix.com	Soft-Tronik	Soft-Tronik SK
Danware	www.danware.com, www.netop.cz	NetOp Tech	
DriveLock	www.centertools.com	Servodata/Abakus	
Eset Software	www.eset.cz, www.eset.sk	AT Computers, Eset Software, SWS	Agemsoft, AT Computer, Eset Software, SWS Distribution
F-Secure	www.f-secure.com	SWS	SWS Distribution
GFi Software	www.gfi.com	SWS, Tech Data Distribution	Tech Data Distribution
Grisoft	www.grisoft.cz, www.grisoft.sk	AT Computers, BGS Levi Czech, SWS, Tech Data Distribution	Agemsoft, AT Computer, Cígler Software, eD' system Slovakia, SWS Distribution, Tech Data Distribution
Check Point	www.checkpoint.com	DNS, Soft-Tronik	
ISS (IBM)	www.iss.net	DNS	
Kaspersky Lab	www.kaspersky.cz, www.kaspersky.sk, www.dataguard.cz	Districom, PCS, divize DataGuard	PCS, divize DataGuard
Kerio Technologies	www.kerio.cz, www.kerio.sk	AT Computers, SWS, Tech Data Distribution	Agemsoft, BGS Levi Slovakia, SWS Distribution
McAfee	www.mcafee.com	DNS, SWS	SWS Distribution
Microsoft	www.microsoft.cz, www.microsoft.sk	BGS Levi Czech, eD' system Czech, SWS, Tech Data Distribution	BGS Levi Slovakia, SWS Distribution
nCipher	www.ncipher.com	DNS	
Norman ASA	http://nvc.cz/	RAY CZ	
PGP Software	www.pgp.com	SWS	SWS Distribution
RSA Security	www.rsasecurity.com	Soft-Tronik	Avnet Technology Solutions, Soft-Tronik SK
Sophos	www.sophos.com	Tempest Czech	Tempest
Symantec	www.symantec.cz	AT Computers, Avnet, eD' system Czech, Servodata/Abakus, Soft-Tronik, SWS	AT Computer, Avnet Technology Solutions, BGS Levi Slovakia, BSP Softwaredistribution, eD' system Slovakia, Soft-Tronik SK, SWS Distribution
Trend Micro	http://emea.trendmicro.com/emea/home/	DNS, RRC-CZ	Atedis, RRC-CZ
Utimaco Safeware	www.utimaco.cz, www.utimaco.sk	Avenet	Avenet
Webroot	www.webroot.com	Servodata/Abakus	
Websense	www.websense.com	DNS, Tech Data Distribution	Tech Data Distribution

Zdroj: DCD Publishing

Vzhledem ke skutečnosti, že nemáme k dispozici veškeré informace o převodu smluv o autorizované distribuci po spojení firem BGS Levi Slovakia a eD' System Slovakia, uvádíme v přehledu stav platný před sloučením.

Dodavatelé bezpečnostního hardwaru – IDS/IPS

Výrobce	Internetová adresa	Distribuce v ČR	Distribuce v SR
3Com	www.3com.cz, www.3com.sk	atlantis datacom, eD' system Czech, RRC CZ, Tech Data Distribution	BGS Levi Slovakia, eD' system Slovakia, Tech Data Distribution
Astaro	www.astaro.com	Annex NET	
Cisco	www.cisco.cz, www.cisco.sk	Alef Distribution, AT Computers, DNS, eD' system Czech, Tech Data Distribution	Alef Distribution, Avnet Technology Solutions
Crossbeam Systems	www.crossbeam.com	DNS, Soft-Tronik	
D-Link	www.dlink.cz, www.dlink.sk	Actebis Computer, eD' system Czech, Konsigna Handel, Tech Data Distribution	ABC Data, BGS Levi Slovakia, eD' system Slovakia, Tech Data Distribution
Enterasys Networks	www.enterasys.com/cz	DNS	
Fortinet	www.fortinet.cz, www.fortinet.sk	SkyNet	SkyNet
HP (ProCurve Networking)	www.hp.cz, www.hp.sk	AT Computers, DNS, eD' system Czech, Servodata/Abakus, Tech Data Distribution	Asbis SK, Avnet Technology Solutions, BGS Levi Slovakia
Check Point Software	www.checkpoint.com	DNS, Soft-Tronik	Atedis
Internet Security Systems (IBM)	www.iss.net	DNS	Atedis
Juniper Networks	www.juniper.net	Soft-Tronik, VUMS DataCom	Soft-Tronik SK
Nortel Networks	www.nortel.cz	Anixter, RRC CZ, Tech Data Distribution	Tech Data Distribution
SafeNet	www.safenet.cz	Gesto Communications	
Secure Computing	www.securecomputing.com	SkyNet	Agem Computers
SonicWall	www.sonicwall.com	RRC-CZ, Tech Data Distribution	Tech Data Distribution
StoneSoft	www.stonesoft.com	DNS	SWS Distribution
TippingPoint	www.tippingpoint.com	Tech Data Distribution	Tech Data Distribution
Zyxel	www.zyxel.cz, www.zyxel.sk	100Mega Distribution, eD' system Czech, Tech Data Distribution	BGS Levi Slovakia, Data, eD' system Slovakia

Zdroj: DCD Publishing

Vzhledem ke skutečnosti, že nemáme k dispozici veškeré informace o převodu smluv o autorizované distribuci po spojení firem BGS Levi Slovakia a eD System Slovakia, uvádíme v přehledu stav platný před sloučením.

červům), tak na aplikačním serveru (kvůli kontinuálnímu hledání infekce v síti), tak u uživatele na jeho počítači. I zde přitom existují specializované hardwarové prvky s integrovaným antivirem, které hledají viry přímo v datech kolujících po síti.

Červ je škodlivý kód, který se obvykle šíří v e-mailových zprávách, ale vyskytuje se na internetu ať již ve formě skriptu nebo spustitelného souboru na webových stránkách (viz dále). I jeho primárním úkolem je šířit se. K tomu červy obvykle využívají e-mail a databázi kontaktů v e-mailovém klientovi, kam se následně rozešlou. Řada červů se přitom chová částečně jako viry a dokonce na infikovaném počítači ničí soubory nebo znemožňuje práci. Velká část červů však využívá infikované počítače k (nechtěnému) rozesílání spamu a distribuovaným útokům (viz dále) na počítače a sítě připojené k internetu. Červy šířící se e-maily obvykle odstaví již přímo antispam. Ostatní červy pak dokáže eliminovat antivirus (viz výše).

Útoky DoS – tzv. Denial of Service neboli DoS (vynucené odmítnutí služby) je útokem, který se zaměřuje na webové a poštovní servery a internetové brány. Jeho jediným cílem je znemožnit užívání služeb daného serveru. Útok probíhá pomocí prostého zahlcení serveru velkým množstvím požadavků, dat či obecně, z čistě technického hlediska paketů, které najednou začnou v krátkém časovém okamžiku přicházet na daný server z určitého místa v internetu. Aby bylo možné skutečně server zahltit, používá se obvykle distribuovaný útok (tj. z více míst), tedy tzv. DDoS, Distributed Denial of Service). Právě k DDoS útokům jsou zneužívány počítače infikované červy. Proti DDoS útokům existují specializované nástroje pro pasivní a aktivní (tj. zpětný útok na útočící počítač) obranu.

Spyware neboli špionážní software má za úkol zpřístupnit své „špionážní centrále" informace obsažené v infikovaném počítači. Ať už jde o celkem obvyklé zachytávání a přeposílání přihlašovacích informací a hesel, anebo méně časté přímé zpřístupňování dat na počítači, riziko je vysoké. Spyware existuje jak necílený, tak je i vyvíjený na zakázku. Největším rizikem spywaru je způsob, jakým se šíří. Spyware je totiž často skryt v nejrůznějších freewarových aplikacích, které samy o sobě mají svůj užitek a nijak neškodí. Za speciální případ spyware lze považovat skrytý adware, který škodí „pouze" tím, že sbírá informace o tom, které stránky uživatel počítače navštěvuje a jaká klíčová slova obvykle zadává do vyhledávačů, a na základě toho mu pak samovolně zobrazuje vyskakovací reklamy. Spyware se do počítače dostává výlučně uživatelovou činností, ať již vědomým stažením nějaké aplikace, kde je spyware skryt, anebo „nechtěnou" instalací nějakého softwaru, což je případ obvykle se vyskytující u stránek s pornografickou tématikou. Ochránit před těmito riziky pomůže uživateli antispyware, který existuje podobně jako antivirus ve verzi pro koncové počítače, servery i v hardwarové verzi pro síť. Instalován by přitom měl být zejména na uživatelských počítačích.

Červy z webu/IM – speciální kategorií červů jsou ty, které se dostávají do počítačů přímo při surfování po internetu. Ty musejí na rozdíl od červů v e-mailech odstranit antivirový program na uživatelském počítači nebo uvnitř sítě. Tyto červi jsou podobně jako antispyware instalovány vědomou činností uživatele. Obvykle se s nimi lze setkat na webových stránkách s pornografií.

Phishing – zajímavým a relativně novým způsobem útoku je phishing. Jde o typ útoku, kdy je uživatel přiveden na web, který vypadá identicky jako jiný web, kam se chtěl uživatel ve skutečnosti dostat (typicky web internetového bankovnictví, web pro přístup do e-mailové schránky apod.). Jakmile uživatel zadá přihlašovací údaje, jsou tyto údaje odeslány útočníkovi a uživateli je buď zobrazena chybová hláška na falešném webu (u amatérských aplikací) anebo je přesměrován na onen skutečný web, který chybovou hlášku zobrazí. Phishing se nejčastěji vyskytuje v podobě e-mailových zpráv, pocházejících jakoby od provozovatele webu, a obsahujících správně napsanou URL na web s hypertextovým odkazem vedoucím ve skutečnosti jinam. Proti phishingu se lze chránit antiphishingovými filtry, které jsou například integrovány v aplikace Microsoft Outlook 2007 anebo jen vyšší pozorností uživatele, který by si vždy měl kontrolovat skutečné URL stránky v prohlížeči.

Záměrná infekce sítě

Velice nepříjemným aspektem mohou být také uživatelé, kteří se záměrně snaží infikovat počítačovou síť ve své firmě (typicky před odchodem ze zaměstnání). Uživatel se tedy snaží spustit nějaký malware na jednom či více počítačích ve firmě. Tuto činnost by však mělo eliminovat jednak nastavení uživatelských práv a jednak síťový antivirus.