Monitoring kybernetické bezpečnosti

18.1.2022 - | INFOPROFI GROUP s.r.o.

Nástroj určený pro bezpečnostní monitoring - Data Lost Prevention/Protection (DLP).

Jak je z názvu patrné, jedná se o nástroj primárně určený pro identifikaci a ochranu citlivých dat před jejich zcizením, ztrátou nebo vyzrazením vlivem chyby. Tentokrát ovšem nikoliv ze strany externího útočníka, ale z řad vlastních zaměstnanců. Ať už se na problematiku kybernetické bezpečnosti podíváme z jakéhokoliv pohledu, zaměstnanec vždy představuje jedno z největších bezpečnostních rizik. Od přírody jsme omylní a jsme nastavení tak, že pro nás vždy volíme nejsnazší cestu. K bezpečnostnímu incidentu ze strany zaměstnanců dochází nejčastěji z důvodů neznalosti, chybovosti nebo obcházení bezpečnostních politik. Všechny případy však vedou k výše zmíněné ztrátě dat.

DLP je vhodné pro společnosti, které vlastní informace, jejichž charakter splňuje definici citlivých, a tudíž neveřejných informací. Může se jednat o osobní data zákazníků, výrobní know-how nebo jakékoliv jiné neveřejné či utajované informace, jejichž ztráta by společnost ohrozila reputačně nebo ekonomicky, případně by přivodila sankce za porušení legislativních nařízení.

Co je DLP?

DLP monitoruje pohyb dat a chování uživatelů na koncových stanicích a serverech. Není tomu tak dávno, kdy se zejména jednalo o řešení provozovaná na infrastruktuře dané organizace. Dnes není výjimkou, že řada vendorů poskytuje DLP jako službu, a to včetně integrace do cloudu a napojení na služby, jako jsou Microsoft 365. Stává se to spíše standardem.

Součástí většiny z nich je i pokročilý monitoring chování uživatelů, který pomáhá v dokreslení situace a umožnuje vyhodnocovat dění v organizaci v širších souvislostech. Jsou to především

informace o způsobu využívání aplikací, přístupy k webovým stránkám a další oblasti činností uživatele, které bývají doplněny o vyhodnocení efektivity. Jedná se mocné nástroje, které poskytují podrobné informace o chování zaměstnanců. To je také důvodem, proč DLP patří mezi nejhůře prosaditelná řešení v oblasti bezpečnostního monitoringu. Jeho nedílnou součástí je i restriktivní část postavená na pravidlech, která brání uživateli nakládat s citlivými dokumenty v rozporu s bezpečnostní politikou organizace.

Na druhou stranu, výstupy z DLP poskytují oddělení bezpečnosti podrobné informace o pohybu citlivých dat a nakládání s nimi. V rámci bezpečnostního dohledu se jedná o další cenný zdroj logových informací.

Jak DLP funguje?

Základní rozdělení DLP je na kontextová a kontentová řešení. Následně dle principu, jak se definují bezpečnostní politiky, na rule based a řešení využívající strojového učení. Klasická DLP jsou postavena na tvrdých pravidlech definovaných administrátorem tzn. rule based řešení. Monitoring činnosti uživatele probíhá prostřednictvím instalovaného agenta na koncovém zařízení, který zároveň zajišťuje restrikce. Integrace s operačním systémem je velmi úzká a DLP jej zásadním způsobem ovlivňuje, což může mít dopad na celkový výkon systému, a to v závislosti na nastavených detekcích. V následující části se zaměříme na oba typy řešení DLP.

Kontextová DLP jsou postavená na sledování pohybu dat vně organizace/systému. Snaží se hledat kontext a neřeší samotný obsah dokumentů. Typickým příkladem je sledování složky uložené na interním file serveru. Přístup zaměstnance je zaznamenán včetně kompletní informace k jakému dokumentu přistupuje. Při pokusu o jeho vynesení z organizace (USB, E-mail, IM, upload na WWW) je vygenerován alert, nebo je daná operace zakázána.

Výhodou kontextového řešení je snazší implementace v rámci organizace a menší nároky na výkon koncových zařízení. Nevýhodou je možnost sledovat pohyb pouze zvenčí.

Kontentová DLP řeší i obsah dat. Umožnují v datech vyhledávat citlivé informace, jako jsou různé osobní údaje, klíčová slova nebo složitější výrazy. Následně je již princip stejný, jako u kontextového DLP, tedy při porušení stanovené politiky je akce zaznamenána či rovnou zablokována.

Velmi důležitá je schopnost provést audit citlivých dat a jejich označení (tagování). Kvalita této funkce by měla být rozhodujícím parametrem při výběru vhodného řešení. Kvalitní klasifikace dat je kamenem úrazu v mnohých společnostech, bez ní však nelze DLP kvalitně naimplementovat a úspěšně provozovat. Těžko budete kontrolovat něco, co je všude a co nejste schopni identifikovat. Schopnost označení citlivých dat naopak zásadně ovlivňuje vynucování restrikcí. Značka je součástí daného datového souboru a obsahuje informace o jeho citlivosti a povolených způsobech zacházení např. zda tento soubor smí být uložen mimo vyznačené úložiště nebo zaslán na externí e-mail či uložen na výměnné zařízení.

Z výše uvedeného je zřejmé, že kvalitní implementaci není možné provést pouze v několika pracovních dnech. V rámci větších organizací se jedná o horizont několika měsíců. Dále je nutné si uvědomit, že podstatná část práce je procesní a promítá se do bezpečnostních politik, nejedná se pouze o nasazení na zařízení jednotlivých uživatelů.

Vzhledem k náročnosti konfigurace jednotlivých pravidel (není myšleno klikání v produktu, ale namapování na procesy organizace) se vývoj vendorů upíná směrem ke strojovému učení a automatizaci pravidel na základě vyhodnocení předchozího chování uživatelů. Viz rozdělení dle způsobu uplatňování bezpečnostních politik výše. Pěkným příkladem rozdílu je sledování pohybu dat

na externích zařízeních, kdy je sledován způsob používání zařízení uživatelem. V klasickém DLP administrátor vytváří pravidla definující firemní externí zařízení a nastavuje hraniční hodnotu např. na množství uložených citlivých dat, nebo množství osobních údajů, které obsahují. Nevýhodou je detekce závislá na osobním pocitu podpořená zkušeností a znalostí organizace.

DLP používající metod strojového učení sleduje uživatele v delším časovém horizontu a zohledňuje množství parametrů jako je typ zařízení, četnost používání, objemy dat, typy dat, množství údajů a čas, kdy uživatel danou operaci provedl. V případě, že se uživatel odchyluje od obvyklého chování, systém generuje alert. Odpadají tak pevná pravidla, která lze znalým uživatelem obcházet, tento však není schopen se pohybovat pod úrovní nastavených pravidel. Nevýhodou je nemožnost úpravy automatizovaných pravidel obsluhou a závislost na kvalitě detekcí dodaných výrobcem.

Závěrem. V rámci implementace DLP je nutné kvalitně odpracovat všechny části projektu, od klasifikace dat, přes technický návrh až po procesní rovinu. V opačném případě systém slouží jako nástroj sledování činnosti uživatelů na webových stránkách a z pohledu bezpečnostního monitoringu je bezcenný.

DLP v rámci bezpečnostního dohledu zdaleka nevyžaduje takové lidské zdroje jako EDR, na druhé straně je náročnější v oblasti implementace. DLP je vhodné zejména pro organizace nakládající s citlivými daty. Dále již neplatí, že DLP je nástroj vhodný pro velké korporátní společnosti. Z pohledu bezpečnostního dohledového centra se jedná o další zdroj dat, který zapadá do konceptu komplexního bezpečnostního monitoringu.

Mgr. Jan Kozák, Projektový manažer ve společnosti AXENTA a.s.