

PRŮZKUM SECURITY PARADOX – HLAVNÍ ZJIŠTĚNÍ STUDIE (Výtah z PDF anglického originálu)

Jako *Security Paradox* označuje společnost McAfee jednak svoji studii, jednak skutečnost, že i přes nárůst malwaru a počítačové kriminality většina středních firem dnes snižuje nebo zmrazuje prostředky na zabezpečení IT.

Metodika průzkumu

Studie analyzuje chování firem (nikoliv vládních agentur nebo neziskových organizací) mezi 50 a 1 000 zaměstnanců v USA, Kanadě, Velké Británii, Francii, Španělsku, Německu, Austrálii, Indii a Číně. Vlastní dotazování provedla na objednávku společnost MSI International. Průzkum se realizoval mezi zaměstnanci IT oddělení nebo lidmi, kteří měli vzhledem k IT rozhodovací pravomoci. Z každé země se podařilo získat okolo 100 vyplněných dotazníků.

Hlavní výsledky v číslech

56 % středních firem zaznamenalo letos více bezpečnostních incidentů než loni. Laboratoře McAfee Labs zachytily jen v první polovině letošního roku zhruba stejně nového malwaru jako za celý rok 2008.

29 % středních firem bylo loni postiženo únikem nebo ztrátou dat.

71 % středních firem připouští, že vážné bezpečnostní narušení a ztráta dat by mohly znamenat konec jejich podnikání.

37 % středních firem strávilo 3 nebo více dní řešením následků útoku proti IT systémům.

65 % těchto firem věnuje na proaktivní zabezpečení IT méně než 3 hodiny týdně.

78 % těchto firem se obává, že by se mohly stát cílem kybernetické kriminality.

19 % středních firem postihl incident týkající se bezpečnosti IT, který způsobil přímé finanční ztráty (tj. např. ztráta zakázek v důsledku výpadku služeb). Průměrná výše těchto škod byla 41 000 dolarů.

40 % případů ztráty či úniku dat se týkalo citlivých soukromých informací o zákaznících, zaměstnancích či obchodních partnerech.

75 % středních firem v roce 2009 zmrazilo či snížilo svůj rozpočet na zabezpečení IT.

322 % představuje nárůst počtu kybernetických útoků proti středním firmám (zde data pouze pro USA) za poslední 3 roky.

5 % je podíl středních firem v USA, které vůbec nedokázaly rozhodnout, zda u nich v posledním roce došlo k bezpečnostnímu incidentu.

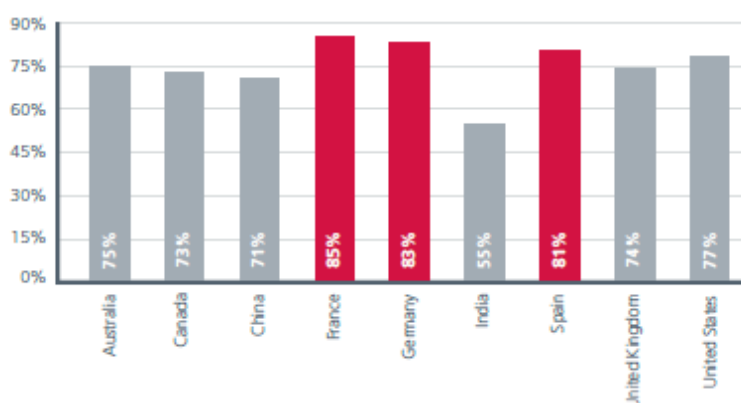
Šetření

75 % firem zúčastněných v průzkumu v letošním roce snížilo nebo zmrazilo rozpočet na zabezpečení IT ve snaze kompenzovat pokles příjmů daný ekonomickou krizí. Netřeba dodávat, že naopak internetoví zločinci v důsledku toho žádnou ekonomickou krizi nepocítují.

Téměř **40 %** z firem, které snižují rozpočty na zabezpečení IT, dosahují úspor omezením investic do nových bezpečnostních produktů. Více než třetina z nich se snaží snížit počet zaměstnanců IT oddělení a stejný podíl přechází na levnější, jednoúčelové (stand-alone) produkty – které však v porovnání s komplexními systémy a službami poskytují nižší úroveň zabezpečení.

Je to paradoxní – ačkoliv téměř všechny firmy uznávají nárůst hrozeb, nepřizpůsobují tomu vynaložené prostředky.

Podíl středních firem, které letos zmrazily nebo snížily prostředky na zabezpečení IT



Velké a malé firmy

Výsledky studie *Security Paradox* ukazují, že kybernetickými útoky jsou dnes zranitelné a ohrožené především firmy mezi 100 a 500 zaměstnanci. Mnoho IT manažerů v těchto firmách se ovšem chybně domnívá, že na rozdíl od velkých firem nejsou jako cíl pro útočníky tak zajímaví. Z toho důvodu soudí, že úroveň zabezpečení odpovídá velikosti jejich společnosti a další investice by již nebyly účelné („overbuilding“). Není to ale pravda. Pokud se zaměříme pouze na firmy, které utrpěly bezpečnostní průnik, pak firmy mezi 101 a 500 zaměstnanci zaznamenaly v posledních 3 letech v průměru 24 bezpečnostních incidentů. U firem s 500 až 1 000 zaměstnanců bylo odpovídající číslo 15 incidentů.

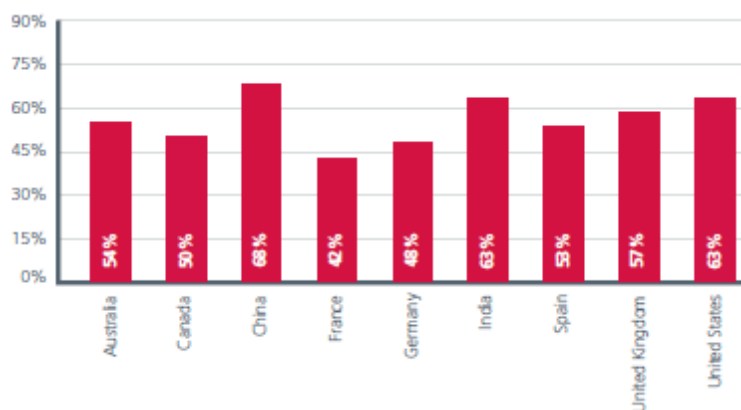
Kybernetičtí zločinci si uvědomují, že velké firmy mají obvykle nejen odolnější systémy, které dokáží útoku vzdorovat, ale také lepší prostředky k identifikaci útočníků a následnému zahájení právních kroků. Útok proti středním firmám s sebou pro útočníky nese mnohem menší riziko.

Malé a střední firmy na rozdíl do těch velkých také nemají podrobně zpracované (nebo dokonce vůbec připravené) plány pro případ bezpečnostních incidentů ani systémy pro řízení rizik. Hrozí jim, že je útok zcela paralyzuje a může znamenat i konec jejich podnikání – zejména v případě, že SMB firma funguje jako partner velké firmy, která v důsledku incidentu (a např. nesplnění termínu) odstoupí od kontraktu.

Geografické srovnání

Graf ukazuje, že největší nárůst hrozeb letos zaznamenaly firmy v USA, Indii a Číně. Není jasné, nakolik jsou útoky proti středně velkým firmám vedeny ze zahraničí. Kybernetickou špionáží v jednotlivých zemích se podrobně zabývala studie *Virtual Criminology Report*, kterou společnost McAfee vydala v loňském roce.

Nárůst hrozeb mezi lety v roce 2008 a 2009



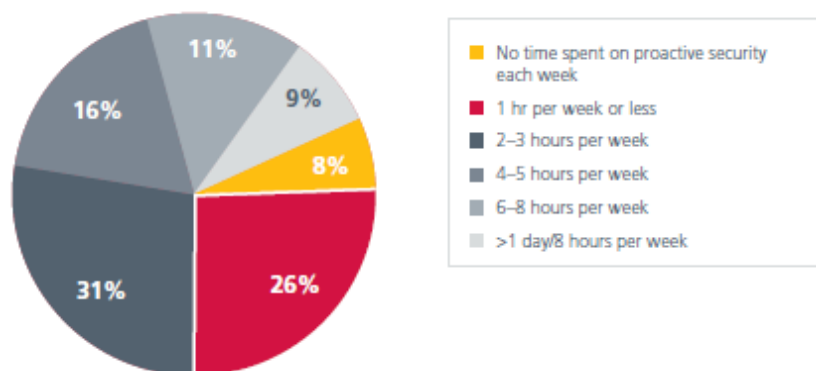
Proaktivní vs. reaktivní přístup

Společnost McAfee ve své studii *Unsecured Economies* (Nebezpečné ekonomiky) odhadla, že ztráty firem v důsledku kybernetické kriminality a úniků duševního vlastnictví přesáhly v loňském roce celosvětově částku 1 bilionu dolarů. Pouze v USA vynaložily loni střední firmy na řešení následků kybernetické kriminality asi 17,2 miliard dolarů. Odborníci z laboratoří McAfee Labs mají veškeré důvody k přesvědčení, že v letošním roce tato částka ještě vzroste.

Firmy zúčastněné v průzkumu mnohdy plně nechápou, že proaktivní (preventivní) investice do zabezpečení vyjde mnohem levněji než řešit až následky útoků proti IT systémům. Graf ukazuje, že 8 % dotazovaných firem nevěnuje proaktivnímu zabezpečení vůbec žádný čas, 26 % méně než hodinu týdně, 31 % 2–3 hodiny týdně (celkem tedy téměř 2/3 firem věnují bezpečnosti IT méně než 3 hodiny týdně). Poměr prostředků vynaložených na prevenci v porovnání s náklady na řešení incidentů se liší regionálně, zvláště znepokojivý je ve Francii a v Číně.

Průzkum přitom ukazuje jednoznačný vztah mezi tím, kolik času se věnuje na proaktivní zabezpečení, a časem potřebným na obnovu systémů po incidentu. 60 % středních amerických firem věnuje prevenci více než 4 hodiny týdně a 40 % těchto firem pak zvládne zotavení po incidentu za méně než 1 den.

Čas věnovaný na proaktivní zabezpečení



Změněná povaha hrozeb

Již během ekonomické recese v letech 2001–2002 se ukázalo, že kybernetická kriminalita nejen vzrostla, ale také se změnila její povaha. Útočníci vyvíjeli sofistikovanější prostředky, snažili se své aktivity „standardizovat“. V době nejistoty měli navíc větší šanci získat pomoc vnitřních nepřátel (insiderů) a podplácet nespokojené zaměstnance či lidi, jimž hrozilo propuštění. Spojení ekonomické krize a hrozby ze strany vnitřních nepřátel dokládá celá řada studií.

V současnosti mohou útočníci s výhodou využívat obrovského nárůstu obsahu informací na Internetu i růstu interaktivity, který přišel s aplikacemi Web 2.0/sociálními sítěmi. Tato situace výrazně usnadňuje použití metod sociálního inženýrství.

Lidé obávající se o další pracovní kariéru tráví dnes hodně času na webech jako LinkedIn (služba pro sdílení pracovních kontaktů). Marketing se v čase snižujících se rozpočtů snaží používat Facebook. Všechny tyto weby jsou přitom plné odkazů na podvodné servery shromažďující například informace o platebních kartách nebo pokoušející se instalovat do počítačů neopatrných uživatelů malware.

Spam není žádnou novinkou, ale nová je míra škod, kterou firmám působí. Dnes má povahu nevyžádané pošty 92 % všech e-mailů a spammeři rozešlou každý den 117 miliard zpráv. Rovněž phishing a další podvody tohoto typu představují stále výnosný byznys.

Povzbudivé nicméně je, že střední firmy si tyto hrozby stále více uvědomují. Meziročně poklesl podíl firem, které si vůbec nebyly jisté, zda u nich došlo k bezpečnostnímu incidentu (pro americké střední firmy z loňských 15 % na letošních 5 %). K řešení

problémů je samozřejmě nutné je v první řadě vůbec dokázat zaznamenat. Firmy dnes obecně stále ve větší míře investují také do systémů pro správu zranitelností.

Střední firmy obvykle věnují na boj s různými hrozbami přibližně stejné prostředky. To na první pohled nepůsobí logicky, protože incidenty různých typů se nevyskytují stejně často – nicméně zase mohou mít vážnější následky. Největším vektorem hrozeb je e-mail, nicméně zotavení po tomto útoku bývá relativně levné, opak platí pro incidenty spojenými se ztrátou/únikem dat.

Jak minimalizovat riziko

Firmy, které chtějí minimalizovat rizika související se zabezpečením IT, by si měly osvojit přístup zahrnující následující opatření:

- Zabezpečení, respektive vrstva ochrany, musí být integrovaná a procházet napříč jednotlivými sítěmi a systémy.
- Hrozby je třeba analyzovat v reálném čase, vhodné je nasazení reputační analýzy.
- Různé systémy zabezpečení a různá prostředí podnikových aplikací by měly být centrálně spravovatelné prostřednictvím jediné integrované platformy a jediné konzole.

I v situaci, kdy firma vyžaduje snižování nákladů na zabezpečení IT, je možné zvolit efektivní postup. K dosažení tohoto cíle existuje soubor doporučených opatření (best practises), která šetří jak náklady na vlastní bezpečnostní řešení a jeho provoz, tak i předchází ztrátám a rizikům v důsledku narušení zabezpečení. K hlavním doporučením podle společnosti McAfee patří:

- Důraz na proaktivní přístup a identifikaci potenciálních rizik.
- Integrace: dávat přednost dodavatelům, kteří poskytují komplexní sady zabezpečení, konsolidovat množství nasazených bezpečnostních produktů.
- Bezpečnostní řešení by mělo zahrnovat všechny vektory, jimiž se šíří malware: ochranu systémů, e-mailu, přístupu k webu, řízení přístupu k síti, ochranu proti vniknutí i ochranu dat na veškerých zařízeních.
- Centrální správa pomocí jediné konzole umožňuje lepší přehled nad celým prostředím a jeho snazší řízení.
- Integrovaná řešení bývají v konečném důsledku levnější, protože se při nich obvykle ušetří na licencích, podpoře dodavatele i nákladech na správu.
- Lze doporučit nasazovat řešení, která mají zabudované mechanismy automatické aktualizace.

Za těchto okolností lze dosáhnout vyšší míry bezpečnosti bez toho, aby to administrátory stálo více úsilí a vynaloženého času. Společnost McAfee například nabízí sadu doporučení „Secure in 15“, která umožňuje realizovat správu zabezpečení malých a středních firem tak, aby vyžadovala pouze 15 minut denně.