УДК 316.4

М. О. Берестенко

РОЗРОБКА ЗАХИЩЕНОГО ДОДАТКУ ОБРОБКИ КОНФІДЕНЦІЙНИХ ДАНИХ З ВИКОРИСТАННЯМ DLP-СИСТЕМИ

Вінницький національний технічний університет

Анотація

В даній роботі було описано захист інформації за допомогою DLP-систем, визначення розробки мобільних додатків, Data Loss Prevention(DLP), розробка та розгортання стратегії DLP, також те, що завдяки їй можна вирішити.

Ключові слова: *розробка мобільного додатку, Data Loss Prevention(DLP), стратегія DLP.*

Abstract

This paper describes the protection of information using DLP systems, the definition of mobile application development, Data Loss Prevention (DLP), the development and deployment of DLP strategy, as well as what it can solve.

Keywords*: mobile application development, Data Loss Prevention (DLP), DLP strategy.*

Вступ

Розробка мобільних додатків — це дія чи процес, за допомогою якого створюється застосунок для мобільних пристроїв, таких як персональні цифрові помічники, цифрові помічники підприємств або мобільні телефони. Ці програми можуть бути попередньо встановлені на телефонах під час виготовлення платформ або поставлятися у вигляді веб-додатків за допомогою обробки на стороні сервера або клієнта, щоб забезпечити «подібний до додатків» досвід роботи в веб-браузері. Розробники прикладного програмного забезпечення також повинні враховувати довгий масив розмірів екрана, технічних характеристик та конфігурацій через інтенсивну конкуренцію в мобільному програмному забезпеченні та зміни в межах кожної з платформ. Розвиток мобільних додатків постійно зростає, зростаючі доходи та робочі місця [1].

Запобігання втраті даних (DLP) - це набір інструментів та процесів, що використовуються для того, щоб несанкціоновані користувачі не втрачали, не використовували або не отримували до них доступ до конфіденційних даних. Програмне забезпечення DLP класифікує регульовані, конфіденційні та важливі для бізнесу дані та виявляє порушення політик, визначених організаціями або в межах заздалегідь визначеного пакета політик, як правило, внаслідок дотримання нормативних вимог, таких як HIPAA, PCI-DSS або GDPR.

Принцип роботи DLP-системи

Розпізнавання конфіденційної інформації в DLP-системах виробляється двома способами: аналізом формальних ознак (наприклад, грифу документа, спеціально введених міток, порівнянням хеш-функції) і аналізом контенту. Перший спосіб дозволяє уникнути помилкових спрацьовувань (помилок першого роду), але зате вимагає попередньої класифікації документів, впровадження міток, збору сигнатур і т. Д. Пропуски конфіденційної інформації (помилки другого роду) при цьому методі цілком вірогідні, якщо конфіденційний документ не піддався попередньої класифікації . Другий спосіб дає помилкові спрацьовування, зате дозволяє виявити пересилання конфіденційної інформації не тільки серед грифованих документів. У хороших DLP-системах обидва способи поєднуються.

До складу DLP-систем входять компоненти (модулі) мережевого рівня і компоненти рівня хоста. Мережеві компоненти контролюють трафік, що перетинає кордони інформаційної системи. Зазвичай вони стоять на проксі-серверах, серверах електронної пошти, а також у вигляді окремих серверів. Компоненти рівня хоста стоять зазвичай на персональних комп'ютерах працівників і контролюють такі канали, як запис інформації на компакт-диски, флеш-накопичувачі і т. д. Хостові компоненти також намагаються відслідковувати зміну параметрів мережі, інсталяцію програм для тунелювання,

стеганографії і інші можливі методи для обходу контролю. DLP-система повинна мати компоненти обох зазначених типів плюс модуль для централізованого управління.

Після виявлення цих порушень DLP здійснює виправлення за допомогою попереджень, шифрування та інших захисних дій, щоб запобігти випадковому або зловмисному обміну даними, які можуть поставити організацію під загрозу. Програмне забезпечення та засоби запобігання втраті даних контролюють і контролюють діяльність кінцевих точок, фільтрують потоки даних у корпоративних мережах і відстежують дані в хмарі для захисту даних у спокої, в русі та у використанні. DLP також надає звіти для задоволення вимог дотримання вимог та аудиту та виявлення зон слабкості та аномалій для криміналістики та реагування на інциденти.

Практично у всіх країнах охороняється законом право на таємницю зв'язку та право на таємницю приватного життя. Використання DLP-систем може суперечити місцевим законам в деяких режимах або вимагати особливого оформлення відносин між працівниками і роботодавцем. Тому при впровадженні DLP-системи необхідно залучати юриста на самому ранньому етапі проектування [2].

Кроки для розробки та розгортання стратегії запобігання втраті даних

Існує ряд основних заходів, які повинні відбуватися під час запуску програми запобігання втраті даних. Цей фреймворк містить загальні вказівки, яким повинна слідувати ваша стратегія DLP. Ці вимоги також можуть бути використані для вибору правильного рішення DLP для вашої організації.

1. Приоритетсність даних

Не всі дані є однаково важливими. Першим кроком у будь-якій програмі DLP є визначення, які дані викликали б найбільшу проблему, якщо їх викрали.

2. Класифікація даних

Класифікація даних часто розглядається як грізна проблема в DLP. Простий, масштабований підхід - класифікація за контекстом; пов’язування класифікації з вихідною програмою, сховищем даних або користувачем, який створив дані. Застосування стійких міток класифікації до даних дозволяє організаціям відстежувати їх використання[3].

3. Розуміння ризику даних

Шифрування та засоби захисту на основі мережі можуть забезпечити безпеку, коли дані перебувають у стані спокою всередині брандмауера. Що стосується даних, що розподіляються на пристрої користувачів або передаються партнерам, клієнтам та ланцюгу поставок, існують різні ризики. У цих випадках дані часто піддаються найбільшому ризику на момент використання в кінцевих точках. Прикладами є приєднання даних до електронної пошти або переміщення їх на знімний пристрій зберігання даних. Потужна програма запобігання втраті даних повинна враховувати мобільність даних та моменти, коли дані піддаються ризику.

4. Моніторинг руху всіх даних

Розуміння того, як дані використовуються, та виявлення існуючої поведінки, яка загрожує даним, є критично важливими.

5. Спілкування та розробка засобів контролю

Контроль використання даних може бути простим на початку ініціативи DLP, націлюючись на найбільш поширені ризиковані способи поведінки, одночасно отримуючи підтримку від лінійних менеджерів. У міру дозрівання програми запобігання втраті даних організації можуть розробляти більш детальний, тонко налаштований контроль для зменшення конкретних ризиків [4].

Питання які вирішує DLP

Запобігання втраті даних вирішує три основні цілі, які є спільними проблемами для багатьох організацій: захист / дотримання персональної інформації, захист інтелектуальної власності (ІВ) та видимість даних.

1. Захист / дотримання персональної інформації : Чи збирає та зберігає організація особисту інформацію (ІПІ), захищену медичну інформацію (ЗОЗ) або інформацію про платіжні картки (ПКІ)? Якщо так, то, швидше за все, організація підпадає під дію нормативних актів, таких як HIPAA (для PHI) та GDPR (для персональних даних резидентів ЄС), які вимагають від вас захисту конфіденційних даних ваших клієнтів. DLP може ідентифікувати, класифікувати та мітити конфіденційні дані та відстежувати дії та події навколо цих даних. Крім того, можливості звітності надають деталі, необхідні для аудиту відповідності.

2. Захист інтелектуальної власності. Чи має організація важливу інтелектуальну власність та комерційну чи державну таємницю, яка може поставити під загрозу фінансове здоров'я та імідж організації у разі втрати чи викрадення? Рішення DLP, такі як Digital Guardian, що використовують класифікацію на основі контексту, можуть класифікувати інтелектуальну власність як у структурованій, так і в неструктурованій формах. Завдяки застосованим політикам та елементам керування є можливим захистити організацію від небажаного проникнення цих даних.

3. Видимість даних: Організація прагне отримати додаткову видимість руху даних? Комплексне корпоративне рішення DLP може допомогти бачити та відстежувати дані в кінцевих точках, мережах та хмарі. Це забезпечить видимість того, як окремі користувачі організації взаємодіють із даними.

Хоча це три основні випадки використання, DLP може усунути безліч інших проблемних ситуацій, включаючи інсайдерські загрози, безпеку даних Office 365, аналіз поведінки користувачів, сутності та розширені загрози [5].

Висновки

З розвитком технологій поява передових кіберзагроз посилюється, що заважає конфіденційності та безпеці інформаційних систем

Незважаючи на те, що існує безліч методів безпеки, які можна запровадити для запобігання несанкціонованому доступу, важко з упевненістю сказати, які методи слід, а що не слід застосовувати, залежно від розміру та сфери діяльності.

Як показують опубліковані дані опитування Deloitte провідних світових фінансовий компаній, 49% респондентів зафіксували внутрішні інциденти (пов'язані з IT-безпекою). Організації, які постраждали від внутрішньої витоку, зізнаються, що велика частка загроз є наслідком недолугості або недбалості службовців (людський фактор - 42%, операційні помилки - 37%), а не злого умислу інсайдерів. Правда, 28% стали жертвою ретельно продуманого і професійного шахрайства, а 18% компаній втратили приватну інформацію клієнтів саме через те, що інсайдери цілеспрямовано допустили витік. Щоб не допустити такі інциденти в майбутньому, 80% опитаних фінансових компаній здійснюють моніторинг дій службовців, а 75% вводять різні обмежувальні заходи на використання тих чи інших технологій або пристроїв.

За даними дослідницького центру компанії InfoWatch, що спеціалізується на виробництві і продажу систем DLP, 42% витоків інформації відбувається ненавмисно по неакуратності або забудькуватості користувачів, внаслідок порушень політик корпоративної безпеки організацій. Більше 40% інформації йде по Інтернет-каналах, і 30% - по мобільних пристроях. Більше 65% інформації витікає з комерційних підприємств, близько 20% з освітніх і 24% з державних підприємств.

Системи DLP на сьогоднішній день найбільш ефективним інструментом для захисту конфіденційної інформації, і актуальність даного рішення буде з часом тільки збільшуватися.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Мобільний додаток для хворих на астму [Електронний ресурс]. – 2010. – Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/35614/1/Tomiko_bakalavr.pdf (дата звернення 25.03.2021).

2. THE CISO'S GUIDE TO DATA LOSS PREVENTION: DLP STRATEGY TIPS, QUICK WINS, AND MYTHS TO AVOID [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://digitalguardian.com/blog/cisos-guide-data-loss-prevention-dlp-strategy-tips-quick-wins-and-myths-avoid (дата звернення 25.03.2021).

3. Системы предотвращения утечек конфиденциальной информации (DLP) [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://studentlib.com/chitat/referat 230150 sistemy_predotvrascheniya_utechek_konfidencialnoy_informacii_dlp.html (дата звернення 25.03.2021).

4. Security Techniques for the Electronic Health Records [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5522514/ (дата звернення 25.03.2021).

5. SECURITY OF PERSONAL DATA [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf (дата звернення 25.03.2021).

Берестенко Михайло Олександрович*- студент групи Уб-17б,факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: mberestenko7@gmail.com;*

Berestenko Mykhailo *- student of the Ub-17b group, faculty of Management and Information Security, Vinnitsa National Technical University, Vinnitsa, e-mail: mberestenko7@gmail.com.*