



Soitron Security Sensor dal ZKW Slovakia obraz o bezpečnosti firemného IT

„Nové riešenia nám priniesli pokročilú detekciu hrozieb, čo nám pomáha chrániť používateľov a pracovné stanice aj od sofistikovanejšieho malvéru.“

Stanislav Smolár
Soitron, Security Manager

1. POŽIADAVKY

- Získať **kontinuálny obraz o bezpečnosti siete a firemných IKT zdrojoch**.
- Preukázať kľúčovým odberateľom **odolnosť voči kybernetickým hrozbám** a schopnosť chrániť dáta.
- **Zvýšiť bezpečnosť** technologickej infraštruktúry.

2. RIEŠENIE

- **Penetračné testy** a nasadenie riešenia **Soitron Security Sensor**, ktoré v sebe integruje viaceré bezpečnostné technológie od rôznych dodávateľov, napríklad Flowmon, Cisco a Fortinet.
- **Audit na základe monitoringu siete** zákazníka a zozbieraných dát.
- Záverečná **správa o aktuálnom stave zabezpečenia IT** a odporúčania pre zlepšenie.

3. VÝSLEDKY

- **Identifikácia nedostatkov**, na ktoré by zákazník bez nasadenia pokročilých technológií neprišiel.
- Možnosť **otestovať viaceré špičkové bezpečnostné technológie** od rozličných dodávateľov v jednom balíku.
- **Posilnenie bezpečnosti IT** v spoločnosti ZKW Slovakia s.r.o.
- **Zlepšenie prehľadu o stave a prevádzke podnikovej siete**, vrátane upozornení na anomálie, vďaka čomu dokáže firma včas identifikovať potenciálne hrozby aj prípadné problémy s výkonnosťou.

Východiská

Priemyselné podniky vo všeobecnosti nepatria k priekopníkom zavádzania technológií pre počítačovú bezpečnosť, pretože cyklus obnovy technológií je násobne pomalší a finančne náročnejší voči IT.

Popredný dodávateľ svetelných systémov a elektroniky v oblasti automotive, spoločnosť ZKW Slovakia s.r.o., sa však radí medzi svetlé výnimky.

Podnik má osem závodov v siedmich krajinách vrátane Slovenska, odkiaľ zásobuje jedného zo svojich strategických partnerov, automobilku Volkswagen. Hoci slovenský závod ZKW Slovakia sa zatiaľ nikdy neocitol pod nezvyčajnou paľbou kybernetických útokov, jeho manažment aj informatici si dobre uvedomujú riziká, ktoré sa v sieti ukrývajú. Jeden z dôvodov je aj to, že ZKW Slovakia významne investuje do vlastného technologického vývoja v oblasti svetelných systémov. Navyše, do čoraz vyššej bezpečnosti ich tlačia aj odberatelia.

Keď ZKW Slovakia potreboval urobiť penetračné testy, ktorými by vedel odberateľom preukázať pripravenosť na kybernetické hrozby, spoločnosť Soitron práve dokončila vývoj svojho nového systému s názvom Soitron Security Sensor. Ide o riešenie, ktoré dokáže zanalyzovať sieťovú prevádzku, ako aj prenášaný obsah

a následne odporučiť kroky na zvýšenie bezpečnosti.

Ponuka prišla firme ZKW Slovakia vhod. Firemní informatici v minulosti hľadali a odstraňovali problémy s firemnou sieťou zdĺhavo a problematicky. Zároveň si uvedomovali, že dnešné špičkové technológie poskytujú lepší prehľad o stave a výkonnosti siete ako mali k dispozícii a umožňujú tiež posunúť bezpečnosť IT na vyššiu úroveň.

Riešenie

Po úvodnej diskusii o detailoch auditu a podpísaní dohody o mlčanlivosti, Soitron nastavil virtuálne stroje a na mesiac zapožičal ZKW Slovakia hardvérový senzor. Ide de facto o server, ktorý v sebe kombinuje viaceré bezpečnostné technológie. Napríklad pre behaviorálnu analýzu siete od firmy Flowmon, novú generáciu firewallov od Cisco a dvojúrovňový sandbox od Fortinetu, ktorý je doplnený špičkovým riešením na ochranu proti škodlivému kódu.

Soitron Security Sensor po nasadení, ktoré trvalo necelé dva týždne, po zvyšok mesiaca zbieral dáta z internej infraštruktúry ZKW Slovakia, pričom odborníci Soitronu priebežne doladzovali nastavenia a identifikovali slabiny v bezpečnosti, ako aj potenciálne hrozby. Na záver všetko zanalyzovali a predložili zákazníkovi výstupnú správu, vrátane odporúčaní, ktoré vyplynuli zo získaných dát.

„Mali sme možnosť otestovať, či bezpečnostné technológie spĺňajú naše požiadavky a či môžu byť pre nás prínosom. Na základe praktických skúseností sme sa rozhodli zakúpiť produkty Flowmon a Cisco, ktoré nám Soitron následne implementoval.“

Luboš Čulák
ZKW Slovakia, System Administrator



„Keď nás zákazník oslovil s požiadavkou o realizáciu penetračných testov, ihneď sme mu ponúkli možnosť vyskúšať aj náš nový systém, ktorý organizáciám umožňuje získať prehľad o slabých stránkach ich IT bezpečnosti a zároveň otestovať súbežne viaceré bezpečnostné technológie od rôznych dodávateľov.“

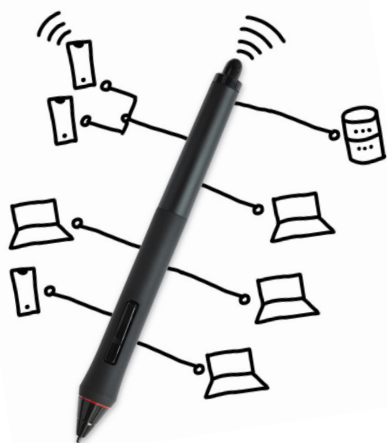
Stanislav Smolár
Soitron, Security Manager

Druhý krok

Hoci test potvrdil, že ochrana podnikovej počítačovej siete nebola úplne „deravá“ a IT infraštruktúra nečelila nezvyčajným kybernetickým útokom, analýzy získaných dát predsa len identifikovali veci, na ktoré by podnik bez auditu možno nikdy neprišiel. Išlo napríklad o niekoľko počítačov, ktoré boli bez vedomia oddelenia IT mimo domény a obsahovali škodlivý kód. Okrem toho Soitron Security Sensor umožnil administrátorom ZKW

Slovakia vyskúšať si, ako sa pracuje so špičkovými technológiami. V prípade záujmu si z nich firma mohla vybrať tie, ktoré vyhodnotí ako najprínosnejšie pre posilnenie bezpečnosti a spoľahlivosti svojej technologickej infraštruktúry.

Výhodou je, že po mesačnej skúsenosti vedia podnikoví informatici s novými technológiami pracovať a môžu ich tak okamžite plnohodnotne využívať.





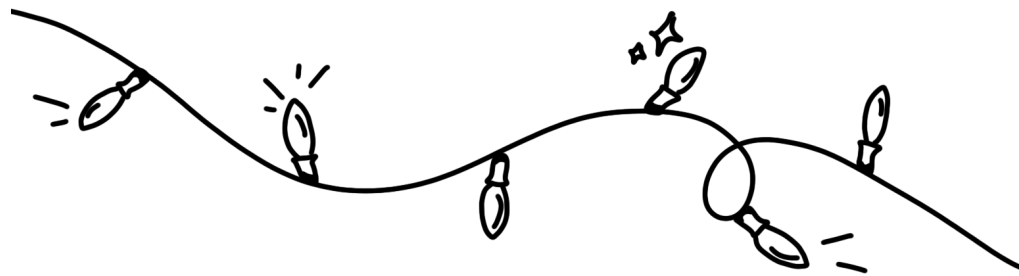
Prínosy

Riešenie **Flowmon** dnes poskytuje ZKW Slovakia detailný pohľad na prevádzku a dátové toky podnikovej siete, čo skraca čas potrebný na odstraňovanie problémov. Administrátori vďaka nemu dostávajú automatické upozornenia na potenciálne výkonnostné problémy siete.

Flowmon však plní aj iné úlohy. Keď firemní informatici potrebovali umiestniť niekoľko serverov a osobných počítačov na vzdialené pracovisko, systém im pomohol vypočítať

a predpovedať minimálnu potrebnú šírku pásma pre spojenie s požadovanou lokalitou.

Druhý nástroj, pre ktorý sa ZKW Slovakia na základe mesačného testovania Security Sensora rozhodol, je **Cisco Stealthwatch**. Na Slovensku ide o jedno z vôbec prvých nasadení tohto systému, ktorý umožňuje identifikovať rozličné typy nových aj doposiaľ neznámych hrozieb, a tým posilniť bezpečnosť podnikového IT.



ZKW Slovakia s.r.o.

ZKW Slovakia s.r.o., člen skupiny ZKW Group, je špecialista na inovatívne prémiové svetelné systémy a elektroniku. Ako systémový dodávateľ je jedným z vedúcich strategických partnerov

automobilového priemyslu. Vyvíja a vyrába prémiové svetelné systémy a elektronické moduly. Tak formuje vzhľad a charakter motorových vozidiel po celom svete.

www.zkw-group.sk

SOITRON, s.r.o., člen skupiny SOITRON Group

Spoločnosť Soitron je stredoeurópskym integrátorom, ktorý pôsobí na IT trhu už od roku 1991. Filozofiou spoločnosti je snaha neustále napredovať, a aj preto je lídrom v zavádzaní unikátnych technológií a inovatívnych riešení. Svojim klientom ponúka produkty a služby v oblasti robotizácie a automatizácie procesov, umelej inteligencie, internetu vecí (IoT), IT infraštruktúry, komunikačných a cloudových riešení, IT bezpečnosti, IT služieb a outsourcingu, IT poradenstva a aplikácií či digitalizácie IT oddelení. Do produktového portfólia patrí aj riešenie pre inteligentné policajné autá – Mosy a služby v oblasti kybernetickej bezpečnosti – Void Security Operations Center. Soitron, s.r.o. je členom skupiny Soitron Group, v ktorej pracuje viac ako 800 medzinárodných odborníkov. Skupina združuje profesionálne tímy na Slovensku, v Českej republike, Rumunsku, Turecku, Bulharsku, Poľsku a Veľkej Británii.