



Manažéri Bratislavskej teplárenskej získali reálny pohľad na citlivé dáta vo firme

„S citlivými dátami dnes vďaka novému systému pracujeme zodpovedným spôsobom, podľa jasne definovaných pravidiel.“

Miloš Žitný

Bratislavská teplárenská
VOD IT a telekomunikácií

1. POŽIADAVKY

- Nasadiť v spoločnosti riešenie **Safetica DLP** na prevenciu úniku dát (DLP = Data Loss Prevention).
- Zabezpečiť súlad vnútrofiremných procesov a technológií s požiadavkami novej legislatívy (GDPR a zákona o kybernetickej bezpečnosti).
- Využiť príležitosť a **aktualizovať existujúce postupy pri narábaní s citlivými údajmi** tak, aby boli v súlade nie len so zákonom, ale aj s očakávaniami vedenia spoločnosti.

2. RIEŠENIE

- **Zmapovanie spôsobov a foriem spracovania dát** pomocou modulu Safetica Auditor - odkiaľ dáta prichádzajú, ako vznikajú, ako sa s nimi narába a kam putujú ďalej.
- **Klasifikácia dát** podľa obsahu, pôvodu a ďalších metadát.
- **Vytvorenie pravidiel** (politik) pre rôzne skupiny citlivých údajov.
- **Vyškolenie IT tímu** klienta.

3. VÝSLEDKY

- **Získanie prehľadu a kontroly nad dátami** vo firme.
- Možnosť okamžite a plošne meniť, ako aj aplikovať pravidlá pre prácu s citlivými informáciami.
- **Systém notifikácií**, ktorý upozorňuje používateľa, aby venoval zvýšenú pozornosť dátam, s ktorými práve prichádza do kontaktu (silný edukatívny účel riešenia).
- **Znemožnenie neoprávneného nakladania s citlivými údajmi** - preposielanie, kopírovanie, tlač alebo nahrávanie na neznáme USB kľúče.
- Nové **analýzy a štatistiky** o dátových tokoch vo firme.

Východiská

Bratislavská teplárenská (skrátene BAT) je významným zákazníkom Soitronu už dlhé roky. Impulz k novej spolupráci prišiel s novým zákonom o kybernetickej bezpečnosti z roku 2018. Podľa neho musia špecifické podniky, ktoré poskytujú takzvanú základnú alebo digitálnu službu, zabezpečiť zvýšenú bezpečnosť svojich dát. Zjednodušene povedané ide o firmy, ktoré majú pre fungovanie krajiny strategický význam - patria sem napríklad banky, telekomunikačné spoločnosti, energetické podniky, nemocnice, producenti chemikálií,

ťažký priemysel, ale aj dopravné a vodárenské spoločnosti a distribútori energií. Teda aj Bratislavská teplárenská. Výrobca a distribútor tepla už jeden systém DLP vyskúšal - no nebol s ním spokojný a obzeral sa po novom dodávateľovi. Soitron mu padol do oka z dvoch dôvodov - okrem predchádzajúcich skúseností to bol certifikát „Gold Partner“ od developera Safetica Technologies, ktorý vyvíja rovnomenný softvérový balík Safetica DLP. Práve o ten mala BAT-ka záujem. Dát, ktoré BAT potrebuje ochrániť, je veľa - od osobných údajov

vlastných zamestnancov, cez informácie o zákazníkoch, ich spotrebe až po finančné údaje a citlivé priemyselné dokumenty - konštrukčné plány, výkresy a dizajnové návrhy. V rôznej miere sa k nim dalo dostať cez 250 pracovných staníc - desktopov a laptopov. Dáta neustále niekam putujú, distribuujú sa cez interný informačný systém, kopírujú sa - nielen digitálne, ale aj fyzicky, alebo sa prenášajú na prenosných médiách - typicky na USB kľúčoch.



Riešenia

BAT patril k menšine zákazníkov Soitronu, ktorý od začiatku vedia, čo chcú. Po otestovaní skúšobných verzií viacerých vývojárov si spoločnosť vybrala na prevenciu úniku dát balík Safetica DLP. Úlohou Soitronu bolo zabezpečiť hladké technologické nasadenie. To znamenalo nadizajnovať

a naškalovať potrebný hardvér, zabezpečiť pilotné testovanie a na jeho základe nastaviť a optimalizovať Safeticu skôr, než ju plošne nasadia. Klient sa hneď v úvode rozhodol, že počas implementácie sa nebude len ticho prizerať so založenými rukami. V BAT-ke sa naopak sformovala pracovná

skupina naprieč celou štruktúrou spoločnosti. Jej členovia dôsledne a otvorene komunikovali s ostatnými zamestnancami na všetkých úrovniach, aktívne od nich získavali spätnú väzbu a organizovali školenia.

Riešenie od Safeticy má dve hlavné časti - moduly. Prvý s názvom Auditor poslúžil na získavanie prvotného obrazu o dátových tokoch v spoločnosti. Na vybraných koncových zariadeniach bežal približne 3 mesiace.

S výsledkami úvodného auditu sa oboznámili najskôr vedúci jednotlivých oddelení, ktorí mali za úlohu porovnať ich s realitou - teda overiť, či to, čo modul Auditor zistil, sedí alebo nie. Okrem toho overili obsah dát, keďže samotný modul sa zameril na sledovanie dátových tokov. Na základe tejto vstupnej analýzy bolo možné navrhnúť:

- Ako majú byť dáta efektívne klasifikované, teda roztriedené a označené.
- Revidovať pravidlá (politiky) pre zaobchádzanie s dátami v jednotlivých skupinách - kto s nimi môže prísť do kontaktu, ako s nimi môže pracovať, distribuovať ich alebo kopírovať.

O dodržiavanie týchto politík sa stará druhý modul - Safetica DLP. IT tím klienta sa pred spustením ostrej prevádzky postaral o distribúciu programového vybavenia Safetica DLP na jednotlivé pracovné stanice pripojené do firemnej siete. Aplikácia pravidiel má dve formy - notifikácia zamestnanca v prípade, že pracuje s citlivými údajmi alebo priamo reštrikcia, ak chce dáta spracovávať neoprávneným spôsobom.

Z pohľadu hardvéru si Safetica nevyžiadala žiadne drastické investície - v systéme bolo iba potrebné vyčleniť jeden virtuálny server a navýšiť hardvérový výkon približne o 5 %. Rozbehnúť celý systém po tom, čo je nastavená klasifikácia a pravidlá je otázkou hodín, maximálne dní. Pri nasadzovaní bol po celý čas k dispozícii aj vývojár celého riešenia - spoločnosť Safetica, ktorý však nakoniec nemusel riešiť žiadny vážny problém.



„Už teraz s Bratislavskou teplárenskou plánujeme systém rozširovať o ďalšie funkcie - nastavovanie pravidiel pre pripájanie ďalších zariadení, šifrovanie diskov a USB kľúčov.“

Marek Cisár
SOITRON
Systémový špecialista





Výsledok

Citlivé údaje dnes zamestnanec BAT nedokáže poslať, kopírovať, tlačiť alebo prenášať na USB disky bez toho, aby túto operáciu zaznamenal a vyhodnotil systém Safetica DLP.

Dáta sú jasne roztriedené a pracuje sa s nimi pod prísny dozor podľa presne vymedzených pravidiel tak, aby boli chránení zákazníci, zamestnanci a aj dôveryhodnosť značky Bratislavská teplárenská.

IT tím BAT aj manažment spoločnosti navyše získal ucelený prehľad o tom, ako sa s citlivými údajmi vo firme narába - odkiaľ prichádzajú, kto a ako s nimi pracuje, kam ich poslať. Na základe toho sa môžu prijímať ďalšie opatrenia - meniť klasifikácia alebo politiky. BAT získala aj oveľa lepšiu predstavu o tom, akú hodnotu majú firemné aplikácie podľa toho, ako intenzívne sa využívajú a na aké operácie.



Bratislavská teplárenská, a.s.

Bratislavská teplárenská, a.s. (BAT) sa zaoberá najmä výrobou tepla, výrobou silovej a regulačnej elektriny, výkupom tepla, rozvodom tepla a rozvodom elektriny. V procese kombinovanej výroby elektriny a tepla zabezpečuje hospodárne prevádzkovanie sústav centralizovaného zásobovania teplom (CZT). Zabezpečuje dodávku tepla na vykurovanie a prípravu teplej úžitkovej vody v prevažnej väčšine

bytových objektov, administratívnych, zdravotných, kultúrnych, školských, športových zariadení v správe odberateľských organizácií ako aj dodávku tepla pre priemyselných odberateľov. V súčasnosti pokrýva približne 55% potreby tepla v rámci hlavného mesta.

www.batas.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, 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, ktoré je známe pod značkou Mosy. 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.