

Některé bezpečnostní technologie, dříve určené spíše nadšencům a profesionálům, jsou již natolik jednoduché, že je může využívat prakticky kdokoli.

Bezpečná komunikace bez finančních ztrát

Jaké jsou z vašeho pohledu nejvýznamnější aktuální trendy v oblasti bezpečnosti?

Zásadní trend bude další profesionalizace útoků, zvláště ve tvorbě malwaru. Pokud bude pokračovat vývoj stejným způsobem, jaký naznačily Stuxnet, Zeus nebo Operation Aurora, tak se můžeme dočkat ještě sofistikovanějších kusů kódu, které budou kombinovat více zero-day zranitelností, budou se zaměřovat na konkrétní data a budou téměř dokonale naprogramované. To svědčí o velkém kapitálu, který za podobnými projekty stojí. V případě Stuxnetu si můžeme být jisti, že za útoky nestála pouze skupina schopných nadšenců.

Oproti profesionalizaci útoků také můžeme očekávat větší množství nástrojů dostupných běžným uživatelům, které budou provádět jednoduché a dlouho známé útoky, ale pomocí dostupného uživatelského rozhraní. Mohou se tak opakovat podobné události, které vyvolalo zveřejnění rozšíření do Firefoxu, nazvané Firesheep.

Státy po vzoru USA investují do zabezpečení své digitální infrastruktury a budou v tom pokračovat dále. Evropa nechtěla zůstat pozadu



Robert Šefr, IT security consultant, Comguard

a společně s agenturou European Network and Information Security Agency (ENISA) bylo provedeno několik testů reakcí na výpadky kritických systémů (např. následkem DDoS útoku). Ale jedná se pouze o jednu z prvních vlastovek řešení bezpečnosti informačních technologií na úrovni EU. První vlastovka ovšem přichází poněkud pozdě a je pouze otázkou času, kdy budeme svědky podobných problémů, jaké způsobil Stuxnet v iránských jaderných zařízeních.

Jakých chyb se v současnosti uživatelé nejčastěji dopouštějí?

Jedním z problémů je stále nezaplatovaný software. Zatímco na aktualizace u operačních systémů si již uživatelé zvykají, aktuální software jako např. Adobe Reader nebo Flash na uživatelských strojích je spíše výjimkou. S doplňkovým softwarem je navíc ten problém, že lze těžko hlídat jeho verze napříč společnostmi, a vznikají tak zranitelná místa v síti, která se těžko opravují.

Dalším problémem je samozřejmě chování uživatelů na sociálních sítích, tedy především na Facebooku. Šíření malwaru, XSS červi, úniky dat, ztráta soukromí, kyberšikana. To vše na Facebooku bez problému najdeme, ale na vině jsou spíše lidská naivita, důvěřivost a lehkomyšlnost než sofistikovanost útoků.

Které nové technologie bychom podle vás měli pozorně sledovat?

Velmi zajímavý bude vývoj antivirových technologií. S přírůstkem malwaru roste i velikost souborů se signaturami, což se negativně projevuje na rychlostech skenování a distribuci aktualizací. Dalším závažným problémem zůstává okno zranitelnosti, kdy systém není chráněn, dokud nejsou signatury aktua-

lizovány. Lokální heuristika většinou nepomůže a navíc má velké problémy s falešnou detekcí. Na oba dva problémy se mohou zaměřit cloudové technologie.

Neznámé soubory (resp. jejich otisk) se kontrolují vůči cloudu, který má přehled o aktuální situaci ve světě, a tedy víc podkladů pro heuristiku, a kontrolou v reálném čase je minimalizováno okno zranitelnosti. Pokud výrobci bezpečnostního softwaru zvládnou optimalizovat rychlost kontroly otisků a potvrdí přínos pro uživatele, možná přijde velmi zásadní změna v boji proti malwaru. Jedním z příkladů může být systém McAfee Global Threat Intelligence, který kombinuje senzory sbírající data a cloud komunikující s klienty.

Za pozornost bude příští rok stát i vývoj produktů společnosti Intel, která svoje zaměření na bezpečnost deklarovala akvizicí společnosti McAfee. Můžeme očekávat hlubší spolupráci hardwaru a softwaru při ochraně dat a systémů.

Některé technologie, dříve určené spíše nadšencům a profesionálům, jsou již natolik jednoduché, že je může využívat prakticky kdokoli. Jedná se hlavně o software na šifrování disků a souborů, který byl vždy považován za nutný, ale také za velmi obtížně nasaditelný.

Šifrování PGP a novinky do nového roku

O produktu a šifrování PGP toho bylo na těchto i jiných stránkách napsáno mnoho, nebudu tedy popisovat samotný produkt, ale jen uvedu jeho některé vlastnosti a především pak, co nového můžeme očekávat od PGP a nových verzí.

Od začátku prosince jsou k dispozici nová verze PGP Desktop 10.1 a nová centrální správa PGP Universal Server 3.1. Obě verze přinášejí zajímavé novinky a posilují bezpečnost a další slavitelnost.

PGP Whole Disk Encryption 10.1 nově přináší podporu Intel Anti-Theft, a tím rozšiřuje možnosti řešení problému ztráty, resp. zcizení přenosných počítačů, jeden z nejčastějších bezpečnostních problémů spojovaných právě s přenosnými počítači. Veškerá data na disku jsou neustále šifrována pomocí PGP Whole Disk Encryption a v kombinaci s novou verzí centrální správy PGP Universal Server 3.1 a dokoupením PGP Remote Disable & Destroy (RDD) lze vzdáleně laptop zablokovat a znemožnit jeho využití

při zachování bezpečnosti uložených dat. V momentě zcizení tak lze zablokovat počítač a přístup k jeho datům. Blokadu můžeme udělat lokálně pomocí předdefinované politiky, např. při dosažení počtu neplatných přihlášení, pokusu o přímý přístup k HW apod. A protože se dříve nebo později dá očekávat připojení cizího laptopu k internetu, druhou možností je jeho zablokování vzdáleně přes internet. Jestliže pak dojde k navrácení laptopu nebo jeho nalezení, můžeme blokadu zrušit a začít jej plně využívat stejně jako před samotným incidentem.

Dalšími novinkami, kromě podpory Microsoft Exchange Server 2010 u PGP Desktop Email, je možnost vynucení změny hesla u PGP Portable na přenosných USB zařízeních a nový command line nástroj u PGP NetShare. Pomocí PGP NetShare lze chránit šifrováním jednotlivé soubory i celé adresáře, a protože se jedná o šifrová-

ní na úrovni obsahu souborů, jednoduchou cestou takto můžeme chránit i sdílené složky, a to bez instalace jakékoliv serverové komponenty.

PGP se pomalu, ale jistě začíná zabydlovat pod křídly Symantecu, plnou integraci PGP do portfolia Symantecu lze očekávat během roku 2011. Přejít na jednotnou platformu se před-



pokládá skrze standardní proces upgrade verzí. Díky postupnému slučování ale již nyní přicházejí drobné změny a prvním krokem v migraci je změna licenčního

portálu (Licence and Entitlement Management System, tzv. LEMS Portal), který se využívá pro stažení softwaru, správu a vygenerování licencí. Jeho hlavní změnou je zjednodušení a eliminace potřeby plánování modelu využití licencí a teprve na jeho základě vygenerování platných licencí. Místo toho je nyní přímo dostupné získání platných licencí. Kompletní seznam změn i s novými FAQ by měl mít v této době každý klient k dispozici.

Michal Mezera,
senior security consultant, Comguard