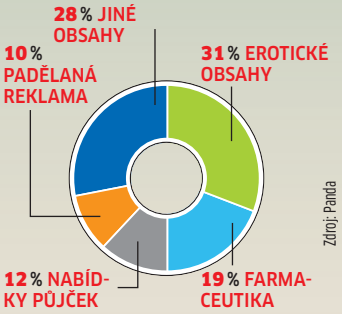
DATA A FAKTA

Barometr nebezpečí

I v povánočním období bývají hackeři velice aktivní. K nárůstu internetových napadení přispívá dokonce i celosvětová finanční krize.

Obsah spamových mailů



Zdroj: Panda

Spamové maily propagují nejčastěji pornografii a léky.

Nebezpečné doplňky

25 %	1. Java
20 %	2. Flash
14 %	3. Shockwave
12 %	4. QuickTime
11 %	5. MediaPlayer
10 %	6. Adobe PDF
5 %	7. Internet Explorer
3 %	8. Firefox

Zdroj: Desine

Tyto nástroje způsobují na ohrožených PC většinu bezpečnostních mezer.

Číslo měsíce

330 000

nových zombie PC každý den. Ty pak po světě rozesílají spamové maily.

Zdroj: Panda

Digitální pas zfalšován!

Stačilo několik kliknutí a jednoduchý hardware, aby bezpečnostní expert **ZFALŠOVAL E-PAS**, s nímž pak prošel kontrolou na letišti.

DOMINIK HOFERER

Elvis Presley žije! Objevil se na letišti Amsterdam Schiphol a nepozorovaně tam prošel bezpečnostní kontrolou. Žádný z úředníků po něm nechtěl autogram, ačkoliv se slavný zpěvák nijak neskrýval. Vždyť svůj elektronický pas i s čipovou kartou nechal zkontrolovat v tzv. „passport self-scan terminálu“ – automatickém čtecím zařízení digitálních cestovních pasů. U těchto přístrojů už se nepředpokládá přítomnost kontrolujících orgánů.

Fanoušky rokenrolového krále však musíme zklamat, neboť zmíněnou osobou samozřejmě nebyl pravý Elvis, ani žádný z jeho napodobitelů, nýbrž bezpečnostní specialista Jeroen van Beek. V soutěži Elvisových dvojníků by nepochybně skončil na posledním místě, jeho silné stránky však leží jinde: zfalšoval e-pas, který v Evropské unii postupně nahradí cestovní pas a který má také přinést větší bezpečnost. Pas však bohužel selhal. Není sice žádným tajemstvím, že s průkazy lze manipulovat, ale to, jak snadno se to expertovi podařilo, je šokující.

S nástroji všude volně dostupnými dokázal získat novou identitu a vyměnit fotku. Hacker dokonce zanesl do svých papírů novou smyšlenou zemi. Elvis by mohl žít v Lummerlandu, aniž by čtečka pasů vyhlásila poplach. A vyšlo najevo i další faux pas: Jeroen van Beek nepoužil žádnou krásně potištěnou bezpečnostní kartu, nýbrž obyčejný bílý plastový „polotovar“, jaký se prodává v obchodech. Optická kontrola karty by takový podvod okamžitě odhalila. A především – kde selhal počítač, tam by si člověk chyby povšiml. Avšak „děravé“ systémy usnadňují hackerům život.

Skladba elektronického pasu

Falšování hračkou: Snadná cesta k nové identitě

Návod a software, s nímž by teroristé mohli neomezeně překračovat hranice států, lze nalézt na webu. Zločinci pomocí čtečky nahrají CAB soubor na záznamové karetní médium a emulují e-pas. Dalším nástrojem pak existující kartu načtou, změní data a vloží novou fotku. Plyne z toho děsivý závěr: Ještě než se e-pas dočkal většího rozšíření, je už zase zastaralý. Komplikovaný odbavovací proces na letištích nám tedy zřejmě zůstane zachován.

INFO: www.thc.org

300 000 UKOŘISTĚNÝCH BANKOVNÍCH ÚČTŮ

Trojský kůň na loupežné výpravě

Na internetu už přes tři roky řádí zvláště zákeřný škůdce a není k zastavení. Bankovnický trojský kůň Sinowal alias Torpig prý sám za posledních šest měsíců vyšpehoval a odeslal do databanky na webu 100 000, celkově ale už přes 300 000 citlivých údajů. Mezi nimi přihlašovací data k bankovním účtům, čísla kreditních karet a FTP účty. Informovala o tom americká výzkumná laboratoř RSA FraudAction Research Lab.

Podle vyjádření antivirového výrobce Kaspersky přitom záškodník postupuje nesmírně rafinovaně: Jakmile se trojský kůň z infikované webové stránky dostane do počítače, nejprve se v něm zamaskuje technikou rootkitu. Poněvadž se zapíše do MBR na pevném disku, aktivuje se při bootování. Když pak uživatel vyvolá svou bankovní stránku, trojský kůň injektuje škodlivý kód a zobrazí falešný přihlašovací formulář. Postiženo má být přes 2 700 mezinárodních bankovních stránek.

INFO: www.rsa.com

Formulář: Originál, nebo falzifikát?

INFO

Nová bezpečnostní rizika

GOOGLE CHROME

Browser z Mountain View vykazuje mezeru, kterou by zločinci mohli využít k phishingovým útokům. Slabina vznikla chybou ve WebKit Engine v kombinaci s kódem Googlu.
Řešením je upgrade na verzi 0.3.154.9, kterou Chrome automaticky nabízí pro aktualizaci, ve které je již mezera zacelena.
INFO: www.google.com/chrome

OPENOFFICE

Hned dvě kritické bezpečnostní mezery jsou obsaženy v OpenOffice verze 2.4.1 a v jejích předchůdcích. Jak se proslýchá, pomocí „heap overflow" lze do počítače propašovat škodlivý kód.
Řešení je snadné – přejděte na OpenOffice 3.0.
INFO: http://www.openoffice.org

WINDOWS

Mezera ve službě Windows RPC usnadňuje červům proniknutí do počítače, odkud pak posílají zašifrovaná data do určitého serveru. Ještě není jasné, co datové pakety obsahují.
Řešením je instalace bezpečnostní aktualizace KB958644, kterou Microsoft nabízí na svém webu.
INFO: www.microsoft.cz

GOOGLE ANDROID

Mobilové viry

Ještě než se smartphone G1 od HTC s operačním systémem Android firmy Google objeví na našem trhu, je už známa jeho první slabina. Bezpečnostní aktualizací ji však „král vyhledávačů" rychle odstranil.

Uživatelé v USA, kde je přístroj na trhu od podzimu 2008, by tak mohli na záškodnických webových stránkách „chytit" škodlivý kód, který se v mobilu samočinně spustí. Malware by ovšem měl jen taková práva jako webový browser; že by se zmocnil kompletního telefonu, to možné není. Google ve snaze zvýšit zabezpečení přístroje totiž naprogramoval operační systém tak, že každá aplikace běží „na vlastním písečku" (v tzv. sandboxu), odděleně od operačního systému. Přesto by hackeři mohli tímto způsobem zachytávat citlivá data on-line bankovnictví nebo došlou poštu.
INFO: www.cnet.com

ON-LINE BEZPEČNOST

Nový ESET Online Scanner

Výhoda: Nový skener od esetu funguje jak v Internet Exploreru, tak i ve Firefoxu.

Nový ESET Online Scanner se dostává do procesu testování. Veřejná beta verze nového on-line skeneru již podporuje všechny hlavní internetové prohlížeče. Přichází také s novým grafickým rozhraním pro jednoduché ovládání a nově implementovanou technologií anti-stealth, detekující rootkity. Beta verze nového ESET Online Scanneru je k dispozici na **www.eset.cz/eos/eset-online-scanner**.

Uživatelé tak získávají možnost otestovat nový bezplatný nástroj na vyhledání a odstranění virů, spywaru, trojských koní, červů a dalších druhů počítačových hrozeb, a to bez potřeby mít nainstalovaný antivirový program. ESET Online Scanner se od své předcházející verze, která je k dispozici od léta 2007 (a která vyhrála náš srovnávací test), výrazně změnil. Ze všech vylepšení a novinek jsou pro uživatele zajímavé především:

► podpora i pro alternativní prohlížeče Firefox, Opera, Netscape a jiné, přičemž technická realizace je řešena přes aplikaci ESET Smart Installer, která nainstaluje potřebné komponenty a spustí on-line skener v novém okně daného prohlížeče;
► implementovaná technologie Anti-Stealth, sloužící pro detekci skrytých hrozeb – rootkitů;
► nový režim „léčení", který umožní do karantény automaticky přesunout všechny nalezené infiltrace;
► přepracované grafické uživatelské prostředí, poskytující jednodušší orientaci a zacházení s programem.

„I když ESET Online Scanner není náhradou za plnohodnotný antivirový software, uživatelé se často nemají jak dostat k plné ochraně proti hrozbám. Tehdy přichází ke slovu tento on-line nástroj. A tak jako většina konkurenčních produktů i ESET Online Scanner léčí počítač a odstraňuje všechny druhy hrozeb," říká Pavel Luka, ředitel pro IT společnosti ESET.
EOS je program, který umožní ověřit aktuální stav bezpečnosti počítače, pokud si uživatel není jistý jeho zabezpečením (např. veřejný počítač v internetové kavárně, ve škole atd.).

HROZBY A TRENDY

Jaké jste měli Vánoce?

Vánoční sezona bývá pro počítačové uživatele nebezpečná především kvůli kyberzločincům zneužívajícím jedno z nejhektičtějších nákupních období roku a spoléhajícím na různé metody sociálního inženýrství a podvodů, kterými lákají nic netušící oběti. Experti Trend Micro zkoumající počítačové hrozby tvrdí, že spotřebitelé, kteří nakupují před Vánocemi na internetu, mohou zvyšovat riziko průniku webových hrozeb, virů a pokusů o krádeže identity do domácích či podnikových sítí. Závěr roku je také ukázkou, co lze čekat v roce příštím a jaké jsou trendy v oblasti počítačových podvodů. Jaké tedy byly loňské Vánoce a co na nás čeká v roce 2009?

Deset nejnebezpečnějších hrozeb podle expertů Trend Micro:

1. Podvody lákající na slevy a výhodnou koupi
Autoři malwaru často přicházejí se slevami a speciálními nabídkami oblíbeného sezonního zboží, na které lákají uživatele klikající na nebezpečné odkazy a zadávající své osobní údaje do speciálně vytvořených falešných stránek a formulářů. Například nedávno objevený malware TROJ_AYFONE.A se v internetovém prohlížeči infikovaného počítače registruje jako objekt BHO (Browser Helper Object), takže je vykonán při každém otevření browseru. Zobrazuje falešnou reklamu na nedávno uvedený telefon Apple iPhone a také falešný web internetového obchodu, kde může být zakoupen.

2. Falešné charitativní weby Přispějte na Červený kříž!

Nebezpečí: Osobní údaje se z vás podvodníci snaží vylákat i pod vidinou velkých výher...

Pomozte obětem hurikánu Katrina! Kyberzločinci jsou experty na zneužívání kalamit a jiných tragédií. Vědí také, že online uživatelé mnohem více přispívají na charitativní akce během vánočního období. Spammeři obvykle posílají zprávy prosící příjemce o dar – ze štědrých uživatelů, kteří zprávu otevřou a kliknou na odkaz, jsou nakonec vymámeny důvěrné informace.

3. Blahopřání, která přinášejí neštěstí
Elektronické pohlednice (čili e-cards) jsou často zneužívány spammery a autory malwaru jako vějička na uživatele, kteří mají kliknout na nebezpečné odkazy. Tento typ útoku se také obvykle objevuje během vánočního období, kdy uživatelé často posílají e-pohlednice distribuované jako odkazy nebo přílohy se soubory. Kliknutím na odkaz nebo otevřením přílohy se pak malware stáhne do počítače.

4. Malvertisements: Nebezpečná reklama
Dobrý obchod chce udělat každý a kyberzločinci často zneužívají on-line reklamu a propagační akce k distribuci malwaru. Jako spouštěč stahování malwaru je často zneužívána reklama umístěná na webech s vysokou návštěvností. Oblíbené stránky jako Google, Expedia.com, Rhapsody.com, Blick.com, a dokonce Myspace byly napadeny škodlivými reklamními bannery obsahujícími malware **(http://blog.trendmicro.com/trojan-yields-google-badvertisements)**.

5. „Otrávené“ výsledky vyhledávání vánočních obchodních nabídek
Výsledky vyhledávání určitých slovních řetězců mohou být zamořeny malwarem. Jeho autoři pečlivě vybírají slovní řetězce podle ročních období a sezon tak, aby byly pokaždé co nejnebezpečnější. V roce 2007 se například ve výsledcích vyhledávání podle slovního řetězce „Christmas gift shopping“ (nákupy vánočních dárků) objevily nebezpečné odkazy vedoucí k rozmanitému malwaru. V tomto roce se mezi výsledky vyhledávání kostýmů pro halloween („Halloween costumes“) objevil odkaz na Rogue AV, malware označovaný jeho autory za antivirový software.

6. Zneužití webů s vysokou návštěvností
Kyberzločinci se orientují na masy – jejich cílem bývají populární weby s vysokou návštěvností zejména během různých svátků, Vánoc nebo lednových výprodejů, kdy do on-line obchodů, na aukce a weby pro e-commerci zavítá mnoho nakupujících.

7. Shromažďování osobních údajů – podvržené propagační akce s dárkovými poukázkami
Riziku tohoto typu podvodů bývají vystaveni uživatelé, kteří vyplňují zdánlivě neškodné on-line průzkumy výměnou za dárkové poukázky, hotovost či bezplatné dárky. Stránka s průzkumem je ve skutečnosti phishingovým webem a je součástí plánu na odcizení důvěrných informací.

8. Phishing zneužívající e-commerci
Kyberzločinci často spustí phishingový útok pomocí e-mailu, který se tváří, jako by pocházel z důvěryhodného zdroje, ale ve skutečnosti obsahuje nebezpečný odkaz. Tento odkaz pak uživatele přesměruje na podvržený web, který na první pohled vypadá reálně a legitimně. Například eBay je jedním z nejpopulárnějších internetových obchodů, ale je to také místo, kde kyberzločinci realizují nejvíce phishingových útoků.

9. Falešné účty za kurýrní služby, které obsahují trojské koně
Podvržené zprávy od oblíbených kurýrních služeb, které ohlašují dodávku balíku a obsahují i fakturu, bývají často infikovány trojskými koni. Snadnými cíli tohoto druhu scamu jsou nakupující přes internet, kteří právě očekávají dodání balíku.

10. Účtenky za fiktivní nákupy
Malwarem jsou infikovány i falešné účty zasílané e-mailem. Pokud uživatelé otevřou nebo kliknou na odkaz na nebezpečném účtu, jsou bezprostředně vystaveni nebezpečí krádeže identity. Stává se, že ze zvědavosti otevřou přílohu e-mailu i uživatelé, kteří online doklad o nákupu vůbec neočekávají.

MEZERA V OPEŘE ODSTRANĚNA

Ochrana browseru

Vývojáři opensourcového prohlížeče Opera uzavřeli aktualizací na verzi 9.62 několik slabých míst. Mezi nimi také závažnou mezeru umožňující „cross site scripting“ – vysoce kritickou chybu, která postihla vyhledávací funkci browseru.

Ve vyhledávacím poli totiž bylo možné spustit libovolný zdrojový kód. Útočník by tak mohl spouštět všechny v počítači nainstalované programy. Přes FTP by hackeři měli možnost zavést do počítače a spustit trojské koně či jiné škůdce. Vstupní bránu odhalil prohlížečový specialista Aviv Raff a poukázal na ni v nedávno uveřejněné ukázce. Proto nyní Opera důrazně doporučuje instalaci nové verze, která je k dispozici na její webové stránce.

INFO: www.opera.com

BEZPEČNOSTNÍ NOVINKA

Nový on-line skener souborů

Na konci roku byla spuštěna nová služba VirusTotal **(www.VirusTotal.com)**, která umožňuje automatickou kontrolu vybraného souboru pomocí 37 různých antivirových nástrojů. Na rozdíl od známé konkurenční služby na adrese **http://virusscan.jotti.org/** komunikuje zmiňovaná novinka i v českém jazyce. Zajímavým detailem je zobrazení výsledků o každém antiviru zvlášť, což může leccos naznačit o schopnostech antivirových programů. Další perličkou jsou podrobné statistiky o nebezpečných hrozbách, aktualizacích a o vytížení služby. Na webu ale bohužel chybí informace o maximální velikosti kontrolovaného souboru.

INFO: www. VirusTotal.com

HROZBA I PRO ČESKÉ UŽIVATELE

Vlna červů na Facebooku

Čím je služba populárnější, tím větší pozornost poutá. Tak by se dal charakterizovat důvod, proč již i čeští uživatelé Facebooku znají červa Win32/Koobface. Jeho různé varianty zneužívají ke svému šíření komunitu uživatelů Facebooku a mohou potenciálně stahovat další infiltrace. Z aktuálních statistik ESET ThreatSense.Net je zřejmé, že nová vlna Koobface začala již na přelomu listopadu a prosince. Řádově zatím zasáhla několik desítek tisíc počítačů po celém světě. Počítače českých uživatelů byly nakaženy doposud v několika desítkách případů, počet útoků však roste každý týden. Důvodem menšího šíření v ČR je fakt, že Facebook u nás není zatím tak rozšířen.

Uživatelé se s červem Win32/Koobface mohou setkat denně při zcela běžných úkonech prováděných v rámci Facebooku, a to tak, že dostanou oznámení od svých přátel, kteří jim doporučí zhlédnout konkrétní WWW link nebo spustit aplikaci. Po kliknutí na link nebo ukončení aplikace se uživatel může ocitnout na infikované stránce, přes kterou se do jeho počítače dostane například trojský kůň, adware atp. Podobnou metodou se již několik let šíří virové nákazy například přes ICQ.

Zmatené informace však zasílá svým uživatelům také samotný Facebook. V současné době, kdy se v rámci této sociální sítě šíří červ Koobface, komunikuje Facebook se svými uživateli zcela nevhodným způsobem. Zasílá jim výzvy na změnu hesla, což podmiňuje kliknutím na neznámý link. Uživatel takové výzvě nemusí věřit a zprávu ignoruje. V takovém případě může dojít až k bizardním situacím – uživatel se nakazí červem Koobface, ten následně stáhne do počítače další škodlivý kód, například trojského koně, který zaznamená přihlašovací údaje k účtu Facebook. Následně uživatel může dostat reálnou zprávu od Facebooku na změnu hesla, kterou ale ignoruje, a tak po chvíli jeho účet ovládne útočník.

ESET uživatelům sociálních sítí doporučuje, aby:
měli aktualizovaný internetový prohlížeč;
měli aktualizovaný antivirový software;
neklikali na neznámé linky;
pravidelně měnili přihlašovací údaje;
používali silná hesla (kombinace velkých a malých písmen, číslic).

Komentář redakce: *Je jen otázkou času, kdy si hackeři všimnou potenciálu českých komunitních sítí – jejich čeští uživatelé jsou ukolébáni minimem hrozeb a o úrovni jejich zabezpečení leccos napovídá i medializovaná krádež fotografií z Libimseti.cz.*

VIRY A MALWARE

Nejvíce nebezpečné jsou přenosné USB disky

Analýza ThreatSense.Net, statistického systému společnosti ESET, odhalila opětovný růst infiltrací šířících se pomocí USB disků a paměťových karet.

V pravidelném měsíčním žebříčku nejrozšířenějších světových hrozeb se na vedoucí pozici v listopadu vrátila směs infiltrací šířící se přes vyměnitelná média (především přenosné USB disky), označovaná jako INF/Autorun (11,74 %). Tyto infiltrace využívají automatického nastavení operačního systému Windows, které zabezpečuje okamžité spuštění obsahu CD, DVD či USB klíčenky ihned po vložení do počítače. Uživateli takové nastavení zpříjemňuje práci s těmito médii, z hlediska bezpečnosti je však velice riskantní. Doporučuje se proto vypnout v nastaveních operačního systému možnost automatického spouštění vyměnitelných médií po jejich vložení či připojení k počítači. Z údajů statistického systému ESET ThreatSense.Net vyplývá, že se jedná o jednu z nejrozšířenějších hrozeb na světě. ESET proto zařadil do plánované verze 4 svých produktů ESET NOD32 Antivirus a ESET Smart Security i speciální nástroj na kontrolu vyměnitelných médií.

Listopad vynesl na druhé místo v celosvětové rozšířenosti Win32/PSW.OnLineGames (11,06 %). Jde o již známou rodinu trojských koní, které monitorují stlačené klávesy a často používají rootkity, jež získávají informace a artefakty z on-line her, jako jsou Lineage či populární World of Warcraft. V průběžných žebříčcích nejrozšířenějších hrozeb si svou pozici neustále „vylepšuje“ Win32/Pacex.Gen. V listopadu zaznamenal celkem 3,78% detekcí ze všech zaznamenaných infiltrací. Je to generická směs hrozeb, která často provází trojany vykrádající hesla, případně informace z on-line her. Potenciálně nevyžádaná aplikace Win32/Toolbar.MyWebSearch byla v listopadu na čtvrtém místě (3,28 %), na páté místo pak pronikla novinka Win32/Patched.BU (2,40 %). Tato hrozba v sobě nenese žádné přímo nebezpečné části, označuje totiž systémové soubory, které byly pozměněny malwarem za účelem automatického spouštění infiltrací současně se spuštěním procesů těchto systémových souborů při startu počítače.

Lokální situace v listopadu neukazuje na rozdíl od světa žádné převratné změny. Na prvním a druhém místě je u nás i nadále známý adware, přičemž hrozby Win32/Toolbar.MyWebSearch (3,48%) a Win32/Adware.Virtumonde (3,41%) si od října jen prohodily pozice. Následuje INF/Autorun 2,48% na třetím místě a jedinou novinkou listopadových statistik je na čtvrtém místě Win32/Patchet.BU s 2,33%.

DATOVÉ HROZBY

Firmám a domácnostem hrozí datový kolaps

V tuzemských počítačích se data hromadí tak závratným tempem, že je uživatelé nestačí řádně ukládat, natož pravidelně zálohovat. V roce 2010 bude množství vytvořených a replikovaných informací tvořit 966 miliard gigabajtů. To je osmnáctkrát více než všechny knihy, které byly kdy napsány. Pomyslný komínek knih by sahal od Slunce až na Pluto a zpět. V záplavě dat hrozí nevratná ztráta klíčových dokumentů či chaos – uživatelé nebudou schopni potřebné informace v nahromaděných datech najít.

Firmám i domácnostem hrozí datový kolaps. Vyplývá to z interní analýzy technologických společností EMC a S&T CZ. Každý uživatel počítače v závislosti na své profesi denně vytvoří megabajty či gigabajty dat. Průměrný uživatel tak ročně vyprodukuje minimálně 40 GB dat, která nejčastěji zahrnují textové dokumenty, e-maily, fotografie a videonahrávky. „Z analýzy vyplývá, že až na výjimky z řad větších firem málokterá firma či jednotlivec řeší ukládání a archivaci dat. Je proto jen otázkou času,

Alternativa: V nedávném testu bezplatných internetových úložišť se dobře umístil i server Humyo.

kdy dojde ke kolapsu," řekl Jan Teuschel, technologický expert společnosti EMC, která je lídrem v oblasti ukládání a archivace dat. Firmy a zejména domácnosti si totiž do důsledku neuvědomují, že dnes uložená data musí být dostupná nejen příští rok, ale třeba i za desítky let. Experti ze společností S&T CZ a EMC se shodují, že rychlé tempo, kterým data na firemních i domácích discích přibývají, znamená reálnou hrozbu. Tou je myšlena situace, kdy potřebná data – například firemní smlouvy či fotografie z dovolené – nejsou dostupná. Datový kolaps může mít řadu podob: selhání či poškození úložného disku, jeho zcizení, neúmyslné smazání dat či třeba poškození nebo ztrátu záložního média. Uchovávání dat vytvořených samotným uživatelem by se dalo ještě zvládnout. Nicméně značnou část ukládaných souborů tvoří kopie dat vytvořených jinde: „E-mail s pětimegabajtovým obrázkem zaslaný deseti kolegům ubere kliknutím myši na firemních discích 50 MB prostoru. Pokud jde o velkou firmu, denní akumulace dat je nepředstavitelná," potvrdil Vojtěch Dvořák ze společnosti S&T CZ. Větší firmy jsou proto přibývajícími daty doslova zavaleny. Šéf informačních technologií společnosti Chevron například tvrdí, že jeho firma denně akumuluje dva terabajty dat, což je datový prostor, o kterém se ještě před několika lety tvrdilo, že by měl dvěma lidem vydržet na celý život.

Firmy mohou přijít o klíčová data a domácnosti o vzpomínky

Kolaps hrozí zejména těm firmám a jednotlivcům, kteří nemají vypracovaný systém ukládání a archivace dat. Mohou v důsledku o cenné informace navždy přijít nebo je jednoduše nenajdou. Nejde jen o pravidelné ukládání, ale i o to, kam se data ukládají a jak se archivuji. Kam tedy data ukládat? Jako nejspolehlivější metoda archivace dat se jeví pevné disky. Sice ani ty nemají neomezenou životnost, ale je možné je snadno monitorovat, a pokud se schyluje k poruše, lze data přenést na jiný disk. Souvisejícím trendem se proto stává budování centralizovaných úložišť dat, přičemž cena úložného prostoru se odvíjí od typu úložiště, množství uložených dat a doprovodných služeb.

Komentář redakce:
Alternativou ke zmiňovanému řešení problémů s daty může být námi několikrát zmiňovaná technologie „cloud computingu" (viz článek na straně 8). Ta předpokládá, že zákazník nebude mít na internetu jen data, ale i samotné programy – nebude si software kupovat a instalovat na disk, ale bude si ho pronajímat a spouštět z webu. Součástí „cloud computingu" je i ukládání dat s možností pravidelné archivace.

ÚTOK MALWARU NA WEB 2.0

Předpověď na rok 2009 podle společnosti Trend Micro

Raimund Genes, CTO společnosti Trend Micro, zveřejnil předpovědi pro letošní rok v oblasti počítačové kriminality. Hlavním rysem bude rostoucí snaha malwaru zneužívat funkce, technologie a kulturu Web 2.0.

Poroste také motivace při vývoji malwaru – v této oblasti jde o s stále větší peněžní zisky.

Předpokládá se, že hackeři budou využívat techniky, které se budou velmi podobat normálnímu zdrojovému kódu. Například IFRAMEs se k různým účelům využívaly už mnoho let před tím, než je hackeři začali zneužívat k distribuci malwaru. Kromě toho budou hackeři pokračovat v šíření infekcí vedoucích ke zneužívání internetových prohlížečů a dalších webových aplikací. Vydání prohlížeče Google Chrome, nadcházející oficiální vydání nové verze IE8 a vzestup aplikací využívajících prohlížeče jako platformy (např. Microsoft Silverlight a Adobe Integrated Runtime) poslouží jako nové cesty zneužitelné k šíření malwaru.

Ve snaze o ještě větší zisky vytvoří kyberzločinci nové modely a architekturu hrozeb. Dá se očekávat rozmach botnetů a útoků podobných „rootkitovým a stealth" hrozbám FAKEAV a MEBROOT. Modely hrozeb začnou využívat internetové prostředí a budou provozovány „in-the-cloud". Jejich tvůrci se zaměří na software a služby, které tyto funkce poskytují (např. Microsoft Azure). Očekává se, že v mnoha oblastech malwarových technologií dojde k dalšímu vývoji, kde budou autoři malwaru i nadále vytvářet zdrojové kódy, jejichž cílem bude vyhnout se odhalení a následnému odstranění. Předpokládá se, že budeme svědky nástupu většího počtu skupin malwaru, ale s menším množstvím variant. Tak bude pro antivirové firmy obtížnější vytvářet heuristicko-generické vzory pro jejich odhalování.

Dále porostou hrozby zneužívající chyby v „alternativních" operačních systémech, zejména s ohledem na rostoucí popularitu počítačů Mac a systému Linux (jehož podíl roste zejména v segmentu netbooků). Primárním cílem autorů malwaru však bude i nadále software Microsoftu. Uvedení Windows 7 v roce 2009 bude pro kyberzločince jistě výzvou k prolomení jejich ochrany. Testovací malware bude zneužívat platformu Microsoft Surface, a jak bylo zmíněno výše, autoři hrozeb také použijí Silverlight a Azure.

Mobilní zařízení budou v roce 2009 pro kyberzločince představovat nejsnáze zneužitelné cíle. Budeme svědky výskytu dalších hrozeb, jejichž účelem bude získávat peníze zneužitím mobilních technologií. S tím, jak budou mobilní telefony a další příruční zařízení propojeny se svými stolními protějšky, se dá čekat, že stále více hrozeb se bude pokoušet pronikat napříč více stroji a zařízeními prostřednictvím společných aplikačních platforem (např. .NET, Java atd.).

Kyberzločinci budou také pokračovat v pokusech o sociální inženýrství a budou k tomu zneužívat události, jména celebrit a politiků. Pozor by si měli dát i hráči, kteří očekávají nadcházející vydání her Starcraft 2 a WoW: Wrath of the Lich King. Útočníci se budou snažit zneužít i globální finanční krizi vzhledem k tomu, že tento problém se dotkne prakticky každého člověka.

Počet spamů během posledních let nepřetržitě rostl, a nejinak tomu bude i v roce 2009. Nejvíce „prospamovanou" zemí zůstanou Spojené státy, nejvíce zasaženým kontinentem pak bude Evropa.

INFO

Nová bezpečnostní rizika

SUN SOLARIS

V operačním systému Sun Solaris byla odhalena zranitelnost způsobená blíže nespecifikovanou chybou v Name Service Cache Daemon (nscd(1M)). Chyba může být zneužita k obejití bezpečnostních opatření a k získání zvýšených privilegií. Chyba je hlášena u Solaris 10 Update 4 (8/07) – platforma SPARC a x86. Řešením je aplikace záplat, které spolu s bližšími informacemi naleznete na webu SunSolve.com.

INFO: zpravy.actinet.cz

KOLIZE V MD5

Na stránkách Technické univerzity v Eindhovenu byl zveřejněn proof of concept (www.win.tue.nl/hashclash/rogue-ca/), který popisuje, jak lze s využitím kolize v MD5 funkci vytvořit falešný certifikát subordinate CA, který se tváří, že je podepsán kořenovou certifikační autoritou. Protože webové prohlížeče automaticky důvěřují certifikátům kořenových certifikačních autorit, zobrazí se stránka jako ověřená. Tím mohou uživatelé získat falešný pocit, že se nacházejí např. na internetovém bankovnictví své banky.

INFO: zpravy.actinet.cz

PŘEHRÁVAČ ZUNE

Zunicida – tento termín se vžil mezi uživateli přehrávačů Zune pro jednu z vlastností, která rozhodně nepotěší. Pokud se zařízení zapne ve středu, zatuhne. Microsoft intenzivně pracuje na odstranění problému. SecurityFocus upozorňuje i na další trable s přenosnými zařízeními (www.securityfocus.com/brief/878), jako byl Apple iPod, popřípadě Samsung s předinstalovanými viry. Podle Microsoftu se problém týká interního ovladače hodin ve spojení s přestupným rokem. Instrukce, jak se dočasně vypořádat s problémem z2k9, najdete na webu **http://coreygo.com/**.

INFO: zpravy.actinet.cz

ROUTERY CISCO

The Register píše o zajímavém objevu výzkumníka z Recurity Labs v Berlíně. V routerech Cisco běžících na procesorech PowerPC a MIPS lze s využitím kódu ROMmonu (podobný BIOS v PC) kompromitovat IOS (software ve většině zařízení Cisco). Více informací naleznete v původním článku **(www.theregister.co.uk/2009/01/05/cisco_router_hijacking/)**.

INFO: zpravy.actinet.cz

SECURITY 2009

Odborná konference

Konference Security 2009 společnosti AEC si za šestnáct let své existence vydobyla pozici jedné z největších konferencí se zaměřením na oblast počítačové bezpečnosti, konaných v České republice.

Její letošní ročník se bude konat ve středu 18. února od 9 hodin v pražském hotelu Diplomat.

Konference bude věnována aktuálním otázkám bezpečnosti informačních a komunikačních technologií. Pořadatelé připravili široký průřez IT hrozbami z pohledu chování uživatelů a bezpečnostních rizik souvisejících s IT strukturou organizací i případných cílených útoků. Se svými příspěvky vystoupí přední odborníci na oblast počítačové bezpečnosti, a to nejen ze společnosti AEC. Konference je určena pro odbornou veřejnost ze státní i soukromé sféry.

Podrobnější informace včetně programu a anotací jednotlivých přednášek naleznete na webových stránkách pořadatele.

INFO: www.konference.aec.cz

DĚTSKÝ FILTR V SOFTWARU TRUSTPORT

Ochrana nejen pro děti

Podle průzkumu Eurobarometr, prováděného od října do prosince ve všech zemích Evropské unie, v průměru 75 % dětí ve věku od šesti do sedmnácti let používá internet. Největší podíl dětských uživatelů internetu byl zjištěn ve Finsku (94 %), nejmenší v Itálii (45 %), mezi státy v pomyslném středu statistiky bylo také Česko (84 %).

Počátkem prosince byla schválena celoevropská kampaň „Bezpečnější internet“, která má za cíl zlepšit ochranu dětí v prostředí stále více se rozvíjejících on-line služeb. Záměr odhlasoval Evropský parlament a následně ho potvrdila Rada ministrů Evropské unie. Kampaň chce zaváděním bezpečnějších webových a mobilních technologií zabránit tomu, aby se internetu zneužívalo proti dětem. Eurokomisařka pro informační společnost a média Viviane Redingová upozornila, že děti dnes vstupují do světa internetových technologií ve velmi raném věku. „Protože jim tyto technologie pomáhají studovat a poskytují jim zajímavé nové způsoby, jak navazovat vztahy s druhými, začínají je často používat dříve než jejich rodiče,“ řekla Viviane Redingová. „Musíme zajistit, aby rozpoznaly možná rizika a dokázaly si s nimi poradit, kdykoli používají webové nebo mobilní služby.“

Standardní součástí bezpečnostního softwaru TrustPort PC Security a TrustPort Antivirus je proto nyní i technologie rodičovského zámku. Tato technologie pracuje na základě neustále aktualizované databáze webových stránek, které svým obsahem spadají do určité nežádoucí kategorie, jako je kupříkladu pornografie. Pro počítačové sítě škol či knihoven lze doporučit řešení TrustPort WebFilter. Toto řešení se instaluje na vstupní bránu sítě a nabízí tak centrální sledování a blokování internetového surfování na všech počítačích v síti. Lze ho implementovat také jako součást uceleného bezpečnostního řešení TrustPort Net Gateway.

Komentář redakce: *Rodičovské zámky a webové filtry jsou už nyní součástí všech pokročilejších bezpečnostních řešení. Důležitou vlastností, která podstatně ovlivňuje výkon takovéhoto filtru, je pravidelná aktualizace databáze. Při výběru bezpečnostního řešení lze navíc rodičům (i firmám) doporučit důkladné vyzkoušení produktu, aby si ověřili, zda vyhovuje jejich potřebám.*

MALWARE

Nová hrozba pro Windows

V poslední době se začíná šířit nebezpečná hrozba Win32/Conficker. Jde o síťového červa šířícího se zneužíváním známé zranitelnosti v operačním systému Windows. Slabina se nachází v RPC podsystému a červ ji dokáže zneužít i na dálku. Win32/Conficker se snaží stáhnout do počítače různé infiltrace, především adware (nevyžádaná reklama). Kromě toho vypíná Windows firewall a spouští http server na náhodném portu. I když většina antivirů tuto hrozbu dokáže odhalit, doporučujeme uživatelům nezapomínat na update operačního systému.

INFO: www.eset.cz