DLP –РІШЕННЯ ДЛЯ ЗАПОБІГАННЯ ВИТОКУ ДАНИХ В ОРГАНІЗАЦІЯХ

А.Ю. Вакула
м. Одеса, Одеський національний економічний університет

Витоки/втрати інформації підривають авторитет компаній і несуть величезні збитки. За даними аналітиків, у найближчі роки корпоративний сектор буде нести втрати приблизно в $1 трлн. щорічно внаслідок витоку конфіденційних даних. "Навіть великі і добре захищені міжнародні конгломерати можуть постраждати від комп'ютерного шпигунства", - йдеться в дослідженні міжнародної антивірусної інтернет-компанії McAfee. Співробітник може умисно або з необережності роздрукувати конфіденційну інформацію, надіслати її на особистий ящик електронної пошти, форум, чат і т. д [1].

Одним з ефективних заходів по запобіганню витоку даних є використання DLP-рішень (Data Loss/Leakage Prevention — запобігання втрат/витоків даних). Для передумов до запровадження DLP-систем можна виділити наступне.

По-перше, на першому місці стоїть еволюційний розвиток/стратегія систем забезпечення інформаційної безпеки (ІБ) в компанії. Адже основне завдання подібних систем - запобігання витоків інформації, засноване на чіткому розумінні критеріїв конфіденційності (класифікації), що є обов'язковою умовою перед впровадженням.

По-друге, серед передумов до впровадження, варто мати усвідомлене рішення організації, яке ґрунтується на розумінні того, які ймовірні збитки може викликати втрата тієї або іншої інформації.

По-третє, впровадження може бути викликано вимогами національних та/або галузевих регуляторів, що просто необхідно для легітимного надання компанією тих чи інших сервісів

Одним з головних аспектів вибору і впровадження DLP-системи є її сумісність з принципами і вимогами роботи всієї організації. Всю інформацію, наявну в мережі можна розділити на кілька типів [2]:

- не класифікована;

- загальнодоступна інформація;
- конфіденційна, але не критична;
- строго конфіденційна інформація.

Глобальна концепція DLP розглядає інформаційну систему з точки зору трьох напрямків регулювання [3], для кожного з яких існує окрема компонента в системі:

- По-перше, в області контролю передачі інформації по каналах електронної пошти та Web (data-in-motion).
- По-друге, у сфері контролю над операціями з конфіденційною інформацією на рівні робочої станції, контроль даних, якими оперують користувачі локально, а саме: за допомогою USB-носіїв, друкування на принтері, запису даних на CD/DVD (data-in-use).
- Нарешті, у сфері сканування мережевих ресурсів для виявлення місць її зберігання: робота з загальним для великої кількості користувачів ресурсом і організація сегментованого (заснованого на правилах) доступу до нього (data-at-rest).

У системах DLP застосовуються складні механізми аналізу: порівняння за шаблонами з використанням словників і регулярних виразів, лінгвістичний та контекстний аналіз, цифрові відбитки. Словники та шаблони зручно застосовувати в конкретних областях, наприклад, для контролю номерів кредитних карт та інших персональних даних.

Ключове завдання DLP забезпечити саме поширення процесів і принципів ІБ. Таким чином, для організації та управління всією системою, адміністраторам достатньо створити єдиний шаблон, який поширюється на всі три компоненти ІБ, замість того щоб робити безліч різних шаблонів для різних потенційно небезпечних систем. Це дуже важливо, так як ймовірність щось пропустити зростає експоненціально по відношенню до кількості систем. В цілому DLP значно спрощує керування ІБ.

За словами представників фірм-розробників, представлені на сьогоднішній день DLP-рішення мають приблизно однакові функції, розрізняючись лише вимогами до апаратної частини, логікою внутрішньої роботи, складністю установки і експлуатації, а також ціною і політикою ліцензування.

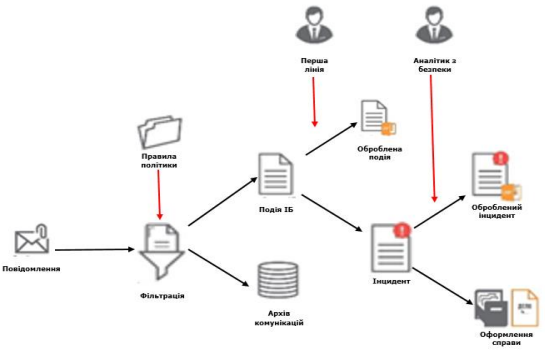

Рис.1. Принцип роботи DLP – системи

Основними продуктами на ринку DLP-систем є наступні[4]: Symantec; Digital Guardian; Force point; Intel Security; RSA; Check point; NFOWATCH; NREND MICRO; Websense; McAfee; CA Technologies; InfoWatch; SecurIT Zgate; SecurIT Zlock; Дозор Джет.

Деякі компанії як, наприклад, Improvement Service [5] пропонують On-Line оцінку захищеності за напрямами: 1) тестування на порушення периметру інформаційних систем; 2) тестування інформаційних систем з позиції локального зловмисника. Об'єктами тестування можуть бути як інфраструктура в цілому, так і окремі системи та компоненти

Література

1. В.Мирошниченко, Д.Ходоров, Е.Щеглова DLP-решения: Как помешать торговле корпоративными секретами [Електронний ресурс] // Інвестгазета №14 10.05.2011 – Режим доступу: https://investgazeta.delo.ua/ praktika/dlp-reshenija-kak-pomeshat-tor-273582/
2. DLP-решения - информационная безопасность – Режим доступу: http://securitysoftline.ru
3. А. Прозоров ALL ABOUT DLP [Електронний ресурс] – Режим доступу: http ://bis-expert.ru/blog/ 2560/51911
4. https://Digitalguardian.com
5. www.pentest.com.ua