Politika rychlostních radarů v IT sítích

Organizace si dobrovolně pouštějí hrozby do vlastní sítě. Co všechno tím riskují? Jak mohou riziko nebezpečí snadno snížit a navíc zavést preventivní opatření známé z rychlostních radarů na našich silnicích?

Člen ostrahy umístil malware do počítače nemocnice. Malware byl připraven vypnout ovládání teploty, ventilace a chladicích systémů, což v důsledku mohlo stát lidské životy. Naštěstí umístil video s plánem činu na YouTube a včas byl zadržen.

Skupina pracovníků ministerstva dopravy spolupracovala, aby si navzájem přivydělala. Vydávala řidičské průkazy nezpůsobilým lidem a dalším, kteří je nemohli získat legálně. Nakonec jsou odhaleni policistou, který se vydával za zájemce o jejich služby.

Tyto incidenty spadají do kategorie tzv. insider threat neboli vnitřních hrozeb – zločinů spáchaných zaměstnanci, dodavateli nebo obchodními partnery napadené společnosti.

Možná jste v médiích zaznamenali, že škody takto napadené společnosti jsou značné, a to včetně finančních ztrát, provozních dopadů, poškození dobrého jména společnosti či jednotlivých zaměstnanců. I aktivity jediného záškodníka způsobily škody od několika ztracených hodin na projektech až po ztráty, které vedly k ukončení činnosti společnosti. Kromě toho mohou mít tyto akce i dopad mimo poškozenou organizaci. Mohou zastavit konkrétní odvětví nebo vytvoří závažné riziko pro veřejnou i národní bezpečnost, vzpomeňme jen na případ Edwarda Snowdena, který vynesl na veřejnost utajované informace o tajných službách.

Co hrozí?

Většina organizací strávila roky zaváděním systémů, jejichž cílem je zabezpečit své zázemí. Databáze, virtuální privátní sítě (VPN), detekce narušení (IDS), řízení přístupu a identit (IAM) a další systémy. Tato řešení sbírají obrovská množství dat a logů ve snaze monitorovat systémy a reportovat, co se děje. Ve většině případů se informace shromažďují v SIEM (Security Information and Event Monitoring) systémech, které sebrané informace korelují a snaží se identifikovat nebezpečné situace. I přesto vzniká velký problém. Správci IT, smluvní externí společnosti a každodenní uživatelé mají přístup k velmi citlivým datům skrze ověřené aplikace. Samozřejmě, musejí přece dělat svoji práci!

V tuto chvíli je již jakýkoli systém neúčinný. Poté, co prošli přes externí zabezpečení, jsou uživatelé uvnitř bezpečnostního perimetru, protože jsou autorizováni pro přístup k těmto informacím (nebo použili ukradené přístupové účty). Nyní jim nic nebrání v odcizení dat, poškozování systémů, nebo dokonce v neúmyslném zveřejnění citlivých informací. Jinými slovy, IT bezpečnostní oddělení využívá většinu svého rozpočtu na ochranu back-end zařízení (servery, databáze), a přitom ignorují front-end nebezpečí ze strany ověřených pracovníků a aplikací. Jakmile se uživatel přihlásí do aplikace s citlivými daty, většina organizací nemá ponětí o tom, co v ní dělá. To je obrovská mezera v zabezpečení většiny společností.

Nezapomeňme na módní trendy

Dnes je již naprosto normální, ne-li požadované, aby zaměstnanci pro práci používali svá zařízení. Tento trend sice přináší společnostem značné úspory, ale zároveň je vystavuje zvýšenému riziku úniků informací. Uvědomme si, že na těchto koncových bodech nemusí být pouze malware, který se přenese do našich interních systémů. Zcela určitě tam jsou i aplikace pro sociální sítě, které ještě usnadňují vynesení citlivých informací a třeba i neúmyslné poškození společnosti.

Dnes již tuto mezeru dokážeme vyplnit a zabezpečit například řešeními z oblasti user activity recordingu. Jedním z nejlépe hodnocených řešení je technologie společnosti ObserveIT, která umožňuje nahrávat aktivitu každého uživatele nebo dodavatele a zároveň zasílat upozornění, pokud poruší bezpečnostní pravidla. Řešení dokáže detekovat kopírování souborů, spouštění neobvyklých aplikací, přihlašování do systému v jinou než pracovní dobu, přístup z neobvyklých zařízení nebo exportování nezvyklých reportů. Kromě jednoduchého nastavení pravidel podle schématu „who-did-what" nám ve formě videí, kde je obrazový záznam každé uživatelské aktivity, poskytuje i forenzní důkazy pro případné soudní pře.

Zajímavé je přirovnání tohoto řešení k rychlostním radarům. Radar zaznamená každý automobil, ale nahlásí jen ty, které překročí rychlost. Jakmile navíc řidiči vědí, že je před nimi radar, naprostá většina z nich upraví rychlost tak, aby pravidla chování nepřekročila. Tím se v měřených úsecích výrazně zvýšila bezpečnost provozu. Proč tedy neimplementovat podobné řešení do IT systémů, když se již osvědčilo na silnicích? ●

ObserveIT je globálním lídrem v oblasti řízení vnitřních hrozeb (insider threat management). Pomáhá více než 1 200 zákazníkům po celém světě odhalit vnitřní hrozby, a zamezit tak ztrátám dat.

observe it

Jiří Kolc,
business development manager pro produkty ObserveIT u distributora Veracomp