BusinessIT.cz
ebook

Bezpečnost firemních dat

Nové hrozby zvyšují rizika ztrát

Redakce BusinessIT a partneři

E-kniha založená na speciálu BusinessIT.cz. Edice BusinessIT eBooks 2013.

Bezpečnost firemních dat: Nové hrozby zvyšují rizika ztrát

BusinessIT.cz

Edice: BusinessIT ebooks
Autoři: Redakce BusinessIT.cz
Copyright © Bispiral, s.r.o., 2013
Vydáno v roce 2013 v Bispiral, s.r.o.
Názvy použité v této knize mohou být ochrannými známkami příslušných vlastníků.
web: www.BusinessIT.cz

Na jedné straně stojí externí útočníci, kteří mají na svědomí mimo jiné rostoucí počet útoků typu DoS a DDoS nebo nové typy malwaru, na straně druhé zaměstnanci, kteří mnohdy svým nezodpovědným jednáním vystavují firemní data zbytečným rizikům. A někde uprostřed pak IT oddělení nebo – v případě malých firem – osamocený zaměstnanec IT, který

má najít efektivní řešení. Jaké jsou aktuální trendy v oblasti bezpečnosti a možnosti obrany?
V této eknize jsme se zaměřili na dvě hlavní témata: Prvním z nich jsou útoky typu DoS a DDoS, o kterých se v posledních týdnech hodně mluvilo i v ČR, ale jejichž počet a intenzita jsou na vzestupu celosvětově. Druhým tématem jsou pak vybrané slabiny zabezpečení IT prostředí ve firmách – které, bohužel, přetrvávají i po mnohých varováních.
K ruce jsme si tentokrát vzali zprávy analytiků i výrobců, abychom výše zmiňované informace mohli dát do konkrétních souvislostí. A pro odlehčení sem přidáváme i náš nedávno publikovaný text o autentizaci prostřednictvím mozkových vln. V praxi sice takové řešení zřejmě ještě nějakou dobu neuvidíme, ale to nic nemění na tom, že jde o zajímavý koncept – s poměrně slibnými výsledky testů.

Redakce BusinessIT.cz

Partnerem této eknihy je:

Je třeba se připravit na nárůst útoků DoS a DDoS

Útoky typu DoS a DDoS zažívají v posledních měsících doslova znovuzrození. A nemáme tím na mysli jen to, že se na začátku března výrazně přihlásily o slovo také v České republice, když byly postupně napadeny zpravodajské weby, největší internetový portál nebo weby bank či mobilních operátorů. K růstu počtu a intenzity těchto útoků dochází celosvětově. Co můžeme očekávat v nejbližší době a jak se připravit?
Analytici IDC upozorňují, že útoky DOS (denial of service) a DDoS (distributed denial of service) v poslední době nabraly nejen na intenzitě, ale také na síle. Útočníci přitom podle nich mají velmi široké zaměření – napadají nejrůznější služby od blogovacích platforem přes firemní informační weby z nejrůznějších odvětví až po internetové prodejce.

Společnost Prolexic upozorňuje, že v letošním prvním čtvrtletí se ale útočníci v zámoří soustředí ze všech nejvíce na poskytovatele internetového připojení, a to DDoS útoky s extrémně vysokou intenzitou odesílání paketů. Její Global DDoS Attack Report pak ukazuje, že zvyšující se intenzita útoků znamená výraznější problémy pro bezpečnostní zařízení i pro sítě poskytovatelů připojení nebo CDN (content delivery networks). V prvním čtvrtletí letošního roku podle stejného zdroje průměrná šířka pásma útoku činila 48,25 Gb/s, což prý oproti předcházejícímu čtvrtletí znamená růst o 718 %.

Útoky jsou stále propracovanější

„V roce 2012 jsme byli svědky nové úrovně propracovanosti organizovaných útoků na firmy po celém světě a je třeba počítat s tím, že v roce 2013 jejich propracovanost a efektivita dále poroste," předpovídá Avivah Litanová, viceprezidentka Gartneru. Připomíná několik masivních útoků na americké banky z konce loňského roku. Nejde prý o náhodu, ale o soustředěnou práci kriminálních živlů.

Hlavním trendem se v příštích měsících mají stát skutečně velmi masivní útoky. Na ty nejsofistikovanější by se pak podle analytiků společnosti Gartner měly letos připravit především firmy poskytující finanční služby a významní internetoví prodejci.

„S tím, jak narostly množství a propracovanost útoků, mnohé organizace byly zastiženy nepřipravené. Kapacity, které měly k dispozici, byly v průběhu útoků rychle vyčerpány a weby se staly nedostupnými. To si žádá proaktivní řešení, které firmy ochrání před současnými i budoucími útoky," tvrdí Christian Christiansen, viceprezident IDC pro výzkum v oblasti bezpečnosti. Analytici této společnosti předpovídají, že trh s produkty a službami pro prevenci útoků DDoS dosáhne mezi lety 2012 a 2017 složené roční míry růstu 18,2 % a v roce 2017 dosáhne objemu 870 milionů amerických dolarů.

Pro uvedené období předpovídají analytici také růst počtu útoků využívajících sofistikovaných přístupů; běžnějšími by se měly stát hybridní útoky pracující na aplikační vrstvě nebo zneužívající šifrování. Analytici Gartneru přitom odhadují, že již v letošním roce bude

čtvrtina útoků typu DDoS zneužívat přímo funkce on-line aplikací. Nicméně největší počet bude stále útoků postavených čistě na hrubé síle a zahlcení velkým počtem jednoduchých požadavků.

Jak se útokům bránit

Útoky typu DoS a DDoS, jak známo, způsobí nedostupnost serverů tím, že je zahltí falešným provozem, takže nezvládnou odbavovat legitimní požadavky uživatelů. Požadavky přitom mohou, jak už bylo naznačeno, mířit na různé komunikační vrstvy systémů.
Zatímco ve svých počátcích byly tyto útoky často dílem nejrůznějších aktivistických skupin, dnes jde prý často především o peníze. S růstem počtu a intenzity těchto útoků, který trvá již od minulého roku, se podle analytiků mnohdy dostane i na firmy, které s něčím takovým dosud neměly žádnou zkušenost. Analytici upozorňují, že běžné firewally a zařízení pro prevenci průniku sice mohou odvrátit útoky menšího rozsahu, ale rozsáhlé útoky jsou nad jejich síly. V některých případech se dokonce mohou stát

spojenci útočníků, protože nejsou schopna rozlišit legitimní a nelegitimní provoz.
Nejlepší obranou proti oběma skupinám útoků bude podle Johna Gradyho z IDC kombinace bezpečnostních zařízení chránících infrastrukturu klienta a využívání cloudových služeb. „Organizace, pro něž je přítomnost na webu kritickou součástí jejich byznysu, by měly využívat vrstveného přístupu, který kombinuje různé druhy ochrany před útoky DoS," radí Litanová. Upozorňuje přitom, že útočníci se svými akcemi mnohdy snaží odvést pozornost obsluhy a získat pak další nenápadnou činností citlivé informace.
Analytici IDC rovněž upozorňují, že s růstem počtu cloudových služeb a se stále větší popularitou mobilních zařízení roste rovněž počet potenciálních cílů útoků typu DoS a DDoS. Jestliže v uplynulých letech se o nich příliš nemluvilo, nyní prý nastává doba, kdy se opět dostanou na výsluní zájmu.

Ochrana dat je leckde poněkud

zanedbávanou prioritou

Ochrana dat patří podle aktuální studie IDC k největším prioritám malých a středně velkých evropských firem – spolu se zajištěním dostatečného výkonu IT infrastruktury a snižováním nákladů na IT. Navzdory tomuto tvrzení se však v ukazuje, že v praxi činěná rozhodnutí k vysoké bezpečnosti mnohdy ani zdaleka nevedou. Důvodů k tomu je několik – od nezkušenosti po podcenění rizik.

Někdy je problémem neznalost

Řada zaměstnanců především malých firem má jen mizivé ponětí o bezpečnostních rizicích. Lze se tak běžně setkat se stavem, kdy se ani citlivá data nešifrují, a to ani při ukládání na disk, ani při přenosu nezabezpečenými kanály (například e-mailem). Mnohdy tu nijak neřeší ani riziko odcizení dat zaměstnanci – neexistují žádná pravidla pro nakládání s CD, DVD nebo flash disky.
Lepší situace bývá u antimalwaru, o jehož užitečnosti už ví i neodborníci. Záleží však na použitém produktu,

jaká rizika pokrývá. Jeho volba přitom záleží na mnoha okolnostech – nikoli ovšem zpravidla na hlubším vyhodnocení požadovaných vlastností, ale spíše na doporučení z okolí nebo na tom, jaký produkt byl na počítači nainstalován při jeho koupi. A tak třeba otázka záplatování bývá ponechána na libovůli nainstalovaných aplikací – a na jejich automatických nástrojích.
S bezpečnostními problémy se ovšem lze setkat i u firem, jejichž techničtí zaměstnanci disponují příslušným know-how. Na některé z těchto problémů opakovaně upozorňují dodavatelé technologií. I přesto, že svými argumenty zpravidla chtějí především podpořit prodej svých produktů, jejich varování nelze brát na lehkou váhu.

Firmy ignorují zranitelná místa

Jedním z problémů je fakt, že firmy na svých počítačích i po celé měsíce nechávají nezabezpečený software. Analýza dat z cloudové databáze Kaspersky Security Network prý odhalila 132 milionů neřešených zranitelností na více než 11

milionech počítačů, což je v průměru 12 zranitelností na uživatele. Z velké škály zranitelností jich ovšem bylo jen osm široce využíváno kybernetickými zločinci – pět z nich v Javě od Oracle, dvě v Adobe Flash Playeru a jedna v Adobe Readeru.
Výzkum ochoty uživatelů přejít na novou a bezpečnější verzi softwaru odhalil, že šest týdnů po vydání nejnovější verze Javy (na přelomu září a října 2012) jich program aktualizovalo jen necelých 30 %, zatímco 70 % nechalo svůj systém zranitelný. Zastaralou a snadno zneužitelnou verzi Adobe Flash Player z roku 2010 mělo na počítačích přes 10 % uživatelů, přičemž po celý rok 2012 se toto číslo téměř neměnilo. Podobně na tom byla i zranitelnost verze Adobe Readeru objevená v roce 2011 – byla přítomná na 13,5 % počítačů.

Stále komplexnější bezpečnostní systémy

Analytici IDC také upozorňují, že bezpečnostní řešení jsou stále složitější, což je problémem pro 41 % firem. IT infrastruktura firem dnes zahrnuje sítě, servery, desktopy, notebooky, chytré telefony i

tablety a kybernetický útok může být zacílen na kteroukoli její součást. Pro mnohé firmy je tak vhodnou odpovědí komplexní multifunkční bezpečnostní řešení, které dokáže zabezpečit jakýkoli koncový bod infrastruktury.

Zástupci společnosti Kaspersky ale upozorňují, že u takových řešení mnohdy vznikají potíže s kompatibilitou a náklady na jejich správu mohou rapidně narůstat. Snadnější tak bývá pořídit jednodušší bezpečnostní řešení, což ale mnohdy znamená kompromisy a sníženou úroveň zabezpečení. Zdánlivě ekonomická úvaha tak může podle nich nakonec vést k značným finančním ztrátám i k poškození firemní pověsti.

Vhodnějším řešením je podle jejich názoru nákup jediné platformy, která zahrnuje rozsáhlé portfolio aktualizovaných technologií schopných zabezpečit všechny části infrastruktury, přičemž správa je řešena pomocí jediné centrální řídící konzole. Taková platforma typicky obsahuje nástroje pro ochranu serverů, desktopů a mobilních zařízení proti aktuálním kybernetickým hrozbám i technologie, které zabrání nepovolaným uživatelům k přístupu k firemním datům.

Zneužívání přístupu na web zaměstnanci

Na jiný problém poukazují zástupci společnost GFI. Podle jejího lokálního průzkumu provedeného v březnu 2013 mezi jejími prodejními partnery až 90 % českých podnikových zákazníků registruje zneužívání pracovního internetu svými zaměstnanci k soukromým účelům. Zástupci firem prý přitom mají obavy ze ztráty produktivity práce, úniku citlivých dat, zavlečení virů do firmy a zahlcení kapacity podnikové sítě.
Faktem, že zaměstnanci firemních zákazníků zneužívají webový přístup k mimopracovním účelům, si je jisto 57,4 % prodejních partnerů, 32,8 % partnerů se domnívá, že ke zneužívání dochází. Jen necelých 10 % respondentů si je jisto, či se domnívá, že u jejich zákazníků ke zneužívání nedochází. Jako největší hrozbu zneužívání pracovního webu vidí podnikový management ztrátu pracovní produktivity zaměstnanců (73,8 %), únik citlivých dat či přihlašovacích informací (54,1 %), zavlečení virů (50,8 %), zahlcení kapacity podnikové sítě (34,4 %)

a právní zodpovědnost za případné porušení autorských práv zaměstnanci (16,4%). 8,2 % respondentů pak nepovažuje soukromé brouzdání po pracovním internetu za hrozbu.
I přes zmíněné obavy pouze 29,6 % podniků pravidelně nebo alespoň občas vyhodnocuje reporty o přístupu zaměstnanců k podnikovému webu s podporou specializovaného nástroje. Téměř polovina z celkového počtu respondentů (49,2 %) alespoň blokuje přístup k určitým webovým stránkám a téměř dvě třetiny (65,6 %) uvedené problémy toleruje.

Liknavá ochrana mobilních zařízení

Podle průzkumu týmu Norton společnosti Symantec zaměstnanci riskují i se svými mobilními zařízeními. Dva z pěti uživatelů mobilních zařízení v Evropě například přiznává, že ne vždy stahují aplikace z důvěryhodných zdrojů, a více než jedna třetina uvedla, že při nákupech ze svého mobilního zařízení nepoužívají bezpečné platební metody. Většina dospělých v Evropě prý využívá bezplatné nebo

nezabezpečené veřejné Wi-Fi hotspoty, a to přesto, že se téměř polovina z nich obává možných rizik. To vše může být problémem v době, kdy se leckde razí přístup BYOD, tedy využívání osobních mobilních zařízení i pro pracovní účely. Ohrožena totiž jsou nejen soukromá data, ale také ta firemní. Naprostá většina (69 %) evropských mobilních uživatelů v průzkumu uvedla, že ukládají citlivé informace do mobilních zařízení, přičemž více než třetina (35 %) jich přiznala, že k ochraně svých osobních údajů nepoužívá heslo. V případě krádeže nebo ztráty mobilního zařízení se tak kdokoli může dostat k osobním informacím, včetně e-mailů, které mohou být branou k dalším citlivým informacím, jako jsou pracovní e-maily a dokumenty, hesla pro ostatní on-line účty nebo bankovní výpisy. Tři z deseti Evropanů přitom už mají vlastní zkušenost se ztrátou nebo krádeží mobilního zařízení.

Největší nepřítel bezpečnosti mobilních zařízení? Složitost firemního systému

Společnost IDC v jedné ze svých posledních studií zveřejnila informaci o tom, že prodej tabletů dohnal v České republice prodej laptopů. Zkombinujeme-li uváděná čísla s prodejem chytrých telefonů, můžeme prohlásit, že mobilní zařízení jsou dnes co do počtu pravděpodobně na špici mezi používaným hardwarem. A nejenom kvůli programům BYOD se jimi musejí začít intenzivně zabývat také podnikoví uživatelé.

Podle celosvětového výzkumu společnosti Forrester ze čtvrtého čtvrtletí loňského roku by rádo své soukromé mobilní zařízení ke každodenní práci využívalo 75 % zaměstnanců. Oproti předchozímu roku je to tříprocentní nárůst. Většina z nich pak preferuje chytrý telefon. Z výzkumů B2B International pro Kaspersky Lab z loňského léta přitom vyplývá, že právě ztrátou nebo odcizením mobilního telefonu zaměstnance došlo k úniku citlivých dat u 38 % dotázaných firem.

Pro podniky to znamená zdolání tří hlavních výzev – ochranu podnikových dat, zvýšení výkonnosti a zabezpečení mobilních zařízení jednotlivých uživatelů. Ochrana podnikových dat je klíčovou záležitostí při

jakýchkoliv úvahách o přístupu zaměstnanců do firemní sítě. Kybernetičtí zločinci v současné době využívají k průnikům do počítačových systémů bezpečnostní díry v běžně používaných programech, jako jsou produkty Adobe nebo Java či webové prohlížeče. Množí se také útoky na operační systém Android, nicméně ani iOS už není v této oblasti bez poskvrny. Uživatelé mohou přicházet o peníze v případě trojských koní, které z mobilu odesílají prémiové SMS bez jejich vědomí.

Problémem je komplexnost

Největším nebezpečím pro podnikové systémy je dnes jejich komplexnost. Pouhý antimalwarový software v této oblasti rozhodně nestačí. Nejmodernější systémy správy mobilních zařízení Mobile Device Management (MDM) si navíc musí umět poradit s několika problémy naráz – nejenom umět sledovat všechna koncová zařízení přistupující do sítě, ale v případě jakékoliv ztráty zabránit úniku informací. Zároveň musí zvládnout ochránit jak přístroje, které dá zaměstnavatel svému

zaměstnanci, tak i ty, které si do práce přinese zaměstnanec sám.
Vhodným řešením může být architektura systému MDM na principu klient/server. MDM server odešle instrukce do mobilního zařízení. Klientské aplikace na něm pak vzápětí zpracují informaci a provedou přidělený úkol. Technologie zavedené do softwaru MDM přitom mohou využít funkčních možností dostupných na oblíbených systémech, jako jsou Apple MDM nebo Microsoft Exchange, případně na specifických řešeních pro určité operační systémy jako je třeba Android.
S pomocí MDM je pak možné vytvořit, standardizovat a nastavit profily mobilních podnikových e-mailů, vytvořit a spravovat pravidla pro mobilní přístup do korportátních sítí, šifrovat a na dálku vymazat data v přístroji, instalovat, aktualizovat a odstraňovat programy nebo aplikace, zablokovat ztracená a odcizená zařízení, spravovat anti-virovou ochranu a mnoho dalšího.

Pomůže centralizace

Ze zkušeností IT administrátorů vyplývá, že zvláště efektivní pak bývá centralizované řešení MDM, napojené nejlépe na správu celé sítě – hardwaru, softwaru i přístupu do ní. Umožňuje totiž IT operátorům mít přehled o celém systému. Vhodný nástroj by také měl umět oddělit v daném zařízení soukromá data od těch firemních, aby se zajistila nejenom bezpečnost podnikového systému, ale i soukromí samotných zaměstnanců.

Nakonec je ale nutné podotknout, že se při úvahách o MDM nesmí podcenit vzdělávání samotných zaměstnanců. Ti totiž také představují riziko pro firmu, zvláště když si na zařízení, které využívají k přístupu do podnikové sítě, instalují zranitelné aplikace či operační systémy. Firemní data často vynášejí na nezabezpečených USB discích a samozřejmě se na cestách přihlašují k síti skrze chytrý telefon nebo tablet. Často přitom neuvažují nad tím, zda je například právě využívaná wi-fi síť bezpečná.

Jan Sekera, Channel Manager, Kaspersky Lab

Útočníci stále častěji ohrožují menší firmy

V roce 2012 došlo meziročně ke 42% nárůstu cílených útoků, přičemž jejich cílem byly často krádeže duševního. Stále častěji jsou terčem firmy z výrobního sektoru a malé organizace - druhé jmenované nyní až v 31 % případů. Tvrdí to alespoň společnost Symantec ve své zprávě Internet Security Threat Report (ISTR). Malé podniky jsou podle zástupců firmy atraktivními cíli samy o sobě, ale zároveň mohou být prostředkem pro ohrožení větších firem prostřednictvím útoků typu „watering hole“.

„ISTR 2013 ukazuje, že kyberzločinci nezpomalují své tempo a pokračují v hledání nových způsobů, jak krást data z organizací všech velikostí,“ říká Stephen Trilling, chief technology officer Symantecu.

„Propracovanost útoků ve spojení s dnešním složitým IT světem, zejména díky virtualizaci, mobilitě a cloudu, vyžaduje od firem i nadále proaktivní přístup a používání komplexních bezpečnostních řešení, pokud chtějí zůstat v bezpečí,“ dodává.

Symantec podle zprávy zaznamenal největší nárůst

cílených útoků mezi podniky s méně než 250 zaměstnanci. Malé podniky jsou nyní terčem ve 31 % všech těchto útoků, což je významný nárůst oproti roku 2011. Zatímco malé podniky mohou mít pocit, že jsou imunní vůči cíleným útokům, zločince zjevně lákají jejich informace o bankovních účtech, údaje o zákaznících i duševní vlastnictví. Útočníci se zaměřili na malé podniky, které často nedodržují adekvátní bezpečnostní postupy a nemají odpovídajícím způsobem zabezpečenou infrastrukturu.

Webové útoky

Počet webových útoků vzrostl v roce 2012 o 30 %. Řada z těchto útoků prý pochází z napadených webových stránek malých podniků. V útocích typu „watering hole“ ohrožuje útočník webové stránky, například blogy nebo webové stránky malých firem, které vytipovaná oběť často navštěvuje. Když oběť později navštíví ohroženou webovou stránku, pronikne cílený útok bez povšimnutí do počítače. Jedním z prvních, kdo začal aktivně využívat tento typ útoků, byl Elderwood Gang. V roce

2012 prý během jednoho dne úspěšně napadl 500 organizací. V těchto scénářích útočník využívá slabé zabezpečení jednoho podniku k obcházení potenciálně silnějšího zabezpečení jiné firmy.
Ze zprávy ISTR plyne, že 61 % škodlivých webových stránek jsou legitimní webové stránky, které byly ohroženy a infikovány nebezpečným kódem. Obchodní a technologické webové stránky a stránky zaměřené na on-line nakupování patří mezi top pět typů stránek se skrytým škodlivým kódem. Symantec uvedený fakt připisuje na vrub neopraveným zranitelnostem na legitimních webových stránkách. Oblíbenou variantou škodlivého kódu se stal ransomware, zvláště nebezpečná útočná metoda, protože přináší útočníkům vysoké zisky. Útočníci zneužijí napadené webové stránky k infikování a uzamčení přístroje nic netušícího uživatele a za jeho odemknutí požadují výkupné. Dalším stále častějším zdrojem infekce na webových stránkách je malvertisement. Zločinci nakoupí reklamní prostor na legitimních webových stránkách a použijí jejk zamaskování svého útočného kódu.

Útočníci zamířili na výrobní sektor

Vládní organizace vystřídal v poslední zprávě na špičce nejčastěji napadaných organizací výrobní sektor. Symantec věří, že za touto změnou je nárůst útoků zaměřených na dodavatelské řetězce. Kyberzločinci vytipují dodavatele a subdodavatele s cennými informacemi, u kterých je pravděpodobnost úspěšného útoku. V případě napadení podniků v dodavatelském řetězci získají útočníci přístup k citlivým informacím ve větších společnostech. Hlavním cílem kyberútoků prý také již nejsou top manažeři. V roce 2012 byli nejčastější obětí těchto typů útoků ve všech odvětvích znalostní pracovníci (27 %) s přístupem k duševnímu vlastnictví a s přístupem k informacím o prodejích (24 %).

Jak je na tom mobilní malware

V minulém roce vzrostl počet mobilního škodlivého kódu o 58 % a 32 % všech mobilních hrozeb se prý pokoušelo ukrást informace, jako jsou například e-mailové adresy a telefonní čísla. Překvapivě tento nárůst nemusí souviset jen s 30% nárůstem

mobilních zranitelností. Zatímco Apple iOS měl nejvíce zdokumentovaných zranitelností, Symantec ve stejném období zaznamenal jen jednu hrozbu. Android měl naopak méně zranitelností, ale více hrozeb než jakýkoli jiný mobilní operační systém. Android se díky svému tržnímu podílu, otevřené platformě a širším možnostem šíření škodlivého kódu stal oblíbenou platformou kyberzločinců. Dodejme, že Internet Security Threat Report vychází z dat sebraných desítkami milionů internetových senzorů. Monitorovány jsou tak skutečné aktivity počítačových zločinců, což poskytuje široký pohled na stav internetové bezpečnost.

Jak se vypořádává s bezpečnostními hrozbami největší hostingová firma v ČR, WEDOS

Jako hostingová společnost s více jak 5 000 virtuálními servery a takřka 35 000 webhostingy se s bezpečnostními hrozbami potýkáme prakticky

pořád. Naše zákaznická i techniká podpora řeší každý den desítky problémů našich zákazníků, kteří podcenili bezpečnostní rizika. Co jsou nejčastější příčiny? K čemu jsou nejvíce využívány napadené služby? Jak bránit svá data online i offline?
(Tato kapitola je partnerským příspěvkem.)

Náš systém

Základem webhostingu je dobře připravený systém. Ten náš, na který jsme patřičně hrdí, byl vybudován na více jak 15 letech zkušeností. Už od základu byl navržen tak, aby byla většina bezpečnostních hrozeb minimalizována. Důraz byl kladen zvláště na prevenci. Když děláte něco tak velkého jako je webhosting, nemůžete se spokojit s improvizací, nedokonalostmi anebo se přizpůsobit stávajícím řešením. Je nutné vše upravit a v případě, že nějaká služba toto neumožňuje, tak si vybrat jinou, či vytvořit vlastní. Díky tomu jsme za 32 měsíců našeho provozu neměli žádný bezpečnostní incident, i když nejen z logů vidíme, jak to každý den někdo zkouší. Ovšem nehodláme do budoucna nic podcenit.

Připravujeme několik výzev pro firmy zabývající se bezpečností a hackery na volné noze, kteří pokud je pokoří a pomohou nám odstranit problém, získají nehynoucí slávu a finanční odměnu.

Zavirované internetové stránky našich zákazníků

Převážná část zavirovaných stránek jsou masově používané redakční systémy - CMS. Přitom jednoduchou a nejúčinnější obranou je pravidelná aktualizace. To platí nejen o samotném CMS, ale i různých doplňcích, které si k němu zákazníci instalují. Spousta lidí používá zrovna ty, které už jejich tvůrci nevyvíjí a neopravují bezpečnostní chyby.
Dalším oblíbeným nešvárem je stahování doplňků z různých neoficiálních stránek. Lákadlem je dobře vypadající „vylepšená verze“ ovšem často se zadními vrátky.
Poslední rok se také šíří trend zpoplatňovat doplňky formou prémiových služeb. Lidé, kteří chtějí ušetřit, si tak často stáhnou doplněk se škodlivým kódem z nějakého warez webu.

Jen pro zajímavost: Většinu bezpečnostních chyb v známých CMS zneužívají roboti k tomu naprogramovaní. Ti prochází doslova internet a hledají neaktualizované verze.

Zcizené FTP údaje

Nějčastěji dochází ke zcizení hesla k FTP prostřednictvím virů, které si je dokáží vytáhnout z oblíbených FTP klientů, jako je například Total Commander či FileZilla. Nejjednoduší je si do nich hesla neukládat. Ovšem trendem dnešních dnů jsou i viry, které prochází emailové zprávy uložené v poštovním klientovi přímo u zákazníka v počítači. Hledají v nich specifické řetězce či odesílatele. Schválně kolik z vás si z Outlooku či Thunderbirdu smazalo email s vygenerovaným heslem k FTP? Právě zkušenosti našich zákazníků nás vedli k myšlence zavést zablokování a povolení FTP přístupu z administrace v zákaznickém rozhraní WEDOS. Je to jednoduchý úkon, který vám může ušetřit spoustu starostí a hodně zákazníků jej i využívá.

Samotné viry pak zákazník nejčastěji chytne ze zavirovaného emailu. Pak jsou to statisticky internetové stránky s falešným antivirem, dále neaktualizovaný Adobe acrobat reader a Java.

Napadené servery a webhostingy

A co se děje s napadanými servery a webhostingy, jakmile k nim získá útočník přístup? Nejčastěji z nich odchází ven phishingové emaily, na druhém místě je to pak klasický spam. Třetí místo u nás mají DoS útoky.

Jak se bráníme proti rozesílání emailů

Tento trend trvá více méně už řadu let, proto jsme také při návrhu webhostingu zvolili omezení 500 odeslaných emailů na den. Za 32 měsíců provozu na tento limit většina zákazníků nikdy nedosála. Ti, kteří potřebují posílat větší množství, si buď emaily rozloží na více dní, anebo po dohodě jim limit můžeme navýšit. Samozřejmě nás musí ujistit, že mají vše patřičně zabezpečené. Víme, že to je pro těch

několik procent lidí nepříjemné, ale díky tomuto limitu mail servery WEDOS nekončí v různých black listech.
V momentě kdy je napadený webhosting, řešíme to zakázáním PHP funkce mail. U VPS je situace složitější. Snažíme se vše urychleně řešit s majitelem, ovšem v momentě kdy ven proudí miliony emailů, je nutné sáhnout v krajním případě i k odpojení. O všem je samozřejmě zákazník informován emailem, popřípadě SMS.

DoS a DDoS útoky

Po emailech jsou to pak s velkým odstupem DoS útoky. Ty ovšem nenapáchají oproti emailům takové škody. Můžeme zasáhnout rychle a vše se vyřeší během pár minut.
WEDOS je známý hlášením pravidelných DDoS útoků, které na nás cílí. Spousta lidí se nás ptá, jak takový DDoS útok vlastně probíhá. Lidé si představují naše techniky jak sedí u počítačů vedle velké interaktivní mapy světa s říkají: „Detekován útok zřejmě z Ruska! Síla 2 Gigabity za vteřinu a

roste! Pokuste se jej lépe zaměřit. Snažím se, ale je přesměrován přes několik proxy serverů. Přesměruj všechnu energii do obranného firewallu! Snažím se, jsme na 50%! Počkat ... zdroj útoku zaměřen. Připravují se k protiútoku...“

Takhle to ve skutečnosti ani zdaleka není. Vlastně je to nudná záležitost. V kancelářích máme velký monitor, kde se vypisují problémy, včetně přetížení jednotlivých tras a úseků, routerů, prostě taková tabule s chybovými hlášeními. DDoS útoky začínají jako oranžové hlášení a většina i tak skončí. Jen výjimečně se zobrazují červené. Kapacita jednotlivých tras to v pohodě utáhne. Uvnitř datacentra máme zase 1Gigabitové propojení mezi routery. Technik se podíva, co se děje a zareaguje podle situace. Většinou jde jen o DoS útok cílený na jednu IP adresu, přes nějaký port. Technik zakáže port a tím to končí. Když se jedná o rozsáhlejší DDoS útok a cílem je nějaká kritická část infrastruktury, postupuje většinou postupným vypínáním útočících IP adres. Takže si jej představte nad počítačem jak myší ukazuje na tabulku IP adres a postupně je klikem zabíjí. Opravdu nic zábavného natož adrenalinového.

Hrozba číhá i mimo internet

Bezpečnost dat na internetu je jedna věc. Ovšem spousta lidí si neuvědomuje, že hrozby číhají i pro data mimo něj. Často se na vašem serveru nachází informace, o které by mohla mít zájem konkurence anebo dokonce nějaký podvratný živel. Osobní informace, čísla kreditních karet, přístupová hesla, marketingová data, dokonce i celé účetnictví se často nachází na serverech. Provozovatel webhostingu je musí chránit nejen online ale i offline. Například u nás dostáváme 3 – 5 oficiálních žádostí ohledně webů přes datovou schránku za týden. To nejsou takové ty naštvané výhrůžky soudem emailem, kde se autor odvolává na velké zvíře v rodině. Ty dostáváme samozřejmě také, ovšem co nejde oficiální cestou jako by nebylo. V tomto ohledu musíme postupovat samozřejmě podle zákona. Převážná část žádostí se týká provozovatele a jeho aktivit. Výjimečně se setkáváme i s žádosti o vypnutí webu, ovšem zamezení provozu jde spíše přes CZ NIC, který může zablokovat rovnou doménu.

V každém případě si neumíme představit, že bychom zákazníkovi vypnuli web, protože se někomu nelíbí jeho obsah a zaplatil si dopis sepsaný právníkem. Takovéto případy se dějí poměrně často. Ovšem k tomu je třeba soudní rozhodnutí, nikoliv jen papír s kulatým razítkem. Bohužel se u nás najdou „provozovatelé webhostingu“, kteří takovému „nátlaku“ podlehnou. Na druhou stranu WEDOS využívá poradenství známé právní kanceláře BBH, takže jsme si i v složitějších případech celkem jisti. Navíc už jsme si nejednou právní šarvátkou prošli. Právě otázka bezpečnosti byla jedním z kritérií, proč jsme v našem datacentru upustili od myšlenky serverhousingu. Nechtěli jsme, aby se nám zde motali cizí lidé. Do serverovny tak mají přístup pouze zaměstnanci WEDOS, k samotným serverům jen oprávněný personál. Vše je navíc monitorováno bezpečnostními kamerami, jejichž obsah se ukládá. Ovšem i tak získání certifikátu ISO 27001 – Bezpečnost dat pro kompletně celý WEDOS nám dalo celkem zabrat. Museli jsme si nechat vypracovat bezpečnostní audit, změnit některá zaběhnutá pravidla a popravdě nejvíce starostí bylo s revizemi naprosto všeho. Každá samostatná

elektronika v budově, ať je to UPSka, monitor anebo prodlužovačka, má svou vlastní kartičku se záznamem, kdo jí používá, kdo je správcem, kdo má oprávnění jí používat. Například někdo má přístup do systému ze své pracovní stanice, ale nemá oprávnění používat tiskárnu, aby nedošlo k úniku informaci. Dále jsou například pevně stanovená pravidla jakou formu musí mít firemní hesla a spousta a spousta dalších věcí.

Závěr

Věříme, že jste se z tohoto reklamního článku dozvěděli něco zajímavého. Na BusinessIT.cz už stejně všichni z vás vědí, že jsme největším provozovatelem webhostingu v České Republice, se super nadupanými ekologickými stroji Fujitsu, značkovými routery, ve vlastním datacentru, které je připojené třemi trasami o rychlosti 10 Gb/s navíc se serverovnou v protiletecké krytu civilní obrany. Takže tentokrát místo reklamy jsme se rozhodli se s vámi podělit o pár zkušeností.
A abychom nezapomněli. Máme pro vás slevový

kupón SAFETYFIRST (SLEVA 33%) s platností do 31. května 2013. Platí pro nově registrované webhostingy a VPS.
WEDOS.cz »
(Tato kapitola je partnerským příspěvkem.)

Autentizace uživatelů prostřednictvím mozkových vln

Autentizace uživatelů je dlouhodobým problémem, který se dnes stále ještě nejčastěji řeší prostřednictvím přístupových hesel. Je sice zřejmé, že jde o řešení nepohodlné, žádná z alternativ jej ale zatím - z různých důvodů - nebyla schopna nahradit. Nejen pro autentizaci uživatelů při přístupu k mobilním zařízením - mobilním telefonům, tabletům apod. - by v budoucnu mohla sloužit technologie rozpoznání uživatele podle jeho mozkových vln. Autoři právě zveřejněné studie hlásí až 99% úspěšnost.
EEG senzory jsou již nějakou dobu běžně dostupné i koncovým uživatelům (jmenujme třeba populární MindWave společnosti NeuroSky - zde je test od

naší sesterské redakce), nicméně jejich masové použití zatím směřovalo spíše do oblasti zábavy. Autoři studie I Think, Therefore I Am: Usability and Security of Authentication Using Brainwaves z univerzity v Berkeley ale zaměřují svou pozornost jiným směrem - na využití podobných zařízení k autentizaci uživatelů.

Podle jejich závěrů se při integraci EEG senzorů do mobilních zařízení stane autentizace využívající mozkových vln uživatele zcela reálnou alternativou stávajících řešení. Autoři studie podle svých slov otestovali využitelnost běžných EEG senzorů určených pro spotřebitelský trh k uvedenému účelu a zjistili, že jsou u jednokanálových EEG systémů (tedy systémů s jedním EEG čidlem, suché provedení, tedy bez nutnosti používat vodivý gel) schopni dosáhnout 99% přesnosti autentizace uživatele, což podle nich odpovídá přesnosti dřívějších pokusů s profesionálními vícekanálovými řešeními.

Ke svým testům využívali produkt MindSet od výše zmiňované společnosti Neurosky, tedy běžné zařízení určené koncovým uživatelům. Testovací subjekty pak nechávali provádět nejrůznější mentální

činnosti, aby určili, které z nich se jak projevují na výstupech čtečky EEG, a jak efektivně je lze využít k autentizaci uživatele. Jen pro představu: **Mentální aktivitou vhodnou pro autentizaci uživatele může být třeba tiché prozpěvování si oblíbené hudební skladby. Nebo představování si vybrané pasáže z oblíbené knihy.**

Ačkoli je zřejmě doba, kdy nás přístroje budou rozpoznávat podle naší mozkové aktivity, ještě poměrně daleko, nemusí jít o tak dlouhou dobu, jak bychom si ještě nedávno mysleli. Jednou ze slabin realizovaných pokusů zatím je, že vybranou mentální aktivitu je třeba provozovat relativně dlouho - při ve studii uváděných pokusech šlo o deset sekund, přičemž lze předpokládat i krátkou dobu mentální přípravy. Nicméně jde o jednu z prvních vlaštovek, a tak je třeba se na studii dívat.