Případová studie: implementace DLP v České průmyslové zdravotní pojišťovně

Data security management | 27.6.2019 | Rubrika: DLP | Strana: 38 |
Autor: Matej Zachar | Téma: Masarykova univerzita, vysoké školy

Data Loss Prevention (DLP) případová studie ochrana dat

O implementacích Data Loss Prevention systémů neexistuje velké množství článků a případových studií1. Tyto produkty historicky dominovaly pouze ve větších organizacích významně regulovaných segmentů, jako jsou např. finanční instituce. S rozšiřováním legislativních požadavků a povědomí o ochraně dat se však dostávají i do menších a středních organizací všech typů. V rámci této případové studie představíme jeden konkrétní projekt implementace Data Loss Prevention řešení, a to v prostředí České průmyslové zdravotní pojišťovny.

Úvod

Technologie se neustále posouvají kupředu, a tak se rozvíjejí i způsoby, jak mohou uživatelé pracovat s daty a sdílet je. Pro zefektivnění pracovních postupů dávají firmy uživatelům daleko větší prostor využívat různé aplikace a služby, na které jsou zvyklí. Mezi stávající firemní infrastrukturou a technologiemi pro práci s daty tak vzniká bezpečnostní vakuum.

1 Jedním z mála je článek „Technologie DLP a její současné limity“ od Pavla Krátkého, který byl publikován v DSM 4/2018.

S odpovědí na tuto problematiku přišly produkty Data Loss Prevention (DLP). Ty dokážou auditovat tok informací v rámci organizace a jednotlivé kanály toku dat pak řídit – např. upozorněním uživatele na neoprávněnou akci nebo úplným zamítnutím operace. Díky tomu DLP systémy pomáhají usměrnit toky dat uvnitř organizace i mimo ni.
DLP systémy jsou specifická řešení, která pomocí bezpečnostních pravidel-politik chrání data na základě obsahu souborů (content) nebo jejich původu (context). Může jít o hardwarové appliance, softwarového klienta nebo jejich kombinaci. Zpravidla dochází k označení-klasifikaci dat, nad nimiž jsou uplatněny zmíněné politiky, nebo jsou data označena na principu dynamického prohledávání citlivých informací uvnitř souborů a v obsahu komunikace.

DLP v České průmyslové zdravotní pojišťovně

Česká průmyslová zdravotní pojišťovna (dále jen „ČPZP“ nebo „zákazník“), o které se více dočtete v Boxu 1, trvale zvyšuje informační a datovou bezpečnost. Jedním z projektů zabezpečení dat byl i projekt nasazení systému DLP.
Pro implementaci DLP v České průmyslové zdravotní pojišťovně byla použita technologie Safetica DLP2. Ta je příkladem architektury softwarového klienta, který se instaluje na koncové stanice a následně připojí na serverovou komponentu, viz Obr. 1. Safetica DLP umožňuje provádět jak datový audit, tak řídit bezpečnostní politiky a hlásit pokusy o jejich porušení prostřednictvím upozornění (alertů) a pravidelných reportů.
Cílem bylo vytvořit bezpečný perimetr, tedy pracovní prostředí takové, ve kterém mohou uživatelé volně pracovat a data se mohou volně pohybovat. Pokud by data měla tento perimetr opustit, systém zasáhne dle nastavených politik a přenos citlivých dat zastaví, omezí nebo v odůvodněných případech povolí s upozorněním a logováním dané operace. Automatizovaným varováním pak bude pověřený správce obeznámen s probíhajícím incidentem nebo pokusem o něj.

Implementace DLP

Implementace DLP se dá obecně rozdělit do několika logických celků, které na sebe plynule navazují. Těmito celky jsou: Proof of Concept (POC) – volitelný, Instalace, Monitorovací období, Konfigurace a Akceptace. Během všech fází dochází k úzké spolupráci s bezpečnostními specialisty zákazníka

včetně jejich postupného proškolení.
Před aplikováním jakýchkoli bezpečnostních politik, které budou upevňovat procesy organizace pro práci s daty, se implementace zaměřuje na analyzování datové bezpečnosti ve společnosti. Ta je zahájena instalací a následnou dobou automatizovaného sběru informací o prostředí produktem (v rámci tzv. Monitorovacího období).
Před započetím monitorovacího období byla tedy provedena distribuce agentů na vybrané stanice. Ty umožňují získat dostatečné informace pro vypracování analýzy stavu bezpečnosti v rámci organizace. Jakmile byl systém na koncových stanicích nainstalován a stanice začaly posílat první data, bylo stanoveno předpokládané ukončení monitorovacího období – dle výchozí hodnoty jednoho měsíce. Během této doby probíhala klasifikace a definice parametrů vlastních konkrétnímu prostředí. Identifikovaly se mimo jiné interní systémy organizace, místa, kde se nacházejí citlivá data, a typ informací, které proudí v rámci organizace.
Na základě získaných dat byla následně vypracována bezpečnostní analýza, jež reflektovala reálné využívání zdrojů pro práci s daty ve společnosti. V návaznosti na výsledky obsahovala i konkrétní doporučení, jak je nálezy možné optimalizovat či vyřešit.
Výsledná zpráva byla zákazníkovi prezentována a jednotlivé problematiky dle potřeby rozvedeny. Pokud nemá zákazník jasně definované cíle již od počátku projektu implementace DLP, může tato zpráva sloužit jako jejich základ. V případě ČPZP šlo pouze o doplnění dopředu definovaných potřeb a politik.
Nejdůležitějšími scénáři pro zákazníka byly ochrana exportů z aplikace příjmové a finanční části v prostředí Microsoft Dynamics NAV (dále jen „MD NAV“) a ochrana exportů z aplikace výdajové části v interní webové aplikaci běžící v prostředí JAVA (dále jen „WebApp“). Tyto dvě aplikace obsahují citlivá data společnosti. Dále je možno označit i další soubory s citlivým obsahem, a to přímo dle interních pravidel pro uživatele informačního systému.
Zákazníkem byla definována jednotlivá pravidla a požadavky na restrikce při definování bezpečného perimetru, varování a reporty tak, aby prostředí zákazníka bylo pečlivě chráněno napříč všemi koncovými stanicemi.
Na základě bezpečnostní analýzy a požadavků zákazníka se tedy stala hlavním cílem ochrana dat ze systémů MD NAV a WebApp. U těchto systémů bylo zapotřebí pokrýt tři oblasti, kde uživatel mohl přijít do kontaktu s citlivými daty. Těmito oblastmi jsou: 1. práce v aplikaci, kopírování dat, obrazovek apod.
2. vytvoření výstupu z aplikace, jehož výsledkem je soubor 3. již existující soubory pocházející z těchto systémů na konkrétních souborových systémech Bez nasazení DLP systému je obecně možné používat operace, které mohou vést k cílenému zcizení či vyzrazení dat nebo ztrátě dat z prosté lidské nevědomosti. Mezi nejkritičtější operace se ze zkušenosti řadí schránka, snímek obrazovky, tisk. Zákazníkovi bylo doporučeno definovat, které z operací by měly být uživatelům povoleny na základě procesů prováděných s daty.
Druhou oblastí byla ochrana dat, jež jsou výstupem z těchto aplikací. Zde bylo doporučeno zabezpečení za pomoci klasifikační technologie, která výstupy aplikace automaticky značí jako citlivé. Posledním cílem v rámci zajištění citlivých dat byla klasifikace již existujících nebo nově tvořených souborů na stanicích uživatelů, pro které se definoval konkrétní adresář.

Konfigurace DLP pravidel

Implementace byla zahájena definováním a vytvořením několika datových kategorií, kde každá reprezentovala konkrétní systém/cílové úložiště, kde se citlivá data nacházejí.
Při tvorbě pravidel pro jednotlivé datové kategorie byla vytvořena tzv. zóna, která definuje bezpečný perimetr pro práci s daty. Zóna může obsahovat mj. konkrétní externí zařízení, tiskárny, e-mailové adresy či domény a jakékoli další cesty, které se běžně používají pro přenos dat.
K ověřování stanovených pravidel byla využita možnost nastavení režimu testovacích politik. V praxi to znamenalo, že veškerá pravidla v prostředí bylo možné otestovat bez jakéhokoli omezení koncového uživatele. Politiky se průběžně vyhodnocovaly a na základě logů bylo možné je následně upravit.
Doposud nastavené politiky pokryly část výstupů z aplikace a již existují data v konkrétních adresářích. Zbývalo nastavit pravidla pro používání operací v rámci aplikace bez jakékoli návaznosti na značená data, reportovací a alertovací systém.

Ať už v případě reportů ze systému DLP i alertů bylo primární zaměření na datové operace uživatelů, které mohou potenciálně směřovat k úniku dat.
Součástí implementace a ladění byla následná optimalizace prostředí na koncových stanicích uživatelů. Kromě nastavení politik a definování skupin uživatelů se jednalo o texty, umístění, frekvenci a dobu viditelnosti oznamovacích oken. Při implementaci bylo nutno dále upravit jak systém Safetica, tak systémová nastavení koncových stanic, prohlížečů a tiskových ovladačů pro doladění problémů, které se v souvislosti s nasazením DLP objevovaly na koncových stanicích.
Nastavení konfigurace prošla několika režimy, které byly postupně hodnoceny a teprve po schválení oběma stranami doručeny na koncové stanice postupnými vlnami nasazení.
1. Režim testovací (logovací) sbíral k označeným citlivým souborům pouze technické logy, které byly vzápětí vyhodnocovány technikem a konzultovány se zákazníkem.
2. Režim edukativní a informativní, který vyšel z předchozího režimu, již uživatele informoval o práci s citlivými soubory, ale žádná z operací nebyla zakázána. Zde došlo k evaluaci s uživateli samotnými, kteří poskytli zpětnou vazbu na chování v prostředí koncových stanic. Tato zpětná vazba byla v několika vlnách zapracována do drobných změn v nastavení.
3. Režim restriktivní, který již operace blokuje, se aplikoval u nejvíce citlivých souborů a vycházel přímo z konfigurace v režimu informativním.
Uživatelé také dostali k dispozici vzor nastavení, který popisoval, jaká ochrana je pro daný typ operace s daty použita. Díky transparentní komunikaci se zaměstnanci již v průběhu implementace došlo k lepšímu přijetí systému uživateli a k efektivnímu nasazení pravidel.

Závěr

Rozhodující pro úspěšnou implementaci je zvolit na základě analýz toku dat a taky na základě posouzení charakteru práce jednotlivých pracovišť zákazníka správné nastavení bezpečnostních pravidel-politik a konfigurací. Ty mohou být odlišné i pro jednotlivá pracoviště zákazníka (skupiny uživatelů). Je potřeba vhodně zařadit jednotlivé aktivity do kategorií: povolená, povolená s upozorněním na riziko a zakázaná. Systém musí přinášet zvýšení bezpečnosti, ale je třeba taky ohlídat, aby nedocházelo k přílišnému omezení samotné práce uvnitř organizace. Tedy nastavit co nejjednodušší systém upozorňování a restrikcí v souladu s potřebami zabezpečení informací a co nejméně ovlivnit regulérní pracovní postupy. Dobrá ergonomie systému, bezpečnostní povědomí všech zaměstnanců zákazníka a podpora top managementu jsou klíčové pro úspěšnou implementaci. Žádný systém, ani ten sebelepší, nezabrání stoprocentně zneužití dat, může vždy využít jen možností daných technikou. Nasazení DLP systému musí jít vždy ruku v ruce s dalšími opatřeními, jako je interní stanovení odpovědností zaměstnanců, edukace v oblasti kyberbezpečnosti atp.
Implementace probíhala díky skvělé součinnosti zákazníka hladce a svižně. Z článku je patrné, že řešení DLP je zpravidla řešením na míru, nelze tedy vždy použít naprosto stejné postupy. Naopak je možné přizpůsobit existující doporučení pro konkrétní prostředí tak, aby zůstal zachován plynulý tok dat i práce uživatelů uvnitř bezpečného perimetru, a zároveň byla chráněna citlivá data při pokusu je přenést mimo tento perimetr.

Česká průmyslová zdravotní pojišťovna BOX 1 ČPZP zajišťuje svým klientům zdravotní služby přes 25 let. Během své historie se sloučila s několika jinými zdravotními pojišťovnami a v současné době zajišťuje lékařskou péči 1,25 mil. pojištěnců. Za léčbu svého nejnákladnějšího pacienta uhradila ČPZP v loňském roce přes 50 mil. Kč. ČPZP má uzavřeny smlouvy s více než 25 500 ordinacemi, nemocnicemi a dalšími poskytovateli zdravotních služeb. Díky tomu mají pojištěnci jistotu lékařského ošetření, kdekoli ho budou potřebovat. Celkem na zdravotní služby ČPZP vynaložila v roce 2018 cca 30,5 mld. Kč. ČPZP je k dispozici svým klientům na 109 pobočkách po celé ČR a zaměstnává 650 zaměstnanců. Samozřejmostí je zabezpečená elektronická komunikace s pojištěnci a partnery přes portál ČPZP, vlastní mobilní aplikace a Infocentrum.

2 Více informací lze nalézt na webových stránkách https://www.safetica.cz. Mgr. Matej Zachar, CISSP Pracuje na pozici Chief Security Officer ve společnosti Safetica Technologies. Mezi jeho hlavní priority patří řízení strategických projektů, interní bezpečnosti a shoda s požadavky zákonů (regulatory compliance). Vystudoval informační bezpečnost na **Fakultě informatiky** Masarykovy univerzity v Brně a v oboru působí již osmým rokem.

Foto popis| Obr. 1: Architektura DLP

O autorovi| Matej Zachar, matej.zachar@safetica.com Speciální poděkování patří týmu informační bezpečnosti společnosti Česká průmyslová zdravotní pojišťovna, zejména Ing. Leovi Večerkovi.