BEZPEČNOST – PLAVBA NEKLIDNÝMI VODAMI

foto: Freelmages

ČLÁNEK PŘIPRAVIL DAVID ČAPEK

Těžko bychom dnes hledali velkou firmu či organizaci, která nemá své informační systémy a data poměrně uspokojivě zabezpečené. Doba pokročila a snad již naprostá většina vedoucích pracovníků chápe, že promyšlené investice do bezpečnosti – byť jejich přínos ani návratnost nejsou jednoduše vyčíslitelné – obvykle neznamenají vyhozené peníze. Je tudíž nezbytné tuto oblast řešit komplexně a jasně definovat podnikovou bezpečnostní politiku. Poněkud odlišná je však situace u středních a malých firem, kde je kvalitní zabezpečení dosud nezřídka zanedbáváno. Zvlášť když se v současnosti „šetří, kde může".

Doba přinesla i hospodářskou recesi a snahu (lépe řečeno nutnost) uspořit v daném okamžiku zbytné náklady. Jak zajistit, aby firmy i přes pochopitelné omezování výdajů – včetně těch na bezpečnost – nebyly výrazným způsobem ohroženy? A přinášejí rozbouřené vlny dnešní ekonomické situace zbrusu nová, dosud nepoznaná bezpečnostní rizika?

Přejděme rovnou k odpovědím na obě otázky. Asi nepřekvapíme konstatováním, že úroveň zabezpečení a s ní spojené nezbytné výdaje by neměly klesnout pod určitou kritickou mez. Tato úroveň může být v každé firmě stanovena různě, důležité je „nastavit" ji po zvážení řady aspektů (mj. právě finančních) přesně a nekompromisně.

Troufáme si rovněž tvrdit, že zcela nové hrozby se neobjevily, spíše některé již existující vlivem okolností nabyly na intenzitě…

Ohrožení nepřinášejí zdaleka jen počítačové viry

Nebezpečí je dnešním IT světě opravdu mnoho a jakýmsi tahounem je v tomto směru nepochybně internet. Asi každý dostává nevyžádanou elektronickou poštu s nabídkami preparátů, jež zaručeně přispějí k dlouhověkosti či úžasné sexuální výkonnosti. V poslední době se vlivem krize – ve skutečnosti jde do značné míry o zneužití nelehké situace řady jedinců i firem – stále více objevují také e-maily nabízející pracovní příležitosti, možnost rekvalifikace či investic do rozličných komodit s okamžitým ziskem.

Jistě ne všechny tyto zprávy jsou vyloženě podvodné, ale značné procento z nich ano. Metody sociálního inženýrství, mj. jak „vytáhnout" z uživatele číslo a PIN jeho kreditní karty nebo přihlašovací údaje do internetového bankovnictví, se stále zdokonalují. „Skutečné hrozby – neošetřené zranitelnosti, škodlivé kódy, přímé útoky – mají co do absolutního počtu stále rostoucí tendenci. V roce 2007 jsme například vytvořili celkem 800 000 konkrétních signatur pro detekci zranitelností, v roce 2008 to bylo 1 700 000 a v tomto roce trend nadále pokračuje," vypočítává Jakub Jiříček, senior principal presales consultant společnosti **Symantec**.

Propouštění a frustrace zaměstnanců znamenají bezpečnostní riziko

Z řady průzkumů již celá léta opakovaně vyplývá, že hlavní bezpečnostní rizika nepřicházejí „zvenku", ale ve většině případů se „nepřítel nachází uvnitř". Ano, řeč je o lidském faktoru, který nezřídka tvoří onen nejslabší článek pomyslného řetězu. Nemusí jít vždy o zlý či zištný úmysl, ale například o nerespektování bezpečnostních předpisů, jejich neznalost, naivitu, snahu zjednodušit si život (např. nechat na monitoru počítače přilepený lísteček s přihlašovacím jménem a heslem). Avšak v době, kdy podniky zažívají pokles tržeb a mnoha zaměstnancům hrozí propuštění z pracovního poměru, vzrůstají právě rizika spojená s úmyslným poškozením zaměstnavatele, zneužitím citlivých dat nebo zcizením firemního know-how.

„Zvýšená fluktuace, zapříčiněná snižováním stavu zaměstnanců v důsledku ekonomické recese, s sebou nese riziko, že ohrožení zaměstnanci mohou shromažďovat takové materiály a data, které by jim pomohly k upevnění vlastní pozice ve firmě, případně jako vstupenka do firmy konkurenční," vysvětluje Karel Zeman, ředitel a člen představenstva společnosti **M-LINE**. „Může se jednat zejména o projektovou dokumentaci, smlouvy s dodavateli a odběrateli, interní směrnice a další zdroje, které firma eviduje v elektronické podobě." Někdy jde vyloženě o pomstu propuštěného pracovníka, který se cítí být zrazen či odkopnut a reaguje iracionálním způsobem.

Karel Schmidtmayer, country manager firmy **CA** v České republice, upozorňuje v podobném duchu: „U společností, které nejsou po stránce IT bezpečnosti připraveny na rozsáhlá propouštění, se významným způsobem zvyšuje riziko zneužívání dat. Pokud zaměstnance propouštíte a nemáte pro to na jedné straně dobře připravený proces a mechanismy propouštění tak, abyste zabránili zneužívání dat, a na straně druhé nedisponujete určitou aplikační nebo jinou platformou, která reálně znemožňuje zaměstnanci nadále

fakta

EDI

komunikace je bezpečná jen tehdy, když jsou využity solidní bezpečnostní kanály, resp. bezpečné protokoly pro přenos po internetu.

Rizika

podle zkušeností odborníků vyvstávají zejména v souvislosti s neodborným nebo nezodpovědným jednáním vlastních zaměstnanců.

s těmito daty nakládat, jednoznačně se vystavujete riziku."

Jde o fenomén základní ochrany dat – aby organizace byla v ideálním případě schopna takovému případu zabránit, a to procesními i technicko-aplikačními opatřeními, jako je řízení přístupu zaměstnanců k síti a informacím, jež se v ní nacházejí. A není-li tato prevence dostatečná, dokázat podobný čin odhalit a následně vést příslušné řízení – interní nebo externí, případně i soudní apod. „Účinnou obranou je standardizace procesů firmy ohledně poskytování zdrojů vlastním zaměstnancům, pečlivé a důsledné rozdělení jednotlivých rolí zaměstnanců a zvážení, zda poskytnutá privilegia nejsou pro daný okruh zaměstnanců příliš obecná. Firemní pravidla a procesy nestačí pouze definovat. Nutné je zejména provádět pravidelnou kontrolu jejich dodržování a uplatňování," potvrzuje Karel Zeman. Tedy nikoli „Velký bratr tě sleduje", ale důsledný požadavek na respektování určitých pravidel ve společném zájmu.

Podstatné jsou nejen technologie, ale i procesy, testy a audity

Stále diskutovanou otázkou, zvlášť v oblasti logistiky a dodavatelsko-odběratelských vztahů, jsou možnosti EDI komunikace a úroveň jejího zabezpečení. Připomeňme, že EDI je automatický přenos a zpracování elektronických dokladů ve formě strukturovaných zpráv, které jsou standardizovány obsahově, významově i z hlediska formátu. „Na trhu jsou zcela jistě technologie, které mohou zajistit naprosto postačující úroveň zabezpečení EDI i ochranu samotných dat. Konkrétní implementace je na rozhodnutí každého provozovatele, kolik se rozhodne investovat, jaké konkrétní technologie, jejich kombinace a jaké procesy zvolí," popisuje Jakub Jiříček.

EDI komunikace může probíhat buď prostřednictvím třetí strany, tzv. VAN operátora, skrze jeho systémy a komunikační rozhraní, anebo přímo mezi dvěma podniky. V prvním případě je bezpečný přenos dat garantován a jakákoli rizika minimalizována, v případě druhém je dostatečnému zabezpečení nutno věnovat větší pozornost. K tomu slouží různé protokoly a standardy. Jakub Jiříček to doplňuje: „Je více než vhodné dodržovat doporučené postupy na průběžné exaktní ověření spolehlivosti systémů, namátkové bezpečnostní testy, audity bezpečnosti a podobně." I zde tedy platí, že bezpečnost nespočívá jen ve zvolených technologiích.

Vše je relativní, i zabezpečení dat a IS

Ochranu před hrozbami – ať už vnitřními či vnějšími – svým způsobem komplikuje překotný technologický rozvoj, kupříkladu masové rozšíření mobilních zařízení využívaných stále častěji pro práci z domova či v terénu, tedy pro vzdálený přístup k firemním informačním systémům, datům a dokumentům. Hranice podnikové sítě jsou nyní nepříliš zřetelné. Na druhou stranu zamezit pracovníkům v přístupu na internet, který je kromě jiného i důležitým pracovním nástrojem a zdrojem informací, je zpozdilé. To vše klade nemalé nároky na administrátory a správce sítí, ale i na propracovanost firemní bezpečnostní politiky. Na tomto místě musíme opět upozornit na důležitost kvalitní správy přístupu k síti – aby se do ní dostal jen ten, kdo má (nikoli osoby „nepovolané"), tam, kam má (přístupová práva jednotlivých zaměstnanců se přirozeně liší), a pouze přes autorizovaná zařízení (např. jen firemní notebooky, ne soukromé).

Z dalších podstatných bezpečnostních zásad, jež by firmy měly dodržovat, a prostředků k tomu určených uveďme nasazení účinného firewallu, filtrování obsahu, kvalitní antivirový systém a v neposlední řadě i šifrování a zálohování dat. Například při krádeži nebo ztrátě notebooku (a jen na letištích po celém světě jich každoročně zmizí mnoho tisíc) se díky šifrování dat nepovolaná osoba nedostane k informacím, které by dokázala „přečíst", naopak díky pravidelnému zálohování jsou i data z odcizeného zařízení autorizované osobě přístupná. Ztráta notebooku či jakéhokoli jiného přístroje je jistě nepříjemná, znamená ekonomickou ztrátu, ale podle řady průzkumů mají nesrovnatelně vyšší hodnotu právě data uložená v těchto zařízeních.

V dnešní době neexistuje firma, která by se mohla uzavřít před světem, odstřihnout od internetu nebo spolupráce s ostatními organizacemi. Ochrana před hrozbami má nesmírnou důležitost, nelze si však myslet, že je možné ubránit se vždy a všemu. Mnohdy je podstatnější, když už k nějakému bezpečnostnímu incidentu dojde, minimalizovat jeho dopady na fungování podniku, realizaci zakázek či vztahy s klienty i obchodními partnery. A tak jde nejen o zdárné proplutí rozbouřenými vodami, ale i o plavbu mezi Skyllou přísných a omezujících bezpečnostních předpisů, které mohou zaměstnancům i celé firmě doslova brát vítr z plachet, např. snižovat efektivitu práce, a Charybdou podnikové bezpečnosti opomíjené, podceňované a nedostatečné. Asi netřeba zdůrazňovat, že obě krajnosti jsou nežádoucí a pravděpodobnost ztroskotání o to reálnější.

odborník

„Pro bezpečnost EDI komunikace jsou klíčové přenosové kanály"

„Z pohledu bezpečnostních rizik pro podnikové IT je nutné zaměřit se na přenosové kanály, které jsou pro EDI komunikaci využívány. V případě využití služeb VAN provideru (specializované firmy na zajištění EDI komunikace mezi obchodními partnery) jsou rizika související s bezpečností IT minimální. V případě přímé komunikace mezi obchodními partnery je potřeba věnovat problematice zabezpečení více úsilí. V současné době existují protokoly, které umožňují zajištění dostačující míry zabezpečení přenosu elektronických dokladů přímo, tj. po internetu. Příkladem takového protokolu může být AS2 (Applicability statement 2), který vyhovuje potřebám zabezpečení přímé EDI komunikace podle mezinárodních multioborových norem EANCOM nebo GS1 XML."

Daniel Lopour
product manager GS1 eCom
GS1 EPCglobal

souvislosti

Malé a střední firmy bezpečnostní rizika znají, ale dostatečně se jim nevěnují

Společnost Symantec provedla v prvním čtvrtletí letošního roku průzkum mezi 1425 malými a středními podniky (SMB) v sedmnácti zemích celého světa. Ukázalo se, že malé a střední podniky sice chápou bezpečnostní rizika, kterým jsou vystaveny, překvapivě velký počet z nich však základní bezpečnostní opatření zanedbává. Například téměř tři pětiny (konkrétně 59 %) těchto firem dosud nezavedly ochranu koncových bodů (software, který chrání před škodlivým kódem „koncové body", jako jsou přenosné počítače, stolní počítače a servery); 42 % malých a středních podniků pak nemá řešení ochrany před nevyžádanou poštou. Téměř polovina nezálohuje stolní počítače, takže jejich důležité informace jsou ohroženy. A konečně třetina podniků nepoužívá ani tu nejzákladnější ochranu – antivirový program.

Zdroj: Symantec Corporation