Kybernetický útok představuje šok

Dokážeme ochránit systém každé firmy za rozumnou cenu, říká Tomáš Filip, šéf nového Cyber Defence Centra společnosti AEC

Václav Herz
herz@mf.cz

Každá firma se dříve či později stane terčem kybernetického útoku. A to bez ohledu na počet zaměstnanců nebo roční obrat, protože i malé advokátní kanceláře nebo investiční skupiny disponují citlivými daty a stojí a padají se svým duševním vlastnictvím. Reakce na incident bývá vždy stejná – pro napadené firmy je to šok a všechny do jedné začnou masivně investovat do své bezpečnosti.

Jakým způsobem u nás firmy řeší ochranu svých systémů?
Pokud vůbec, snaží se chránit nejčastěji samy. Činí tak za pomoci nemalých prostředků, které na to vyčlení, a s lidmi, které se jim poštěstí sehnat, zaplatit, vyškolit a občas i udržet. Specializovaná centra, jako je naše CDC (Cyber Defence Center), nabízejí nesrovnatelně efektivnější způsob ochrany. Za cenu, kterou má na dnešním trhu práce jeden schopný bezpečnostní analytik, si může jakákoli firma outsourcovat služby týmu expertů z nové unikátní divize zavedené společnosti AEC.

Co nová služba zákazníkům nabízí?
AEC, která je na trhu déle než 25 let, v současnosti disponuje divizí bezpečnostních technologií, týmem etických hackerů a skupinou analytiků. Každá z těchto samostatných jednotek se zaměřuje na specifické služby a dohromady umí poskytnout všechny myslitelné typy jednorázových bezpečnostních řešení. CDC, které vzniklo letos, tvoří čtvrtou skupinu, zaměřenou na včasnou detekci, rychlé řešení a proaktivní budování ochrany klientů založené na dlouhodobější spolupráci. Jedná se o expertní kompetenční centrum, které monitoruje dění u zákazníka a reaguje na ně v reálném čase.

Jak dnes vypadá běžná nabídka na trhu s IT bezpečností?
Co se týče klasických poskytovatelů bezpečnostních technologií, je to často tak, že mají omezený počet specialistů, a pokud řešení nějakého problému převyšuje dostupnou kapacitu, jsou ztraceni. Zákazník má uzavřenou smlouvu s nějakou IT firmou přes kybernetickou bezpečnost a ta mu zasílá reporty o dění v jeho infrastruktuře, potažmo o incidentech. Ty už ale tato IT firma neřeší a zákazník je odkázaný na vlastní zdroje.

Ve vašem případě to probíhá jak?
CDC je specifické v tom, že my primárně poskytujeme službu. Náš klient si nepotřebuje kupovat software, nemusí shánět kontraktory nebo nabírat nové specialisty, v podstatě nepotřebuje ani žádný hardware. Řekne: tady mám prostředí, povězte mi, co je pro mě důležité a ochraňte mě. Jsme unikátní ve schopnosti detekovat problém a zároveň máme nástroje, které nám umožňují ten problém efektivně řešit. A to aniž bychom tím klienta zatěžovali nad rámec běžné komunikace.

Pomáhá nějak klientům to, že CDC je součástí větší firmy?
Pokud klient využije služeb CDC, disponuje zároveň veškerým know-how všech týmů AEC. Jedná se o synergické využití velice širokého spektra znalostí a zkušeností. Díky tomu si dokážeme lépe než kdo jiný poradit s naprostou většinou událostí, incidentů či útoků. Klíčové je, že vysoce efektivní servis CDC je i díky bezprostřednímu napojení na kapacity AEC k dispozici za rozumnou cenu všem bez rozdílu. Včetně malých a středních firem, pro něž jsou běžná řešení stále příliš robustní a nákladná.

Liší se v tomto ohledu situace u nás a v zahraničí?
Hlavní rozdíl není v tom, že bychom tu neměli špičkové technologie a firmy do nich neinvestovaly. Jde o to, že ty firmy pak nedokážou tyto nástroje reálně využívat. Rozdíl je v tom, že společnosti na západ od nás investují vedle nástrojů především do lidí a nebojí se přitom outsourcovat. Nebojí se říct: Toto my neumíme, požádáme někoho kompetentního, aby nám s tím pomohl.

> Každá firma se dříve či později stane terčem kybernetického útoku.

Proč takový postup není standardní i u nás?
Setkáváme se s tím, že firmy v České republice mají strach outsourcovat interní bezpečnostní funkce. Obávají se například toho, aby se do nepovolaných rukou nedostaly logy, tedy záznamy o tom, co se děje v jejich systémech. Přitom ale těm stejným firmám nevadí, že už mají na internetu Outlook, Office, prostě veškerá citlivá data, kde má potenciální útočník vysvětlené všechno pěkně v kontextu. Pro CDC je věcí profesionální cti poskytovat svým zákazníkům tu nejvyšší úroveň zabezpečení. A to se samozřejmě týká i nakládání s jeho daty. ●

FOTO: archiv