rozhovor

Ubránit útokům se dokáže i malá firma

Na náš rozhovor přiletěl z Hradce Králové do Prahy pětimístným letadlem Socata TB20 v barvách firmy. Jako by to podtrhovalo fakt, že v oblasti bezpečnosti IT jde mnohdy o hodiny či dokonce minuty. Což může být oříšek pro malé a střední firmy, na něž se právě GFI Česká republika a Slovensko primárně zaměřuje. Naštěstí i tyto firmy se dnes podle Martina Říhy, jejího ředitele pro strategii, mohou proti útokům na své systémy a data účinně bránit.

Foto: Ondřej Petrlík

Věnujete se dnes řadě oblastí, které převážně souvisejí s bezpečností IT. Co tvoří jádro vašeho byznysu a jaký podíl mají jednotlivé oblasti?
Zastřešujeme celé portfolio společnosti GFI Software. Začínali jsme s jejím faxovým serverem, prvním, který měl dořešenou integraci se serverem Exchange. Dnes tvoří jádro nabídky bezpečnostní řešení. Velmi úspěšným produktem byl serverový antispam GFI MailEssentials, který přišel v době začátku masového šíření spamu.

V oblasti bezpečnosti byl topproduktem GFI LanGuard, ten je dodnes v IT pojmem na poli bezpečnostních skenerů, správy záplat atd. Z dalších nástrojů mohu zmínit produkty pro analýzu bezpečnostních logů napříč firemní síťovou infrastrukturou. Nabízíme tak ucelené portfolio nástrojů pro komunikaci a bezpečnost, přičemž se soustředíme na prostředí Microsoftu, které je ve firmách ze segmentu SMB dominantní.

Jaké trendy jsou dnes podle vás určující z hlediska potenciálních bezpečnostních hrozeb?
Vektor útoku dlouhá léta sledujeme, neustále se vyvíjí. Většina firem již využívá poměrně kvalitní antiviry, které jsou schopny zabránit většině útoků šířeným například e-maily. Ve světě Windows se povedlo účinně odstranit většinu rizik souvisejících se zranitelnostmi operačních systémů a aplikací Microsoftu.

Jako největší hrozbu v současné době vidíme útok, který je veden přes chyby a zranitelnosti v aplikacích třetích stran, jako jsou Flash, Java, internetové prohlížeče atd. Útoky vždy směřují tam, kde je možné cílit na co největší skupinu uživatelů. Proto budou v nejbližší době směřovat na platformu, která se momentálně překotně vyvíjí – a tou jsou podle naší studie momentálně zejména chytré telefony a tablety se systémem Android, počet těchto zařízení letos celosvětově přesáhne počet instalovaných PC. Přitom např. po převzetí kontroly nad vaším smartphonem může útočník získat třeba přístup k vašemu internetovému bankovnictví.

Setkal jste se s tím, že by české firmy byly vystaveny finančně motivovaným útokům?
Jen několik týdnů zpět se potvrdilo, že doména kyberterorismu není něčím z říše sci-fi. Například škodlivý kód CryptoLocker je důkazem toho, že útočníci mají ze svých činů reálný prospěch. Jde doslova o hijacking – únos – vašich dat tím, že dojde k jejich zašifrování, a následně vyžadování výkupného. V rámci GFI máme reporty reálných případů nejen z Evropy, ale i přímo z Čech, kde bylo zaznamenáno minimálně pět případů firem, které byly tímto kódem napadeny, podstoupily celý proces a ačkoliv se říká, že s teroristy se nevyjednává, zaplatily výkupné a data dostaly zpět. To je důkazem toho, že to funguje a finanční motivace pro tento typ konání rychlým tempem poroste.

Nedávná studie GFI potvrdila, že situace v českých firmách např. ohledně záplatování softwaru není zcela růžová. Jak vidíte současnou situaci z hlediska zájmu malých a středních firem bezpečnost řešit? Jak velký problém to je?
Ten problém je větší se zmenšující se velikostí firmy, je to obrácená přímá úměra. Čím menší firma, tím méně času, aby se někdo věnoval bezpečnosti. Je potřeba se na to podívat s určitým odstupem. Řada firem je dnes v režimu, dá se říci, až bojovém. Spousta jich bojuje doslova o holý život. A pokud bojujete – ať už do vás tne konkurence nebo Česká národní banka kurzem měny –, bezpečnostní rizika v IT se ocitají na vedlejší koleji, nemají prioritu.

Bojujete s dennodenními potížemi, které vás ohrožují daleko víc a nejsou to jen potenciální rizika či hrozby – firmy čelí problémům, které se právě skutečně odehrávají.

Pokud přece jen menší či střední firma má vůli se bezpečností zabývat, co je podle vás nezbytné minimum?
Nemyslím si, že by bylo třeba i pro malou firmu složité dosáhnout žádoucí úrovně bezpečnosti tak, aby ji to nestálo příliš mnoho peněz nebo úsilí. Důležité je rozhodnutí ji řešit. Alespoň minimální profylaxi pro zajištění počítačové bezpečnosti by měla mít každá firma. Stačí zvolit alespoň základní nástroje, tedy antivirus a správu bezpečnostních záplat, a k tomu pravidelně školit uživatele, ukázat jim, jakým způsobem se chovat, aby omezili vysloveně rizikové jednání. Už tato kombinace je pro malou firmu vším, co potřebuje. Právě tady mohou pomoci on-line nástroje, které zajistí např. správu záplat z cloudu za přijatelný měsíční poplatek.

Vaše produktové portfolio dnes zahrnuje i on-line či cloudová řešení v různých formách…
S tím, jak se začal vyvíjet a měnit styl využívání výpočetní techniky a přišla úplně nová zařízení, jako jsou tablety, smartphony atd., jsme na tyto trendy zareagovali a postupně začali přicházet s celou řadou on-line řešení s tím, jak se v posledních letech vize cloud computingu začaly měnit v realitu. Naše první cloudové řešení, GFI Max Remote Management, jsme spustili v roce 2009. Od té doby máme v Čechách instalovanou bázi zhruba 2 000 serverů a 10 tisíc stanic, které její řešení využívají. Je tedy vidět, že to není záležitost pro pár zapálených jedinců-průkopníků.

Prostřednictvím řešení GFI Max, jež agreguje množství služeb od řízeného antiviru a managementu záplat přes skenování sítě až po síťový a softwarový audit atd., naši prodejci a partneři poskytují řízené bezpečnostní služby svým koncovým zákazníkům. V rámci nich kompletně zajišťují proaktivní správu zabezpečení IT pro malé, střední i větší firmy. Hodně často jsou řízené služby výhodné pro malé firmy, které provozují nejen několik počítačů, využívají MS Office 365, poštu, kalendáře i dokumenty mají v cloudu a kromě malého úložiště NAS ani nemají server. Poskytovatel se v rámci řízené služby o jejich zabezpečení za měsíční poplatek postará se vším všudy.

Letos v srpnu jsme spustili také službu GFI Cloud, která je naopak vytvořena pro firmy, které nechtějí bezpečnostní řešení instalovat a provozovat on-site, ale správu si chtějí ponechat ve vlastních rukou. Mají vlastní IT personál, takže si samy volí, které bezpečnostní nástroje budou využívat a službu si řídí samy. Nemusejí se však starat o provoz a údržbu samotné infrastruktury.

Jaký dnes mají jednotlivé formy doručování tohoto softwaru na vašich výsledcích podíl?
V minulosti byla lokální instalace vlastně jediným mainstreamovým způsobem, jakým používat software, proto do dneška největší instalovaná báze spočívá v on-site produktech. Pokud se však podíváme na prodeje nových licencí, tak zde dnes už jasně vede cloud.

Tradiční produkty prodáváme i nadále, zde se nám podařilo nasytit trh. Noví, ale často i stávající zákazníci často konvertují k on-line verzím těchto produktů, do cloudu. A bylo i naší vizí, abychom jim umožnili určitý hybridní přístup, a to tím, že máme prakticky tentýž produkt ve verzi on-site i on-line. Umožňujeme tak zákazníkům, aby si stanovili oka- ▶

mžik, který je pro ně nejvhodnější pro přechod z on-site řešení na on-line – například s ukončením životnosti jejich stávající hardwarové infrastruktury.

To naznačuje, v čem je hlavní výhoda tohoto řešení...
Je to jednoduché – namísto toho, aby kupovali nový server, převedou řešení do on-line režimu, takže ušetří za pořízení hardwarové techniky. Ale nejen to, roli zde hrají například i úspory za podkladové licence Microsoftu a zanedbatelná dnes není ani úspora elektrické energie. To jsme pro zákazníky několikrát počítali a v běžné firmě, která nenakupuje elektřinu ve velkoobchodním režimu, malý server spotřebuje v přepočtu na finance jednou tolik energie, kolik je jeho cena. To se výrazně odráží na TCO serveru. Započtěte náklady na chlazení a klimatizaci a při kalkulacích často opomíjenou cenu za to, že se o tuto infrastrukturu musí někdo starat, spravovat ji a aktualizovat. A to vše jsou faktory, které pokud si spočítáte, činí cloud pro mnoho firem zajímavějším.

Pokud bychom se ale chtěli přece jen zastat tradičního pojetí IT a bezpečnosti, komu se on-site provoz vyplatí?
Některé společnosti potřebují provoz části infrastruktury doma z toho důvodu, že jde o specifické, oborově úzce zaměřené či přímo zákaznické aplikace. Je možné, že v rámci této infrastruktury zbývá určitá kapacita, ať už lidských zdrojů, tak hardwaru a základního softwaru, kterou lze využít na provoz dalších softwarových řešení, tedy např. pro zabezpečení. Jsou proto samozřejmě případy, kdy se firmám a obzvláště těm větším dodnes vyplatí provozovat aplikace vnitrofiremně. Netvrdím však, že je přechod do cloudu nějaké dogma.

V případě cloud computingu se obecně stále mluví o určité nedůvěře a konzervatismu ze strany zákazníků, setkáváte se s ním také?
My fungujeme striktně přes prodejní kanál. A tady historicky vždy platilo a platí, že koncoví zákazníci, ať už využívají software instalovaný on-site nebo řízenou službu poskytovanou on-line, v první řadě věří svému prodejci. Pro zákazníka je důvěra v dané řešení založena na důvěře vůči svému prodejci či poskytovateli služby – pokud je pro něj navrhovaná on-line služba také finančně výhodná. Na úspory slyší firmy vždy. Samotný GFI Cloud jsme spustili teprve nedávno a firmy i nadále vkládají důvěru v IT specialisty ve své lokalitě, které mají nablízku a kterým věří.

Velkým trendem je používání vlastních mobilních zařízení ve firemním prostředí, tzv. BYOD. Jak se toto odráží v praxi v oblasti bezpečnosti? Jak na ni reagují české firmy?
Ještě před pár lety se to týkalo pouze majitelů firem a několika nejvyšších manažerů, ale dnes má smartphone nebo tablet prakticky každý. Jde o soukromá zařízení zaměstnanců, která se aktivně připojují různými kanály do sítě, stahují si e-maily, přistupují k datům. V principu využívání těchto mobilních zařízení usnadňuje práci, to je pravda, pouze není dobré, když firma nemá jakoukoliv kontrolu nad tím, k jakým datům takto mohou pracovníci přistupovat. Zájem o takové řešení je opravdu obrovský a my jej postupně reflektujeme.

Martin Říha (40) založil v roce 1997 se svým kolegou společnost PB Com orientující se na dodávku IT produktů a služeb. Od roku 2001 spolupracuje se společností GFI Software v oblasti výhradní distribuce pro ČR a SR na pozici ředitele pro strategii. Ve volném čase se věnuje létání a renovování vysloužilých motorových vozidel. Martin Říha žije v Hradci Králové, je ženatý a má tři děti.

Jednou z vašich prvních reakcí byla akvizice britské společnosti Visual Mobile, která se zabývala vývojem softwaru pro správu mobilních zařízení především na platformách Android a iOS. Co bude dál?
V současnosti tento software postupně integrujeme do našeho řešení GFI Max. Cílem je poskytnout možnosti reportovat o dění v síti, na dálku řídit přístup do ní a zajišťovat provisioning tak, aby u zařízení, jemuž je povolen přístup do sítě, byla správně nastavena pošta, antivirus, hesla atd.

Nabídne ale např. i vzdálené smazání dat, likvidaci profilu a vypnutí, aby nedošlo ke zneužití zcizeného zařízení, nebo geofencing pro kontrolu pohybu zaměstnanců, ať už z důvodu sledování produktivity, nebo pro omezení služeb podle toho, kde se nachází a přes jakou síť se k firemním systémům a datům připojuje – zda přes firemní, či veřejnou.

Nedávnou akvizicí jste vstoupili také do oblasti on-line zálohování dat...
On-line zálohování patří k nejžádanějším on-line službám a ne náhodou se jím v současnosti zabývá řada firem. My se díky akvizici holandské společnosti IASO pokoušíme nabídnout unikátní vlastnosti, díky nimž se proces denního zálohování podstatně urychluje. Zatímco objemy záloh jsou čím dál tím větší, díky naší technologii jsou přenosy dat minimální, což hraje velkou roli mj. při horší konektivitě.

Jak to zapadá do vaší filozofie?
On-line zálohování velmi dobře doplňuje naše bezpečnostní portfolio. Řada firem zálohování ve vzdálené lokalitě podceňuje. Ovšem pokud máte zálohu veškerých dat, která je šifrována a uložena v geograficky vzdálené lokalitě, můžete nejen snadno obnovit svá data po havárii či povodni, ale navíc máte také prostředek jak se bránit například při útoku škodlivého kódu, jakým je CryptoLocker. Pokud takový kód zablokuje data napříč celou firmou, máte svá data odkud obnovit a můžete se tak ubránit a nemusíte se stát obětí kyberterorismu. ■

Petr Velecký