OVOR

LAV DVOŘÁK,
CKÝ ŘEDITEL, ESET

Jaké jsou aktuální hrozby pro firemní IT?

Lidé, kteří dnes stojí na pomyslné druhé straně barikády, už nejsou jednotlivci, ale dobře organizované skupiny motivované penězi a hladem po důvěrných informacích, říká Miroslav Dvořák, technický ředitel společnosti Eset.

Jak odpovědně se stavějí firmy k otázce IT bezpečnosti?
Obecně můžeme říci, že odpovědněji přistupují větší společnosti, které si uvědomují, co mohou ztratit, a znají cenu svých dat. Menší a střední firmy jsou z našeho pohledu podstatně méně zabezpečené. Paradoxně to ale neznamená riziko pouze pro ně, ale i pro ostatní uživatele. Na neprofesionálně vytvořených stránkách se mohou nejčastěji vyskytovat zranitelné skripty a obecně zranitelný dynamický obsah. Typickým příkladem je exploit na stránkách uživatele, který o tom nemá ponětí.

nvestovat
ny dolarů do
mení velké kor-
:e, když za do-
několik dolarů
ıu proniknout
ovek firem?

Znamená to tedy, že velké firmy jsou v bezpečí?
Útočné skupiny se chovají ekonomicky. Proč investovat miliony dolarů do prolomení velké korporace, když za doslova několik dolarů mohou proniknout do stovek organizací? Z toho důvodu většina útoků směřuje na menší společnosti, které mají nižší úroveň ochrany. Na druhou stranu ani prolomení ochrany velké společnosti není nemožné. Jen se při něm zpravidla používají jiné techniky.

Jaké jsou v současnosti největší bezpečnostní hrozby pro firmy?
Z externích hrozeb je to sociální inženýrství. Proč by útočník komplikovaně prolamoval složité IT zabezpečení, když lze lsti získat heslo od samotného zaměstnance? IT bezpečnost proto není otázkou jen spolehlivého softwaru. Často se opomíjí pravidelné školení zaměstnanců. Přitom právě uživatel je zpravidla tím nejslabším článkem v celé komplexní IT bezpečnosti.

Mohl byste to více upřesnit?
Není neobvyklé, že se z běžného zaměstnance stane tzv. insider. Nejčastějším případem je nespokojený zaměstnanec, který si na přenosný disk stáhne firemní data a vyvede je z organizace. Bez využívání nástrojů pro ověření přístupu a prevence ztráty dat je krádež dat pro insidera až příliš snadná, a tedy i lákavá. Mezi další nástroje patří aplikace umožňující zachytávání konkrétních informací ve firmě, např. keylogger pro získávání uživatelských hesel či vzdálený přístup. Mnohá APT je složité odhalit bez softwaru pro detekci anomálií v síti

Jak se těmto hrozbám účinně bránit?
Bezpečnost je mozaika a je třeba myslet na komplexní přístup Základem jsou vícevrstvá ochrana zahrnující nástroje počítačové bezpečnosti na úrovni koncových bodů a vstupních bran funkční systém zálohování a obnovy dat, nástroje pro vícefaktorovou autentizaci či systém pro správu dokumentů a přístupu k nim. Lidé, kteří stojí na druhé straně barikády, nejsou hloupí. Nemůžeme proto spoléhat na uživatele, ale musíme jim pomoci.

NTÁŘ

VEBER,
ARCHITEKT,
NET

Na bezpečnosti se musí vytrvale pracovat

Jaké jsou požadavky na pozici manažera bezpečnosti? Zdá se, že to je schopnost generovat směrnice, procesy a papíry vůbec. A především dovednost nenaslouchat vlastním kolegům, síťařům a naopak velká schopnost naslouchat marketingovým slibům dodavatelů bezpečnostních řešení. Podle mého by každý manažer bezpečnosti IT měl být původem síťař. Vždyť bezpečnost v IT je dnes především o síťové bezpečnosti, o bezpečnosti ve světě protokolu IP v kombinaci s aplikacemi.

Před časem jsme dodávali specializované zařízení na obranu proti útokům DDoS a součástí bylo zpracování směrnice pro řešení DoS/DDoS útoků. Manažer bezpečnosti nad směrnicí zajásal a dokument založil. Zařízení na ochranu proti DDoS útokům je výborný nástroj. Jenže u tohoto řešení není možné jej na začátku nastavit a myslet si, že je hotovo. Jak se s novými aplikacemi mění provoz, je nutné dynamicky měnit konfiguraci. To znamená měnit nastavení tresholdů. Jenže na konfiguraci tohoto zařízení už nikdo ani nesáhl. Zákazník má manažera bezpečnosti a ten má směrnici pro řešení DDoS útoku. Jenže nemá bezpečnostního analytika = síťaře, který by dokument využíval a hlavně průběžně měnil nastavení zařízení na ochranu proti DDoS.

Nebo jeden velký úřad. Parta šikovných kluků, znám je dlouho. Znají svoji síť a mají ji zabezpečenou přiměřeně velikosti sítě a finančním možnostem. Jenže úřad rostl, a tak došlo na vytvoření Odboru rozvoje a architektury ICT a Odboru kybernetické bezpečnosti. Vše paralelně vedle současných správců sítě. Za rok po vytvoření nových oddělení nikdo z bezpečnostních manažerů nepřišel za síťaři a nezeptal se: „Jak ta naše síť vlastně funguje? Co vás trápí? Co dělat lépe?" Za to jim vygenerovali novou hromadu směrnic a nařízení.

e s novými apli-
ni mění provoz,
tné dynamicky
t konfiguraci.

Manažeři bezpečnosti měli v obou případech jedno společné. Tedy kromě směrnic a procedur. Básnili o SIEM. To je v jejich představách podpořeno marketingem velkých výrobců, všemocný nástroj, který rozbliká kontrolku, když útočník na útok jen pomyslí. Koupíme SIEM, necháme naimplementovat a bude navždy vyřešeno.

Zakoupeno (licence za hromadu peněz), nainstalováno (to bylo jednoduché), implementováno (spousta manday dodavatele). Jenže o systém se nikdo dále nestaral, nikdo jej nerozvíjel, nikdo jej neladil, nikdo s ním nežil. Pozice bezpečnostního analytika zůstala neobsazena, nenašel se kandidát. A správci sítě marně volají po centrálním úložišti dat, které se mělo v rámci SIEM vytvořit. Nejsou licence, došly peníze.

A jsme u jádra pudla. Kdo chyběl v obou uvedených scénářích? Anebo tam byl a nikdo s ním nekomunikoval? Bezpečnostní analytik a síťař, klidně v jedné osobě. Vždyť dobrý síťaři je vlastně bezpečnostní analytik. Musí znát svoji síť, musí s ní žít, musí všechna ochranná zařízení a aplikace dynamicky přizpůsobovat změnám v síti. A musí mít kde hledat v logách. Ne rozptýlených po zařízeních a aplikacích, ale uložených v centrálním úložišti logů. Takovém, které není svázáno licencemi jako velká SIEM řešení. Ale disponuje základními vlastnostmi SIEM jako alerting, reporting a korelace.