КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (21), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.21.149161
УДК УДК 004.738.5

Ахрамович Володимир Миколайович
Д.т.н., професор, професор кафедри
систем інформаційного та кібернетичного захисту
Державний університет телекомунікацій, м. Київ, Україна
ORCID ID: 0000-0002-6174-5300
12z@ukr.net

ЗАХИСТ ДАНИХ НА СТАДІЯХ ЇХ ФУНКЦІОНУВАННЯ

Анотація. Комп'ютерні та інформаційні технології сьогодні охопили усі галузі економіки. Для будь-якої сучасної компанії інформація стає одним із головних ресурсів, збереження та правильне розпорядження яким має ключове значення для розвитку бізнесу та зниження рівня різноманітних ризиків. Актуальною проблемою сьогодення є забезпечення інформаційної безпеки. Методи та способи захисту даних залежать, в тому числі, від того, в якому стані знаходяться дані. З урахуванням сказаного в статті зроблена спроба розглянути методи та способи захисту даних в залежності від станів даних (дані у стані спокою; :дані, що передаються; використані дані). Так, наприклад, для стану неактивних даних (стан спокою) характерні методи та способи захисту: у вигляді застосування різних методів шифрування, управління правами доступу, наприклад, такі як SealPath, використання інструментів MDM (вони дозволяють обмежити доступ до певних корпоративних програм, заблокувати доступ до пристрою або зашифрувати дані на мобільному телефоні чи планшеті), DLP (запобігання витоку даних), CASB (брокери безпеки хмарного доступу): Це системи, які дозволяють застосовувати політики безпеки до документації, яку ми маємо в хмарних системах, наприклад, таких як Office 365, Box, Salesforce і т.д. Для стану даних, що передаються характерні методи та способи захисту у вигляді застосування: шифрування електронної пошти; керована передача файлів, наприклад, технології MFT; технології DLP забезпечують захист, оскільки вони можуть виявити, чи намагаються надіслати конфіденційні дані за межі організації; CASB (Cloud Access Security Brokers): стосується даних, що передаються ненадійним користувачем для цього типу даних), вони можуть бути заблокованими для завантаження; технології SealPath; і т.д. Для стану даних, що використовуються характерні методи та способи захисту у вигляді застосування: уданому випадку рекомендовано технології захисту цифрових прав або IRM який є одним з найефективніших засобів захисту даних, оскільки він поєднує шифрування + керування дозволами + контроль ідентифікації. Цей захист дозволяє зберігати документацію в безпеці в трьох її станах і відслідковувати в будь якому стані послідовно.

Ключові слова: стан функціонування даних, захист даних, методи та способи захисту.

ВСТУП

Коли справа доходить до захисту конфіденційної інформації, ми виявляємо, що клієнти потребують різних підходів до захисту. Деякі клієнти повинні захистити інформацію на своїх мобільних комп'ютерах або ноутбуках у разі втрати. Інші хочуть, щоб їхня документація була захищена на файлових серверах, коли вона могла бути навіть захищена від неправильного доступу з боку IT-персоналу. Іноді деяким клієнтам необхідно захистити документацію, коли вона передається в електронному листі, тому що вони використовують керовані поштові сервери або хмари. Деякі клієнти просять захистити документацію, коли вона надсилається третім особам або навіть усередині компанії, щоб звести до мінімуму ймовірність того, що вона буде скопійована, незахищена або доступна невідповідним користувачам.

Тобто користувачі хочуть мати надійний захист даних на всіх життєвих стадіях функціонування.

Постановка проблеми.

Потреби користувачів, підприємств, суспільства в захисті даних зростають з кожним роком. Аналогічно зростають способи та методи захисту даних, їх кількість та різноманітні технології. Дослідження в даній статті присв'ячено, аналізу захисту даних від стадій їх функціонування та вибору (передбаченню) комплексних технологій, які забезпечують захист на всіх етапах (стан спокою, передачі та використання). Це дозволить акцентувати увагу науковців, розробників технологій захисту на комплексних системах захисту які забезпечують захист даних на всіх життєвих стадіях. Що дозволить підвищити рівень захисту даних.

Аналіз останніх досліджень і публікацій.

В роботі [1] наведено набір статистичних тестів для генераторів випадкових і псевдовипадкових чисел для криптографічних програм розроблених національний інститутом стандартів і технологій США. Не розглядається захист даних від їх стану.

В статті [2] вказано на три стани даних, але розглянуто описово тільки захист даних в хмарних технологіях.

В роботі [3] наведено практичні завдання та результати захисту даних в комп'ютерних мережах без врахування інших станів даних.

В статті [4] наведено описово захист даних в мережі Інтернет. Не розглядається захист даних від їх стану.

В статті [5] наведено організаційний та технічний захист даних без врахування станів даних.

В роботі [6] наведена систематизована сукупність відомостей, що забезпечує з'ясування понять захисту інформації з обмеженим доступом, як однієї з найважливіших сфер діяльності держави, опанування основними термінами та категоріями технічного захисту інформації на рівні їх тлумачення і відтворення для практичного застосування та втілення у процесі фахової та професійної діяльності із забезпечення національної безпеки в інформаційній сфері. Не розглядається захист даних від їх стану.

В роботі [7] відображено сучасні погляди на стан та гарантування інформаційної безпеки особистості, суспільства та держави та визначає необхідність захисту інформації в сучасних умовах. Розглянуто основні питання захисту інформації та інформаційної безпеки. Не розглядається захист даних від їх стану.

В статті [8,9] розглянуті основні загрози інформації та методи захисту. Не розглядається захист даних від їх стану

В роботі [10] розглянуті основні загрози від різних типів витоку інформації та методи захисту. Не розглядається захист даних від їх стану

В роботі [11] розглянуто основи сучасного захисту інформації в комп'ютерних системах, не пов'язаних із державною таємницею. Викладено основні поняття та визначення захисту інформації, формування політики безпеки, критерії оцінки захищеності комп'ютерних систем, основи криптографічного захисту інформації, захисту інформації від несанкціонованого доступу в сучасних операційних системах, а також описано комплексні системи захисту в корпоративних інформаційних системах. Не розглядається захист даних від їх стану.

Мета статті.

Метою статті є висвітлення підходів комплексного захисту даних послідовно в залежності від стадій їх функціонування (стан спокою, передачі та використання), що дає

змогу ефективно і з мінімальними витратами розбудовувати систему захисту даних та прогнозувати перспективи в даній сфері діяльності.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Розглянемо три стани для інформації або даних:

Дані у стані спокою: Під цим терміном маються на увазі дані, які не доступні та зберігаються на фізичному чи логічному носієві. Прикладами можуть бути файли, що зберігаються на файлових серверах, записи в базах даних, документи на флеш-накопичувачах, жорстких дисках і т.д.

Передавані дані: дані, що надсилаються електронною поштою, через Інтернет, програми спільної роботи, такі як Slack (головною особливістю Slack є канали – організовані простори, де можна зібрати всіх співробітників та все необхідне для роботи. Канали дозволяють спілкуватися співробітникам із різних відділів, офісів, часових поясів і компаній. Широкі можливості Slack дозволяють працювати коли, де та як зручно. Легко можна спілкуватися в чаті, надсилати аудіо- та відеоповідомлення або влаштовувати дзвінки, щоб обговорити все необхідне з колегами наживо.), або Microsoft Teams (дозволяє налаштувати статус доступності, слідкувати за оновленнями в інформаційному каналі активності, створювати групові чати, а також працювати разом із колегами над документами в реальному часі. Включає інклюзивну систему онлайн-освіти або на її гібридну модель, упевнено користуйтеся навчальними інструментами та залучати студентів до активнішої взаємодії.), обмін миттєвими повідомленнями або будь-який тип приватного чи загальнодоступного каналу зв'язку. Це інформація, яка подорожує з однієї точки до іншої.

Використані дані: коли вони відкриваються одним або декількома програмами для їх обробки або споживаються або доступні користувачам.

Захист неактивних даних (рис.1).

Рис. 1 Приклади захисту неактивних даних

Документація вважається захищеною у стані спокою, коли вона зашифрована (так що для її розшифрування потрібна велика кількість часу, або кошторису, наприклад, в атаці методом перебору), ключ шифрування відсутній на тому ж носії даних, а також ключ має достатню довжину та рівень випадковості, щоб зробити його несприйнятливим до атаки за словником.

У цій галузі ми знаходимо різні технології захисту даних. Наприклад:

Повне шифрування диска або пристрою: Шифрування жорсткого диска приводить до того, що наприклад, у разі втрати ноутбука або комп'ютера дані, що містяться в ньому, не можуть бути доступні шляхом простого підключення жорсткого диска або пристрою до іншої машини. Його перевага полягає в тому, що він «прозорий» для користувача,

якщо користувач правильно увійшов до системи, він або вона може отримати доступ до документів так само, як він чи вона на незашифрованому комп'ютері. Однак, якщо комп'ютер або файловий сервер доступний адміністратору, ніщо не заважає нечесному користувачеві отримати доступ до даних, скопіювати їх, повторно надіслати і т.д. Дані захищені під час перебування на пристрої або жорсткому диску, але більше не захищені після їх вилучення з пристрою (копіювання на інший пристрій, повторного надсилання тощо).

Шифрування на рівні файлів: В указаному випадку жодний розділ або жорсткий диск не шифруються, лише окремі файли. Наприклад, шифрування з відкритим ключем або симетричне шифрування дозволяє шифрувати файли. Файли не тільки шифруються, коли вони зберігаються на диску, але також можуть бути захищені під час передачі, коли вони відправляються, наприклад, як вкладення в електронному листі. У такому випадку втрачається прозорий доступ з боку користувача, а також прозорий захист користувача. Тобто, з PGP, наприклад, необхідно мати відкритий ключ людини, з яким я хочу поділитися захищеним файлом, а з іншого боку він повинен мати мій відкритий ключ, щоб мати можливість його розшифрувати. З іншого боку, щойно документ був розшифрований одержувачем, він може зберігатися незахищеним, повторно відсилатися незахищеним тощо.

Шифрування бази даних: Системи баз даних, наприклад, такі як SQL Server або Oracle, використовують прозоре шифрування даних для захисту даних, що зберігаються в базах даних. Технології TDE виконують операції шифрування та розшифрування файлів даних у режимі реального часу. Це дозволяє розробникам додатків, наприклад, працювати із зашифрованими даними за допомогою AES або 3DES, наприклад, без необхідності змінювати існуючі програми. Цей тип шифрування захищає неактивні дані в базі даних, але не тоді, коли дані вже були доступні відповідному додатку і можуть бути вилучені.

Захист за допомогою управління цифровими правами (IRM): Технології управління правами на дані, такі як SealPath (Управління правами на доступ до даних, дозволяють шифрувати документацію, застосовуючи до неї постійний захист. Документація, що зберігається, шифрується і доступна тільки користувачам, які мають до неї права доступу. На відміну від шифрування на рівні файлу, користувач може отримати до нього доступ для читання і навіть зміни, але не може повністю розшифрувати файл (якщо йому або їй не призначені дозволи на повний доступ до файлу).

MDM (Керування мобільними пристроями): Одним із способів керування даними на мобільних пристроях є інструменти MDM. Вони дозволяють обмежити доступ до певних корпоративних програм, заблокувати доступ до пристрою або зашифрувати дані на мобільному телефоні чи планшеті. Як і у випадку зі стандартним шифруванням, дані корисні у разі втрати пристрою, але коли дані надсилаються назовні, вони залишаються незашифрованими.

DLP (Запобігання витоку даних): Захист від втрати даних, крім інших функцій, забезпечує пошук чи розташування конфіденційних даних у кінцевій точці або мережевому репозиторії. У разі даних у репозиторії, вони можуть видалити дані, наприклад, або заблокувати доступ до певних користувачів у випадку, якщо це порушує будь-яку політику безпеки (наприклад, знаходиться на комп'ютері, якого не повинно бути). Вони дійсні, поки дані знаходяться всередині організації, але вони не можуть діяти після відправлення даних за межі організації.

CASB (брокери безпеки хмарного доступу): Це системи, які дозволяють застосовувати політики безпеки до документації, яку ми маємо в хмарних системах,

наприклад, таких як Office 365, Box, Salesforce і т.д. Для простоти можна сказати, що це DLP-система , що застосовується до хмарного додатку, а не до периметру організації. Що стосується неактивних даних, CASB здатні виявляти конфіденційні дані у певних хмарних сховищах даних та застосовувати політики захисту до документації, наприклад, видаляючи публічне посилання на документ та обмежуючи доступ до нього групою користувачів, якщо дані визначені як конфіденційні. Як і DLP (Це рішення для запобігання витоку конфіденційних файлів за межі мережі компанії. DLP-системи аналізують всю вхідну та вихідну інформацію і за допомогою неї виявляють підозрілі операції та ризики.), вони можуть діяти, поки дані знаходяться в хмарі (наприклад, G-Suite) (рис. 2).

Проблеми захисту даних під час зберігання

Сучасні IT-відділи стикаються з численними проблемами, коли мова заходить про захист документації, що зберігається:

Дані можуть зберігатися на різних носіях та обладнанні: важлива документація не тільки знаходиться на файлових серверах або в менеджерах документів, але також можливі копії на ПК користувачів, USB-пристроях і т.д.

Мобільні телефони та планшети є ще одним робочим інструментом, який може містити важливу документацію у стані спокою, яка має бути захищена. Необхідно враховувати, що в багатьох випадках, коли конфіденційні дані використовуються, мобільні пристрої, в яких вони знаходяться, є не корпоративними, а особами поза зоною контролю IT-відділів.

Неможливість управління хмарним сховищем: багато постачальників сховищ пропонують шифрування та захист даних, якими вони керують у стані спокою. Однак ключі шифрування належать постачальнику сховища, а не компаніям, які їх наймають, тому контроль над документацією, що зберігається в цих хмарах, втрачається.

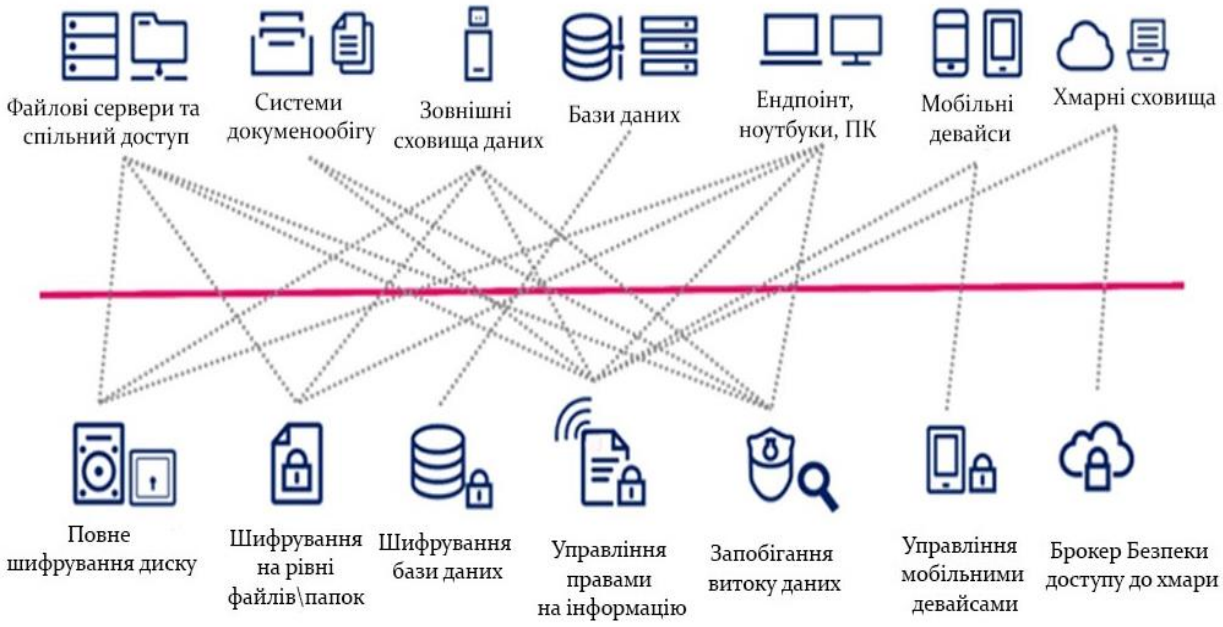

Рис. 2 Дані захищені, поки знаходяться в хмарі

Необхідно дотримуватись різних правил захисту даних: Залежно від вертикалі, в якій працює компанія, на неї можуть поширюватися суворі правила щодо даних щодо захисту та контролю над даними. Наприклад, дані пацієнтів у секторі охорони здоров'я або дані клієнтів у фінансовому секторі захищені такими правилами, як EU-GDPR (Загальний регламент про захист даних. У поточній редакції OB L 119, 04.05.2016; кор. OJ L 127, 23.5.2018 як акуратно оформлений веб-сайт.), HIPAA, PCI (У Законі про передачу даних та обліку в системі медичного страхування США (Health Insurance Portability and Accountability Act, HIPAA) та Законі про застосування медичних інформаційних технологій в економічній діяльності та клінічній практиці США (Health Information Technology for Economic and Clinical Health Act, HITECH) формалізовані технологічні підходи до безпеки та конфіденційності у сфері охорони здоров'я.), тощо залежно від території. Ці правила накладають політики захисту на неактивні дані, незалежно від того, зберігаються вони у базі даних, на файловому сервері чи мобільних пристроях.

Щоб подолати ці проблеми, IT-відділи повинні проаналізувати основні ризики, з якими вони стикаються щодо управління своїми неактивними даними, та вибрати технологію чи технології, віддаючи пріоритет тим, які усунуть чи пом'якшать ті, які найбільш ймовірні та/або мають найбільший вплив на їхню організацію (рис. 3).

Захист даних, що передаються. Ми живемо в епоху цифрового співробітництва, і є багато способів поділитися нашими даними з іншими користувачами. Одним із найбільш широко використовуваних традиційно є електронна пошта. З більш ніж 3,9 мільярдами користувачів, які сьогодні використовують електронну пошту (Statista, 2020), ці цифри, як очікується, зростуть до 4,3 мільярда користувачів до 2023 року. Тим не менш, ми переміщуємо дані через інші платформи, такі як Slack або Microsoft Teams, через хмарні програми для зберігання, такі як Box, OneDrive, Dropbox і т.д.

Серед різних технологій захисту даних можна виділити такі (рис. 3):

Рис. 3 Захист даних, які передаються

Шифрування електронної пошти: забезпечує наскрізний захист текстів повідомлень та вкладень Існує широкий спектр інструментів для шифрування електронної пошти. Один із них заснований на PKI (Public Key Infrastructure), комбінації закритого ключа (відомого тільки вам) та відкритого ключа (відомого тим, кому ви хочете надіслати захищене повідомлення). Електронна пошта та вкладення захищені за допомогою відкритого ключа одержувача, а при отриманні одержувач використовує свій закритий ключ для розшифрування вмісту. Після того, як електронний лист або вкладення було розшифровано, контроль над ним губиться, і його можна пересилати, копіювати і т.д.

Керована передача файлів (MFT): це безпечна альтернатива передачі файлів, наприклад, через FTP. Файл завантажується на платформу і генерується посилання для

завантаження. Це посилання надсилається електронною поштою або іншим способом одержувачу, який робить завантаження через HTTPS. Можна встановити термін дії посилання, пароль для доступу до неї і т.д. Як це відбувається із шифруванням електронної пошти, після завантаження файлу він не захищений, і з ним можна робити, що захочеться.

DLP (Data Leak Prevention): Технології DLP забезпечують захист, оскільки вони можуть виявити, чи намагаються надіслати конфіденційні дані за межі організації (наприклад, номери кредитних карт) і заблокувати відправку таких даних. Вони також дозволяють блокувати копії даних на USB-накопичувач, відправляти на мережеві диски, завантажувати в веб- або хмарні програми і т. д. Проблема, яку вони представляють, полягає в тому, що якщо дані були надіслані, їх більше не можна контролювати. Крім того, вони можуть бути схильні до помилкових спрацьовувань та блокувати дійсні запити, які мають бути виконані.

CASB (Cloud Access Security Brokers): Що стосується даних, що передаються, вони можуть бути виявленими, якщо користувач намагається завантажити конфіденційні дані, і якщо він не дотримується певної політики безпеки (наприклад, не є надійним користувачем для цього типу даних), вони можуть бути заблокованими для завантаження. Як і у випадку DLP, якщо дані були завантажені, контроль над ними втрачається. Вони застосовують безпеку до кінцевого числа хмарних програм, зазвичай найбільш відомих.

Захист при передачі з цифровими правами: наприклад, за допомогою SealPath можна застосовувати в електронній пошті не тільки для шифрування даних та вкладень, але й для застосування прав використання, залишаючи лише контент для перегляду, або для перегляду та редагування, але не для друку тощо. Вони також дозволяють, наприклад, обмежити пересилання електронної пошти одержувачам, якщо це необхідно. Оскільки файл, захищений цифровими правами, переміщується із захистом, захист під час транспортування пропонується через будь-який носій. Існує інтеграція з такими інструментами, як DLP або CASB, тому якщо конфіденційний документ виявляється як вихідний з мережі або конфіденційний документ завантажується з хмарної програми, вони можуть автоматично захистити його залежно від політики безпеки (рис. 4).

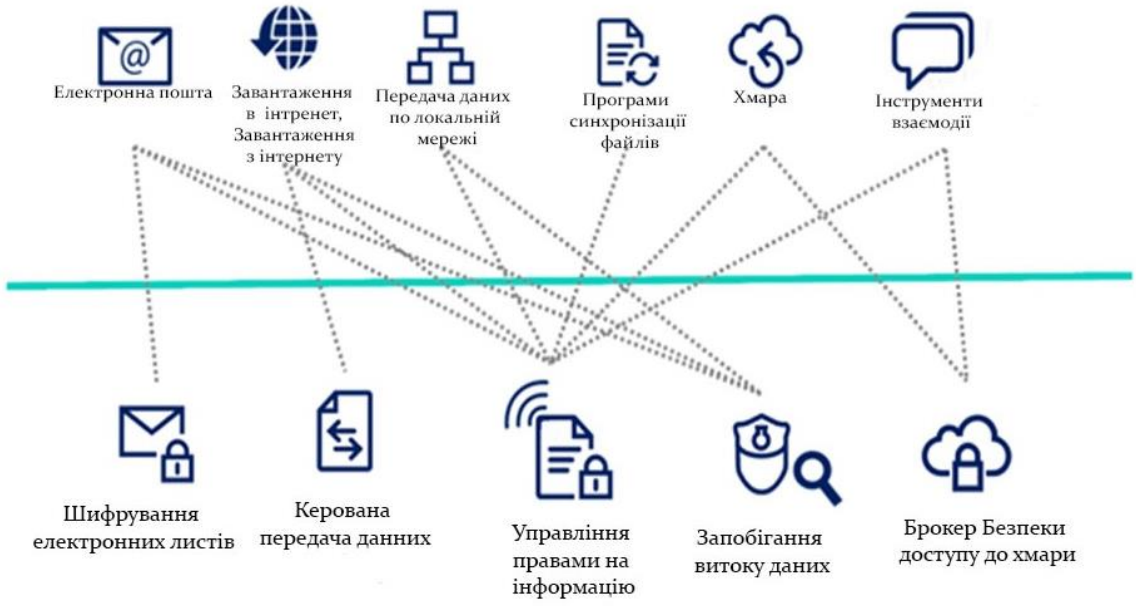

Рис. 4 Захист даних при транспортуванні

Проблеми захисту даних під час транспортування

Існує безліч засобів і каналів зв'язку: ці інструменти зазвичай захищають певний канал, такий як електронна пошта, веб-завантаження і т. д

Нескінченність хмарних програм захисту: Якщо ми говоримо про підхід типу CASB для захисту даних, які завантажуються з хмари, дуже важко дістатися до будь-якої програми. Опції зазвичай доступні найпопулярніших хмарних додатків, як-от O365, G-Suite, Salesforce, Box тощо.

Неможливість зберегти контроль на приймаючому кінці: у разі шифрування електронної пошти або MFT, як тільки одержувач отримав файл і розшифрував його для нього, контроль втрачається. Вони пропонують захист «крапка-крапка», але не далі, за винятком захисту цифрових прав.

Складність визначення того, що має бути захищене, а що ні, важке для системи DLP чи CASB визначити, що має бути заблоковане, а що ні. Деякі правила можуть бути встановлені, але можуть призвести до помилкових спрацьовувань, які блокують виведення даних за необхідності. Іноді підхід «захистити всіх» (з винятками) є кращою політикою, наприклад, у разі шифрування електронної пошти, тому що, якщо хтось скомпрометує поштову скриньку, ми впевнені, що він отримає доступ до зашифрованих даних, але це не завжди можливо в залежності від типу організації.

IT-відділи повинні подивитися, чи варто запобігати більшості потенційних проблем при передачі частини даних, що передаються. Наприклад, якщо вони висвітлюю 20% засобів масової інформації, електронну пошту або певні програми, то необхідно запобігати 80% можливих проблем (рис. 5).

Як згадувалося вище, йдеться про дані, що використовуються при доступі до них програми для лікування. Зазвичай за додатком знаходиться користувач, який хоче отримати доступ до даних, щоб переглянути їх, змінити і т.д. у разі, якщо дані були зашифровані).

Для захисту даних, що використовуються, елементи керування зазвичай повинні бути встановлені на доступ до вмісту. Наприклад, через:

Інструменти керування ідентифікацією: щоб перевірити, що користувач, який намагається отримати доступ до даних, є тим, ким він себе називає, і не було жодної крадіжки особистих даних. У цих випадках дедалі більшого значення набуває захист доступу до даних за допомогою двофакторної автентифікації.

Рис. 5 Захист даних, що використовуються

Засоби умовного доступу або управління доступом на основі ролей (RBAC): дозволяють доступ до даних на основі ролі користувача або інших параметрів, таких як IP-адреса, розташування і т.д.

ISSN 2663 - 4023

Однак у цих випадках ми захищаємо дані, більш точно обмежуючи тих, хто може і не може отримати до них доступ, але після того, як база даних або документ були отримані, ми не можемо перешкодити людині робити з даними те, що вона хоче.

За допомогою захисту цифрових прав або IRM: ми можемо отримати ефективний захист під час використання даних, оскільки ми можемо обмежити дії, які користувач може вжити після отримання доступу до даних. Наприклад, ми можемо заборонити редагувати, друкувати та ін. Але документ, повністю незахищений.

За допомогою захисту IRM, (керування правами доступу до інформації (IRM) дає змогу вказати дозволи на доступ до повідомлень електронної пошти. За допомогою IRM неавторизовані користувачі не можуть читати, друкувати, переспрямовувати та копіювати особисті дані. Крім того, за допомогою засобу IRM організації застосовують корпоративну політику, яка регулює розповсюдження конфіденційної інформації, як у межах організації, так і для клієнтів та партнерів.), що застосовується безпосередньо до файлу (а не до менеджера документів або самої платформи спільної роботи), ми можемо застосовувати захист, який поширюється разом з документами та обмежує дозволи на відкриття, де б він не знаходився. Незалежно від того, чи знаходяться дані в хмарі, чи був завантажений, можна дозволити користувачеві побачити їх, але не повністю зняти захист, заборонити друк і т.д. (рис. 6).

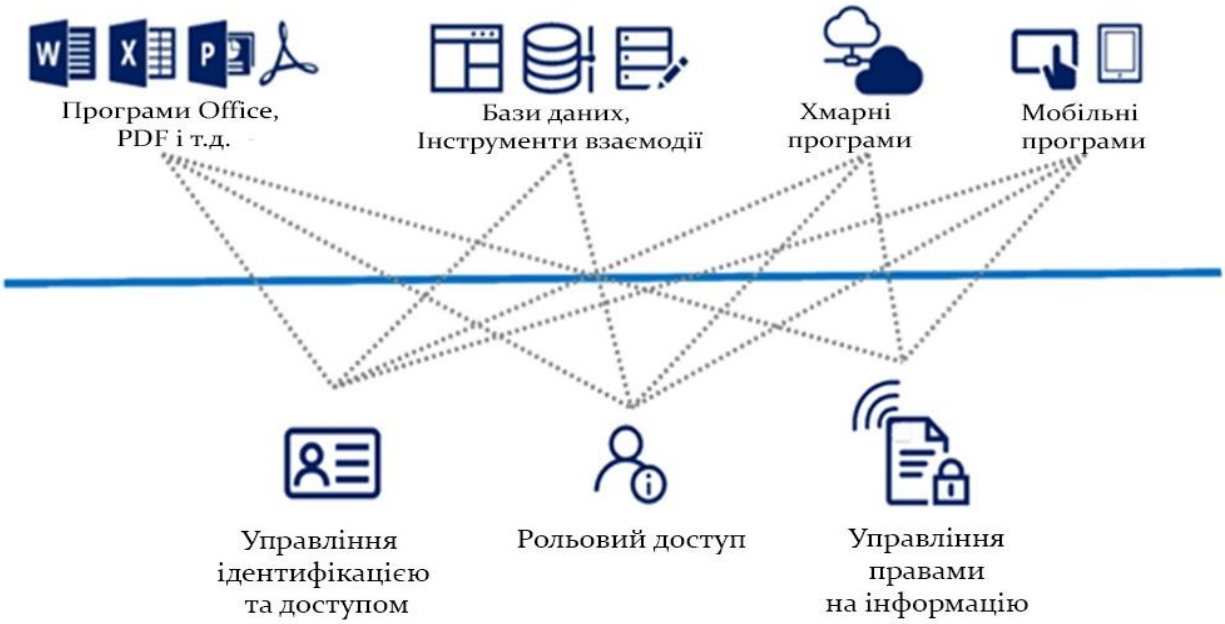

Рис. 6 Приклади заборон для користувача

Захист даних, що використовуються.

Більшість інструментів, які контролюють доступ до даних, роблять це через дозвіл на доступ, але після перевірки, як ми вже говорили вище, складніше контролювати, те що можна зробити з даними.

Навіть якщо обмежено дозвіл на документацію, якщо вона показується користувачеві у додатку, у засобі перегляду, він завжди може зробити знімок, хоча можна пом'якшити цю дію за допомогою динамічних водяних знаків на відкритому документі.

Платформи для співпраці, які обмежують права, такі як заборона завантаження або лише дозвіл на перегляд документа, можуть бути ефективними, коли потрібно лише отримати доступ до документа, але мають обмеження, якщо потрібно змінити документ, наприклад, за допомогою інструменту на робочому столі. Крім того, не треба забувати, що на самій хмарній платформі документ розшифровується під час доступу та зберігається в їхніх системах, тому доступ до його вмісту є технічно можливим. Це може бути проблемою, коли ми говоримо про конфіденційні дані або щодо суворих правил захисту даних.

Не вдаючись до питань захисту даних, що використовуються, шляхом шифрування даних у пам'яті, поки програма відкрита, щоб уникнути їх скидання, захист цифрових прав або IRM є одним з найефективніших засобів захисту даних, оскільки він поєднує шифрування + керування дозволами + контроль ідентифікації.

Рис. 7 Захист даних, що поєднує шифрування + керування дозволами + контроль ідентифікації

Цей захист дозволяє зберігати документацію в безпеці в трьох її станах: у стані спокою, у дорозі, та у використанні. Захист подорожує з документом і супроводжує його, куди б документ не подорожував, дозволяючи користувачеві працювати з даними, знаючи, що в разі необхідності він не матиме повного контролю над ними.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Досліджено методи, способи та технології захисту даних в залежності від стадій їх функціонування та вибору (передбаченню) комплексних технологій, які забезпечують захист на всіх етапах. Це дозволить акцентувати увагу науковців, розробників технологій захисту на комплексних системах захисту які забезпечують захист даних на всіх життєвих стадіях. Що, в свою чергу, дозволить підвищити рівень захисту даних.

Подальші дослідження будуть пов'язані з дослідженням найбільш сучасних технологій захисту даних, що гарантують захист їх на всіх стадіях функціонування даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 NIST SP 800-22rev1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications//National Institute of Standards and Technology Special Publication 800-22rev1a, 2010, -131 p

2 Protecting the three states of data. https://www.sealpath.com/blog/category/data-protection.

3 Ахрамович, В., Чегренець, В., Котенко, А. (2018). *Комп'ютерні мережі. Архітектура, проектування, захист.* ДУТ. https://www.dut.edu.ua/ua/lib/1/category/2438/view/1679

4 Ахрамович, В., & Білоцерківець, О. (2019). Методика підвищення ефективності застосування засобів забезпечення інформаційної безпеки користувачів послуг Інтернет. У *«Инфраструктура ИКТ как основа цифровой экономики»*.

5 Ахрамович, В.М., Амелькін, С.В. (2019). Система захисту інформації підприємства. Організація служби захисту. *Сучасний захист інформації*, *1*, 17-23. http://journals.dut.edu.ua/index.php/dataprotect/article/download/2301/2200

6 Богуш, В.М., Бровко, В.Д., Кобус, О.С., Козюра, В.Д. (2022). *Технічний захист інформації*. Ліра -К.

7 Хорошко, В. О., Павлов, І. М., Бобало, Ю. Я., Дудикевич, В. Б., Опірський, І. Р., Пархуць, Л. Т. (2020). *Проєктування комплексних систем захисту інформації*. Видавництво Львівської політехніки.

8 Захист інформації в системах обміну даними. https://www.mil.gov.ua/ukbs/zahist-informaczii-v-sistemah-obminu-danimi.html

9 Інформаційна безпека та захист інформації. https://www.bitgroup.com.ua/informacijna-bezpeka.php

10 Ленков, С.В., Перегудов, Д.А., Хорошко, В.А. (2008). Методы и средства защиты информации (в 2-х томах). Арий.

11 Остапов, С. Е. (2013) Технології захисту інформації : навчальний посібник. ХНЕУ.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (21), 2023
ISSN 2663 - 4023

Volodymyr Akhramovych
Doctor of Technical Sciences, Professor, Professor
Department of Information and Cyber Defense Systems
State University of Telecommunications
ORCID: 0000-0002-6174-5300
12z@ukr.net

DATA PROTECTION AT THE STAGES OF ITS FUNCTIONING

Abstract. Today, computer and information technologies have covered all areas of the economy. For any modern company, information becomes one of the main resources, the preservation and proper management of which is of key importance for business development and reducing the level of various risks. Ensuring information security is an urgent problem today.
Methods of data security depend, among other things, on the state of the data. Taking into account what was said in the article, an attempt was made to consider the methods of data security depending on the data states (data at rest; data being transmitted; used data).
So, for example, the state of inactive data (state of rest) is characterized by methods of security: in the form of the use of various encryption methods, access rights management, for example, such as SealPath, the use of MDM tools (they allow you to limit access to certain corporate programs, block access to a device or encrypt data on a mobile phone or tablet), DLP (data leakage prevention), CASB (cloud access security brokers): These are systems that allow us to apply security policies to the documentation we have in cloud systems, for example, such as Office 365, Box, Salesforce, etc.
For the state of the transmitted data, typical methods of security in the form of application: encryption of e-mail; managed file transfer, such as MFT technology; DLP technologies provide protection because they can detect if sensitive data is being sent outside the organization; CASB (Cloud Access Security Brokers): refers to data transmitted by an untrusted user for this type of data), it may be blocked for download; SealPath technologies; etc.
For the state of the data used, the typical methods of security in the form of application: in a successful case, digital rights protection technologies or IRM are recommended, which is one of the most effective means of data protection, because it combines encryption + permission management + identity control. This security allows documentation to be stored safely in its three states and tracked in any state sequentially.

Keywords: state of data functioning, data security, methods of protection.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 NIST SP 800-22rev1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications//National Institute of Standards and Technology Special Publication 800-22rev1a, 2010, -131 p
2 Protecting the three states of data. https://www.sealpath.com/blog/category/data-protection.
3 Akhramovych, V., Chehrenets, V., Kotenko, A. (2018). Kompiuterni merezhi. Arkhitektura, proektuvannia, zakhyst. DUT. https://www.dut.edu.ua/ua/lib/1/category/2438/view/1679
4 Akhramovych, V., & Bilotserkivets, O. (2019). Metodyka pidvyshchennia efektyvnosti zastosuvannia zasobiv zabezpechennia informatsiinoi bezpeky korystuvachiv posluh Internet. U «Ynfrastruktura YKT kak osnova tsyfrovoi эkonomyky».
5 Akhramovych, V.M., Amelkin, S.V. (2019). Systema zakhystu informatsii pidpryiemstva. Orhanizatsiia sluzhby zakhystu. Suchasnyi zakhyst informatsii, 1, 17-23. http://journals.dut.edu.ua/index.php/dataprotect/article/download/2301/2200
6 Bohush, V.M., Brovko, V.D., Kobus, O.S., Koziura, V.D. (2022). Tekhnichnyi zakhyst informatsii. Lira - K.
7 Khoroshko, V. O., Pavlov, I. M., Bobalo, Yu. Ya., Dudykevych, V. B., Opirskyi, I. R., Parkhuts, L. T. (2020). Proiektuvannia kompleksnykh system zakhystu informatsii. Vydavnytstvo Lvivskoi politekhniky.

8 Zakhyst informatsii v systemakh obminu danymy. https://www.mil.gov.ua/ukbs/zahist-informaczii-v-sistemah-obminu-danimi.html
9 Informatsiina bezpeka ta zakhyst informatsii. https://www.bitgroup.com.ua/informacijna-bezpeka.php
10 Lenkov, S.V., Perehudov, D.A., Khoroshko, V.A. (2008). Metodы y sredstva zashchytы ynformatsyy (v 2-kh tomakh). Aryi.
11 Ostapov, S. E. (2013) Tekhnolohii zakhystu informatsii : navchalnyi posibnyk. KhNEU.