CHRÁNIME VAŠE HODNOTY

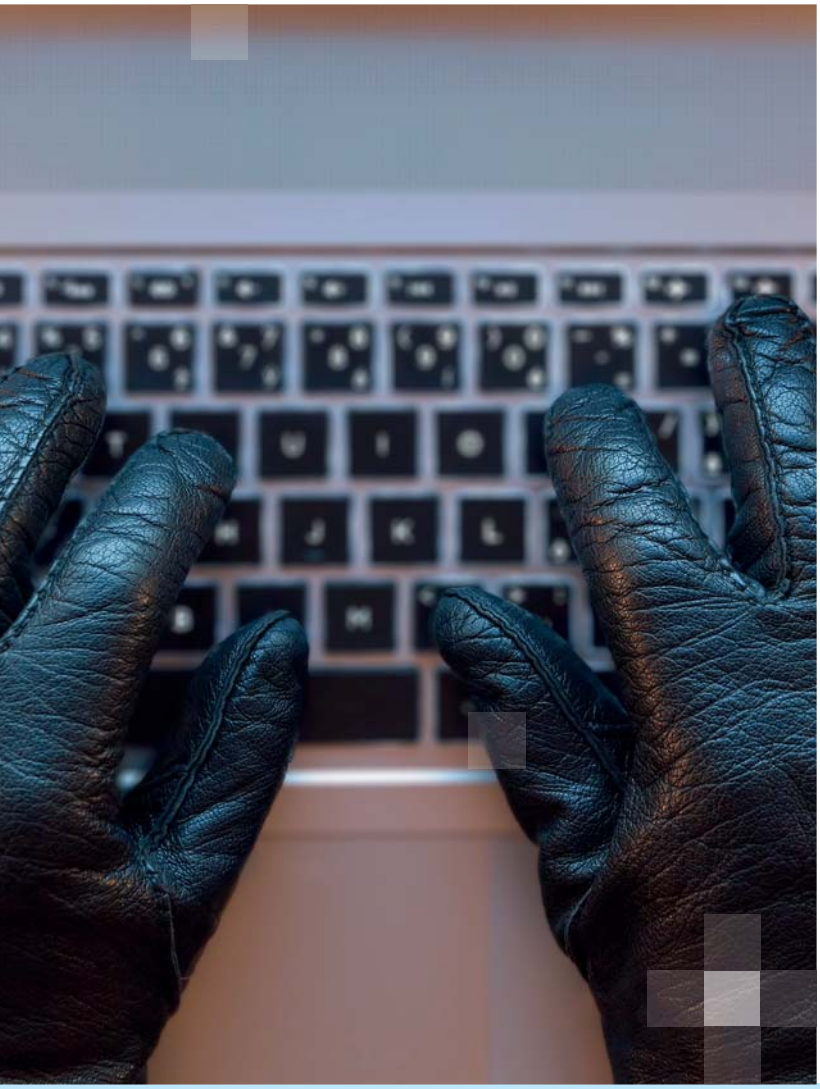
Prípadová štúdia

Implementácia DLP systému pomohla banke minimalizovať možnosti úniku dôverných dát

Implementácia riešenia
na prevenciu úniku dát

Požiadavky zákazníka

U zákazníka z finančného sektora bola identifikovaná potreba v oblasti informačnej bezpečnosti implementovať riešenie na monitorovanie, detekciu a blokovanie úniku citlivých dát a informácií prenášaných formou webovej prevádzky t. j. prostredníctvom webových služieb.



Pôvodný stav

Dôležitou a podstatnou fázou implementácie riešenie prevencie úniku dát je fáza analýzy, nakoľko jej výstupom je poskytnutie informácií o možnostiach implementácie riešenia a ďalších nevyhnutných a podstatných informácií pre samotnú implementáciu. Z analýzy základných informácií od zákazníka o ich IT infraštruktúre vyplynulo, že zákazník mal vo svojom prostredí pôvodne už implementovanú a využívanú webovú bezpečnostnú bránu, avšak bez funkcionality prevencie úniku dát pre webovú prevádzku – Web DLP. Podpora rozšírenia riešenia daného existujúceho produktu webovej bezpečnostnej brány o funkcionalitu Web DLP bola overená s jej výrobcom. Výrobcom bola táto podpora jednoznačne deklarovaná. Následne bola v spolupráci so zamestnancami zákazníka zodpovednými za informačnú bezpečnosť uskutočnená analýza a vyšpecifikovanie typov a rozsahu informácií, ktoré by mali byť rozširujúcou funkcionalitou Web DLP monitorované. Na základe toho bolo vykonané posúdenie, či v tej dobe už využívaná hardwarová konfigurácia webovej bezpečnostnej brány, t. j. technické vybavenie zákazníka, bude kapacitne postačovať zvýšeným nárokom rozšírenia funkcionalít Web DLP, alebo bude potrebné do implementácie zahrnúť taktiež zmeny hardwarovej konfigurácie. Výsledkom posúdenia bolo, že hardwarová konfigurácia spĺňala kapacitné požiadavky definované výrobcom riešenia. Po úspešnom ukončení tejto fázy bola zákazníkovi vypracovaná ponuka na implementáciu riešenia.

„Spolupráca so zákazníkom bola počas realizácie celého projektu vynikajúca. Zamestnanci zákazníka plnili svoje úlohy zodpovedne, k celému projektu pristupovali proaktívne. Pri riešení problémov, ktoré pri realizácii komplexného a zložitého projektu, akým implementácia webového filtra a DLP nesporne je, poskytovali potrebnú súčinnosť.
Výsledkom spolupráce bolo dokončenie projektu načas a k spokojnosti zákazníka.“

Ing. František Boda
vedúci projektu za spoločnosť EMM

Implementácia riešenia

Implementácia riešenia zahŕňala rozšírenie existujúcej webovej bezpečnostnej brány o funkcionalitu prevencie úniku dát pre webovú prevádzku, t. j. pre dáta prenášané prostredníctvom webových služieb (Web DLP) cez webovú bezpečnostnú bránu.

Výsledkom už skôr vykonanej fázy analýzy a špecifikácie typov a rozsahu chránených informácií boli nasledovné príklady typov citlivých údajov, ktorých výskyt v prenosoch dát prostredníctvom webových služieb bol zahrnutý do monitorovania:

- rodné čísla osôb
- čísla účtov
- niektoré technické informácie súvisiace s IKT
- údaje relevantné podľa štandardu Payment Card Industry Data Security Standard (PCI DSS)
- špecifikované súbory
- a iné

Po úspešnej inštalácii potrebných súčastí riešenia bolo možné pristúpiť následne k procesu konfigurácie riešenia, ktorého súčasťou boli aj nasledovné:

- integrácia s IT infraštruktúrou, t. j. napr. so servermi adresárov používateľov, emailovým serverom a s riešením SIEM
- nastavenie klasifikácie citlivých údajov vrátane nastavenia fingerprintovania špecifikovaných súborov, t. j. ich monitorovania pomocou „odtlačkov“ súborov
- vytvorenie politík, t. j. systému bezpečnostných pravidiel pre monitorovanie, detekciu alebo blokovanie úniku citlivých dát alebo dokumentov obsahujúcich citlivé dáta
- nastavenie notifikácií a reportovania
- nastavenie plánu zálohovania

Celý proces implementácie Web DLP riešenia bol ukončený poslednou fázou, kedy bolo implementované riešenie vyladené, otestované a následne odovzdané do správy zákazníka.

Súčasťou ponuky vypracovanej zákazníkovi a taktiež súčasťou dodaného riešenia bolo zároveň aj nasledovné:

- upgrade pôvodných licencií pôvodného produktu webovej bezpečnostnej brány na požadované licencie produktu s funkcionalitou Web DLP na viac rokov
- optimálny program technickej podpory výrobcu s možnosťou dodávateľa riešenia kontaktovať technickú podporu výrobcu a komunikovať so špecialistami technickej podpory výrobcu v zastúpení zákazníka
- zaškolenie personálu zákazníka

„Spolupráca s dodávateľskou spoločnosťou bola počas projektu nasadenia DLP riešenia na webový komunikačný kanál na vysokej odbornej úrovni. Zástupcovia dodávateľa vykonali analýzu našich potrieb, na základe ktorej navrhli vhodný postup implementácie a konfigurácie jednotlivých bezpečnostných politík a ďalších parametrov. Ak sa počas ktorejkoľvek fázy projektu vyskytli problematické skutočnosti, tieto riešili priamo s technickým personálom výrobcu. V spolupráci s nimi sa nám podarilo uviesť do produkčného používania funkčné a udržateľné DLP riešenie.“

Vedúci projektu za zákazníka

Zhrnutie výsledkov

Implementáciou DLP riešenia sa v prostredí banky podstatným spôsobom zredukuje šírenie citlivých údajov naprieč datacentrami, klientskými systémami, pobočkami a zariadeniami koncových používateľov. Zároveň bude možné identifikovať toky týchto údajov, čo umožní nastavenie biznis procesov spôsobom, aby lepšie zohľadňovali potrebu ochrany citlivých údajov pred ich zneužitím, či stratou. Ďalším benefitom bude taktiež monitorovanie a ochrana komunikácie s citlivým obsahom smerom na verejné webstránky. Dosiahnutie týchto cieľov bude možné realizovať pomocou definovania jednotných a univerzálnych politík v rámci DLP riešenia, naprieč celou IT infraštruktúrou banky.

Čo prináša DLP riešenie

Ochrana citlivých dát je v súčasnosti dôležitou témou a odcudzenie alebo únik citlivých dát môže mať nepriaznivé následky pre ďalšie fungovanie spoločnosti, vrátane následkov vyplývajúcich z platnej legislatívy.

Riešenie prevencie úniku dát, t. j. DLP riešenie poskytuje možnosti monitorovania, detekcie alebo blokovania potenciálneho úniku citlivých dát a informácií. Informácie o výskyte takýchto zaznamenaných udalostí umožňuje sprístupňovať a uchovávať, čím zároveň umožňuje adekvátne na takéto udalosti reagovať a prijať vhodné opatrenia.

DLP riešenia môžu okrem toho poskytovať:

- vyhľadávanie citlivých dát na dátových úložiskách a koncových staniciach
- monitorovanie citlivých dát v dátovej komunikácii
- uplatňovanie politík na aktivity vykonávané s citlivými dátami na koncových staniciach
- analyzovanie obrázkov a PDF súborov s využitím optického rozoznávania znakov (optical character recognition - OCR)

CHRÁNIME VAŠE HODNOTY

ISO 14001

ISO 9001

ISO/IEC 27001

EMM, spol. s r. o., Sekurisova 16, 841 02 Bratislava 42
tel +421 2 602 54 111, fax +421 2 602 54 901

www.emm.sk