



Manažeři Bratislavskej teplárenskej získali reálny prehľad o citlivých datech ve firmě

„Díky novému systému dnes s citlivými daty pracujeme zodpovědně a podle jasně definovaných pravidel.“

Miloš Žitný
Bratislavská teplárenská
VOD IT a telekomunikací

1. POŽADAVKY

- Nasadit ve společnosti řešení **Safetica DLP** na prevenci úniku dat (DLP = Data Loss Prevention).
- Zajistit soulad vnitrofiremních procesů a technologií s požadavky nové legislativy (GDPR a zákon o kybernetické bezpečnosti).
- Využít příležitost a **aktualizovat stávající postupy nakládání s citlivými údaji** tak, aby byly v souladu nejen se zákonem, ale i s očekáváními vedení společnosti.

2. ŘEŠENÍ

- **Zmapování způsobů a podob zpracování dat** pomocí modulu Safetica Auditor – odkud data přicházejí, jak vznikají, jak se s nimi nakládá a kam směřují dál.
- **Klasifikace dat** podle obsahu, původu a dalších metadat.
- **Vytvoření pravidel** (zásad) pro různé kategorie citlivých údajů.
- **Proškolení IT týmu** klienta.

3. VÝSLEDKY

- **Získání přehledu a kontroly** nad daty ve firmě.
- Možnost okamžitě a plošně měnit i aplikovat pravidla práce s citlivými informacemi.
- **Systém notifikací**, který upozorňuje uživatele, aby věnoval zvýšenou pozornost datům, s nimiž právě přichází do kontaktu (silný edukativní efekt řešení)
- **Žádné neoprávněné nakládání s citlivými údaji** – přeposílání, kopírování, tisk nebo nahrávání na neznámé USB klíče.
- **Nové analýzy a statistiky** o datových tocích ve firmě.

Východiska

Bratislavská teplárenská (zkráceně BAT) je už dlouho významným zákazníkem Soitronu. Impuls k další spolupráci přišel s novým zákonem o kybernetické bezpečnosti z roku 2018. Podle něj musí konkrétní podniky poskytující takzvané základní nebo digitální služby zajistit zvýšenou bezpečnost svých dat. Zjednodušeně řečeno jde o firmy, které mají pro fungování země strategický význam – patří sem například banky, telekomunikační společnosti, energetické podniky, nemocnice, výrobci chemických látek, těžký průmysl, ale i do-

pravní a vodárenské společnosti a distributoři energií. Tedy i Bratislavská teplárenská. Výrobce a distributor tepla už jeden systém DLP vyzkoušel, ale nebyl s ním spokojený a rozhlížel se po novém dodavateli. Společnosti BAT padl Soitron do oka ze dvou důvodů – kromě předchozích zkušeností to byl certifikát Gold Partner od vývojářské firmy Safetica Technologies, která vyvíjí stejnojmenný softwarový balík Safetica DLP. Právě o ten měla BAT zájem. Dat, která BAT potřebuje ochránit, je spousta: osobní údaje vlastních zaměstnanců, informace

o zákaznících a jejich spotřebě až po finanční údaje a citlivé průmyslové dokumenty, jako jsou konstrukční plány, výkresy a designové návrhy. V různé míře se k nim dalo dostat přes 250 pracovních stanic – desktopů a laptopů. Data neustále někam putují, distribuují se přes interní informační systém, kopírují se nejen digitálně, ale i fyzicky, nebo se přenášejí na přenosných médiích, typicky na USB klíčkách.



Řešení

BAT je jeden ze zákazníků Soitronu, kteří od začátku vědí, co chtějí. Po otestování zkušebních verzí různých vývojářů si společnost k prevenci úniku dat vybrala balík Safetica DLP. Úkolem Soitronu bylo zajistit hladké technologické nasazení. To znamenalo

navrhnout a naškálovat potřebný hardware, zajistit pilotní testování a na jeho základě nastavit a optimalizovat Safeticu předtím, než ji plošně nasadí. Klient se hned v úvodu rozhodl, že během nasazování nebude přehlížet se založenými rukama. V BATce

naopak vznikla pracovní skupina složená z odborníků z různých složek společnosti. Její členové důsledně a otevřeně komunikovali s ostatními zaměstnanci na všech úrovních, aktivně od nich získávali zpětnou vazbu a organizovali školení.

Řešení od Safeticy má dva hlavní moduly. První z nich je Auditor, který posloužil při získávání prvotní představy o datových tocích ve společnosti. Na vybraných koncových zařízeních běžel přibližně tři měsíce.

S výsledky úvodního auditu se seznámili nejprve vedoucí jednotlivých oddělení, kteří měli za úkol porovnat je s realitou, tedy ověřit, jestli zjištění modulu Auditor sedí, nebo ne. Navíc ověřovali i obsah dat, protože samotný modul se zaměřil na sledování datových toků. Na základě této vstupní analýzy bylo možné navrhnout:

- způsob efektivní klasifikace dat, tedy jejich třídění a označování,
- revizi pravidel (zásady) pro zacházení s daty v jednotlivých skupinách – kdo s nimi může přijít do kontaktu, jak s nimi může pracovat, distribuovat je nebo kopírovat.

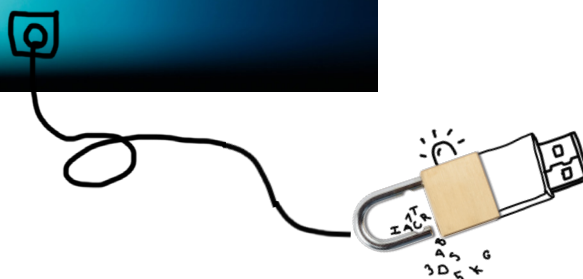
O dodržování těchto zásad se stará druhý modul – Safetica DLP. IT tým klienta zajistil před spuštěním ostrého provozu distribuci programového vybavení Safetica DLP na jednotlivé pracovní stanice připojené do firemní sítě. Aplikace pravidel má dvě podoby – notifikace zaměstnance v případě, že pracuje s citlivými údaji nebo přímo restrikce, pokud chce data zpracovávat neoprávněným způsobem.

Z pohledu hardwaru si Safetica nevyžádala žádné drastické investice. V systému bylo potřeba pouze vyčlenit jeden virtuální server a navýšit hardwarový výkon přibližně o 5 %. Jakmile je nastavená klasifikace včetně pravidel, je spuštění celého systému otázkou hodin, nejvýše dnů. Během nasazování byl celou dobu k dispozici i vývojář celého řešení, společnost Safetica, ale nakonec nebylo třeba řešit žádné vážné problémy.



„Už teď s Bratislavskou teplárenskou plánujeme rozšíření systému o další funkce jako nastavování pravidel pro připojování dalších zařízení nebo šifrování disků a USB klíčů.“

Marek Cisár
SOITRON
Systémový specialista





Výsledek

Citlivé údaje dnes zaměstnanec BAT nemůže posílat, kopírovat, tisknout nebo přenášet na USB disky, aniž by operaci zaznamenal a vyhodnotil systém Safetica DLP.

Data jsou jasně roztříděná a pracuje se s nimi pod přísným dozorem podle přesně vymezených pravidel. Tak, aby byli chráněni zákazníci, zaměstnanci a také důvěryhodnost značky Bratislavská teplárenská.

IT tým BAT i management společnosti navíc získaly ucelený přehled o tom, jak se s citlivými údaji ve firmě zachází, odkud přicházejí, kdo a jak s nimi pracuje a kam je posílá. Díky tomu je možné přijímat další opatření a měnit klasifikace nebo zásady.

BAT získala i mnohem lepší představu o hodnotě firemních aplikací podle toho, jak intenzivně a k jakým operacím se využívají.



Bratislavská teplárenská, a.s.

Bratislavská teplárenská, a.s. (BAT) se zabývá hlavně výrobou tepla, výrobou silové a regulační elektřiny, výkupem tepla, rozvodem tepla a rozvodem elektřiny. V procesu kombinované výroby elektřiny a tepla zajišťuje hospodárné provozování soustav centralizovaného zásobování teplem (CZT). Zajišťuje dodávku tepla pro vytápění

a přípravu teplé užitkové vody v převážně většině bytových objektů, administrativních, zdravotních, kulturních, školských a sportovních zařízení ve správě odběratelských organizací i dodávku tepla pro průmyslové odběratele. V současnosti pokrývá přibližně 55 % potřeby tepla v hlavním městě.

www.batas.sk

SOITRON, s.r.o., member of SOITRON Group

Soitron is a Central European integrator operating in the IT market since 1991. The company's philosophy is to constantly move forward, and that is why it is a leader in implementing unique technologies and innovative solutions. It offers its clients products and services in the field of robotization and process automation, artificial intelligence, the Internet of Things (IoT), IT infrastructure, communication and cloud solutions, IT security, IT services and outsourcing, IT advisory and applications, and IT department digitalization. Its product portfolio includes smart police car solutions – Mosy and cyber security services – Void Security Operations Center. Soitron, s.r.o. is a part of the Soitron Group and employs more than 800 international experts. The group brings together professional teams in Slovakia, the Czech Republic, Romania, Turkey, Bulgaria, Poland, and the UK.