PATRON-IT staví svůj monitorovací systém na technologii N-able

Společnost PATRON-IT je jednou z nejrespektovanějších českých společností, které se specializují na IT bezpečnost. Její hlavní činností jsou dodávky SaaS (Security as a Service) služeb s garancí bezpečnosti a obrany proti útokům. Firma rovněž řeší akutní ransomwarové události v případě konkrétních útoků včetně dešifrování dat, krizového managementu či vyjednání výkupného. PATRON-IT pro své zákazníky pořizuje řešení dostupná na trhu, nastavuje je a vylepšuje s pomocí vlastních skriptů a dodává formou MSSP – tedy poskytování řízených služeb IT bezpečnosti.

Martin Haller (vlevo) a Martin Melich, spoluzakladatelé PATRON-IT

Oblast IT bezpečnosti se zásadně proměnila s příchodem kryptoměn, které hackerům umožnily snadno a diskrétně monetizovat svou činnost. Ransomwarových útoků je proto čím dál více a možností napadených firem jsou omezené – mohou obnovit data ze zálohy, v případě ztráty záloh případně dešifrovat, a v krajním případě zaplatit výkupné. Avšak nejefektivnější je prevence před útoky s pomocí správně nastavených řešení. PATRON-IT si jednotlivá řešení testuje s pomocí simulovaných útoků a validuje je, aby byly schopné obstát v prostředí skutečných útoků. Takto validovaná řešení pak využívá k ochraně svých zákazníků.

RMM platforma + vlastní skripty

Jednou z využívaných platforem je také **N-able N-sight RMM** (dříve SolarWinds RMM, původně GFI MAX), jejímž distributorem je společnost **ZEBRA SYSTEMS**. V minulosti v PATRON-IT hledali nástroj monitoringu IT infrastruktury, protože potřebovali zpětnou vazbu k prováděným bezpečnostním opatřením. Zásadní problém v konkrétních organizacích totiž spočívá v nesouladu toho, co by si firmy přály mít nastaveno a co je skutečně nastaveno. Většinou se tak děje z důvodu, že organizace nevyužívají automatizaci a nemají k dispozici zpětnou vazbu.

„Firmám nepomůže si koupit jenom samotný bezpečnostní nástroj, který jednou provždy vyřeší všechny problémy. Pokud si nepotvrdí, že toto řešení pracuje podle jejich představ a jsou přes všechno napadeny hackerským útokem, přichází velké zklamání. My se snažíme naše zákazníky varovat před přehnanými očekáváními a pomáháme jim nastavit jejich IT bezpečnost tak, aby tato řešení fungovala i v reálném světě," říká **Martin Melich, jednatel a spoluzakladatel PATRON-IT.**

PATRON-IT proto léta buduje monitorovací systém, který nesleduje jen obvyklé údaje jako např. místo na disku a výkon serverů, ale navíc hlídá pečlivost prováděných opatření v daném prostředí. K tomu využívají cloudovou platformu N-able N-sight a na ní postavené vlastní pokročilé skripty, které společně tvoří ucelený kontrolní nástroj. Takto si v podstatě vytvořili řešení nepřetržitého auditu, kam se zadávají nejčastější zjištěná zneužití a aktuální hrozby, a tím se automatizovaně kontroluje celé prostředí zákazníka.

Monitorování

Primární funkcí celého systému je monitorování. S jeho pomocí se PATRON-IT snaží monitorovat vše, co je důležité a co pomůže s prevencí nebo včasnou detekcí chyb. Systém hlídá veškerou IT infrastrukturu včetně serverů, stanic, storage, UPS, switchů, routerů, kamer, wifi AP a detekce neznámých zařízení. Kdyby se to všechno mělo kontrolovat manuálně, kontrola trvala by celé týdny. Přitom monitorovací systém to zvládne každých 5 minut.

Protože hlavní činností firmy je prevence stávajících zákazníků před útoky, upravené RMM řešení je nasazováno u všech zákazníků k monitoringu a auditu. Vedle této funkčnosti jsou součástí ochrany také nástroje antiviru, zálohování, správy apod.

Správa aktualizací a správa majetku

Jelikož monitorovací systém má integrovanou správu patchování, využívá se také k pravidelným aktualizacím. Vše je v jedné konzoli (rychleji se zaučuje, vše je na jednom místě a je potřeba méně „agentů" na stanicích), u zákazníků jsou lokální cache (aby si 100 počítačů nestahovalo stejný update zvlášť) a provádějí se aktualizace softwaru jak od Microsoftu, tak od jiných výrobců.

Monitorovacím systémem PATRON-IT řeší i správu majetku. Systém udržuje přehled o tom, jaké jsou u zákazníků servery, počítače, notebooky (včetně konfigurace) a síťová zařízení (routery, switche, kamery, telefony, Wifi AP a jiné krabičky). Je to užitečné v tom, že existuje přehled zařízení a nestojí to žádný čas ani práci navíc. Pokud chce zákazník znát, jaký má počítačový „park", jaké jsou nejstarší stroje, anebo jen hledá, na jakých PC je nainstalován určitý software, není problém.

„Produkt N-sight RMM představuje dobrý start, ale je nutné připravit se na to, že instalace je jenom začátek. Pak je třeba si ujasnit, co se bude monitorovat, jak se to bude monitorovat, jak má systém upozorňovat na chyby apod. My systém používáme už od roku 2013 a jsme mezi 3 největšími uživateli v ČR a SK. Za tu dobu jsme se systémem nasbírali hodně zkušeností a poměrně významně si jej upravili – ke spokojenosti své i našich zákazníků," dodává Martin Melich. ■