ПРОГРАМНЕ ШИФРУВАННЯ ТА ДОТРИМАННЯ НОРМАТИВНИХ ВИМОГ: БЮДЖЕТНЕ РІШЕННЯ ТА СЕРЙОЗНІ БЕЗПЕКОВІ РИЗИКИ

НОРМАТИВНІ ВИМОГИ

Раніше безпека даних була справою IT-відділів, однак через постійні витоки даних уряди багатьох країн світу почали встановлювати для бізнесу жорсткіші вимоги щодо шифрування та захисту всіх даних, які ідентифікують людину.

Шифрування конфіденційних даних регламентується на законодавчому рівні — від HIPAA у сфері охорони здоров'я до GDPR у країнах Європи, Близького Сходу й Африки та CCPA в Каліфорнії. Протягом останніх 3 років значно збільшилася кількість наглядових організацій, а з ними і кількість правових норм, розміри штрафів та ризики правових наслідків.

Через ці зміни IT-відділам стало складніше боротися з ризиками для безпеки та збільшенням витрат. В умовах пандемії COVID зростають витрати на закупівлю додаткового обладнання та брандмауерів через привернення уваги до шифрування даних.

Зростає популярність програмного шифрування з використанням Microsoft BitLocker® або програм адміністрування кінцевих точок від Symantec, McAfee тощо. Крім того, деякі організації та споживачі використовують стандартні USB-накопичувачі з програмними сховищами, що надаються деякими постачальниками.

ШИФРУВАННЯ ТА ДАНІ В РУСІ

Співробітникам і споживачам потрібно носити із собою свої дані. Для цього їм пропонують скористатися декількома варіантами:

1. Хмарні служби: це чудовий варіант, оскільки вони матимуть доступ до даних із будь-якого пристрою, який може під'єднатися до Інтернету. Проте така гнучкість має свою ціну. Зберігання даних у хмарі позбавляє користувача або компанію контролю над даними та створює потенційні ризики, оскільки ми бачили, як хмарні сервери залишалися незахищеними.
2. Стандартні USB-накопичувачі: Хоча USB-накопичувач здається безпечнішим рішенням, існує високий ризик витоку даних через його втрату. Наприклад, є безліч історій про втрачені USB-накопичувачі із секретною інформацією або про пральні з ящиками, заповненими загубленими USB-накопичувачами.
3. USB-накопичувачі з апаратним шифруванням: Ці USB-накопичувачі мають спеціальну архітектуру, яка містить вбудований контролер шифрування та контролю доступу. Дані шифруються з використанням найнадійнішого 256-бітного AES-шифрування в режимі XTS та інших можливих заходів захисту для пом'якшення фізичних і програмних атак. Ці накопичувачі виготовляються компаніями, які спеціалізуються на пристроях безпеки. Хоча вони й дорожчі за стандартні USB-накопичувачі, вони забезпечують найкращий захист даних. Накопичувачі, що відповідають вимогам FIPS 197 або FIPS 140-2 рівня 3 забезпечують користувачам найвищий рівень захисту та спокій.
4. Стандартні USB-накопичувачі з програмним шифруванням: З міркувань безпеки, якщо того вимагають правові норми, можна використовувати програмне шифрування разом із BitLocker або іншими інструментами. Це непогані рішення, оскільки вони коштують недорого, забезпечуючи так само 256-бітне AES-шифрування в режимі XTS.

Недивно, що підприємства та галузі переважно обирають 4-ий варіант, використовуючи стандартні USB-накопичувачі з програмним шифруванням через те, що програмне шифрування, як-от BitLocker або інші сховища інформації, — це безкоштовне рішення.

ПРОГРАМНЕ ШИФРУВАННЯ НЕ ВІДПОВІДАЄ НОРМАТИВНИМ ВИМОГАМ

Фахівці в галузі безпеки підприємств можуть отримати від програмного шифрування все те, що мають дорожчі USB-накопичувачі з апаратним шифруванням. Але чи так це? Через обмежені бюджети підприємства переходять на програмне шифрування з метою дотримання вимог, не підозрюючи про негативні аспекти програмного шифрування.

Які загрози несе USB-накопичувач з програмним шифруванням? Чи 256-бітне AES-шифрування в режимі XTS не застосовується для даних при зберіганні та при передачі? Загалом — застосовується. У чому полягає проблема: програмне шифрування розглядається як «шифрування з можливістю видалення».

Що — з можливістю видалення? Чи означає це, що користувач може видалити функцію шифрування в USB-накопичувачі з програмним шифруванням?

Так. Користувачі можуть видалити функцію програмного шифрування зі своїх USB-накопичувачів. Ви запитаєте, навіщо їм це? Тому що вони можуть це зробити, і тому що вони хочуть просто відкривати файли без використання пароля або вони забули пароль, але їм потрібно користуватися USB-накопичувачем.

ЯК ВИДАЛИТИ ПРОГРАМНЕ ШИФРУВАННЯ ІЗ ЗАШИФРОВАНОГО USB-НАКОПИЧУВАЧА

Користувач, який не хоче вводити складні або будь-які інші паролі для отримання доступу до своїх даних, повинен виконати кілька простих дій:

1. Під'єднати накопичувач з програмним шифруванням до комп'ютера
2. Відформатувати накопичувач
3. Після завершення форматування будь-яке шифрування буде видалено
4. Скопіювати файли з секретною або конфіденційною інформацією на накопичувач для отримання швидкого доступу

Це можна швидко зробити на комп'ютері, на який не поширюються обмеження. IT-відділи обмежили використання команд форматування на комп'ютерах компанії, але це можна зробити на будь-якому іншому комп'ютері, що не належить компанії.

З метою дотримання вимог швидке видалення шифрування даних означає, що наданий компанією накопичувач тепер не має можливості шифрування. Крім того, дані, які було зашифровано, вважаються загубленими назавжди після видалення шифрування за допомогою описаного вище методу (ключі шифрування прив'язані до даних). Будь-які дані, скопійовані на пристрій після видалення шифрування, вважаються незахищеними й такими, що потенційно не відповідають вимогам і можуть призвести до порушення вимог HIPAA, GDPR, CCPA тощо.

НАСЛІДКИ ВТРАТИ НЕЗАШИФРОВАНОГО НАКОПИЧУВАЧА

Якщо закріплений за компанією USB-накопичувач було втрачено, а потім знайдено, навіть якщо компанія одразу не дізналася про це, але пізніше отримала відповідну інформацію через соціальні мережі, починають діяти особливі нормативні вимоги, які, можливо, вимагатимуть від компанії:

1. Провести судову експертизу, щоб визначити, які дані було втрачено
2. Визначити, чи мало місце порушення закону на основі консультацій з юридичним відділом
3. Визначити, чи потрібно проінформувати про це клієнтів

Це той випадок, коли втрата одного USB-накопичувача може коштувати дуже дорого. З судовими витратами, які перевищують багато сотень доларів на годину, цей процес може призвести до збитків в тисячі доларів, не враховуючи потенційних штрафів, клієнтських та інших судових позовів і ганьбу через розкриття даних.

Коли програмне шифрування розглядається як низькозатратне рішення, ці ризики та величезні фінансові наслідки не враховуються.

Існує ще одна загроза, пов'язана з використанням незашифрованих USB-накопичувачів у корпоративній мережі. Її зазвичай називають «BadUSB». BadUSB — це клас шкідливих програм, які зловмисники використовують для зламування брандмауерів компанії та впровадження шкідливого ПЗ у систему кіберзахисту компанії через USB-накопичувачі.

BadUSB

Коли USB-накопичувач під'єднується до комп'ютера, системний контролер комп'ютера встановлює зв'язок із контролером USB-накопичувача через мікропрограму. Цей обмін даними відбувається перед тим, як операційна система, наприклад Microsoft/macOS/Linux, дізнається про під'єднання USB-накопичувача. Кожен USB-накопичувач має мікропрограму, яка запускається одразу після під'єднання накопичувача до USB-роз'єму.

Зловмисники зрозуміли, що вони можуть впроваджувати шкідливі програми за допомогою цього механізму ініціювання з'єднання, замінюючи мікропрограму, яка запускається на USB-накопичувачі, іншою шкідливішою мікропрограмою, що запускає шкідливе ПЗ в цільову комп'ютерну систему, коли та взаємодіє з USB-накопичувачем. Стандартний USB-накопичувач не захищає свою внутрішню мікропрограму, яка виконується його контролером. Зловмисники почали використовувати звичайні USB-накопичувачі для обходу брандмауерів і порушення систем кіберзахисту, започаткувавши у такий спосіб метод атак BadUSB.

Багато компаній намагаються заборонити використання USB-накопичувачів у своїх системах або навіть заливають USB-роз'єми епоксидною смолою. Проте вони виявили, що деяким категоріям співробітників потрібно носити із собою дані на USB-накопичувачах. Наприклад, керівники хочуть взяти із собою дані для роботи або надання інформації зовнішнім юридичним або фінансовим консультантам, які не мають доступу до хмари компанії; підрядники компанії, яким потрібні дані для роботи, але з обмеженим доступом до баз даних компанії; фінансові аналітики, які поспішають закрити щомісячні звіти та повинні працювати з електронними таблицями вдома.

Як показує попередній аналіз, використання стандартного USB-накопичувача разом із програмним рішенням для шифрування пов'язане зі значним ризиком. Те, що на перший погляд здавалося бюджетним варіантом, виявилося потенційно дуже шкідливим і невиправдано затратним. Лише вартість 2- або 3-годинної консультації з юристом стосовно потенційного витоку даних зводить нанівець будь-яку економію від використання дешевшого рішення.

USB-НАКОПИЧУВАЧІ З АПАРАТНИМ ШИФРУВАННЯМ — НАЙКРАЩИЙ ВАРІАНТ ДЛЯ ЗАБЕЗПЕЧЕННЯ ДОТРИМАННЯ НОРМАТИВНИХ ВИМОГ.

Що робить USB-накопичувачі з апаратним шифруванням найкращим рішенням для таких сфер застосування:

1. USB-накопичувачі з апаратним шифруванням обладнані шифруванням, яке завжди ввімкнено: користувачі не можуть вимкнути шифрування, скинути правила створення паролів (мінімальна довжина, складність) і вимкнути автоматичні запроси повторного введення пароля. На відміну від програмного шифрування, яке не запобігає підбору пароля за допомогою словникових атак, апаратні версії обмежують кількість повторних спроб введення пароля та блокують дані, якщо невірний пароль введено 10 разів поспіль або навіть менше. Це дуже безпечно в епоху використання суперкомп'ютерів.
2. Накопичувачі з апаратним шифруванням використовують контролери шифрування преміум-класу та містять безліч функцій безпеки: Хоча ми не завжди розкриваємо всі захисні контрзаходи, існує спосіб захиститися від BadUSB. Ще на заводі, коли мікропрограма завантажується на накопичувачі з апаратним шифруванням, вона отримує цифровий підпис. Це означає, що після під'єднання цих зашифрованих USB-накопичувачів контролер шифрування спочатку перевіряє цілісність мікропрограми за допомогою цифрового підпису та завантажує її лише в разі успішного проходження перевірки. Будь-яка спроба замінити мікропрограму заблокує накопичувач, і він перестане працювати. Отже, більше немає ніякої загрози.
3. USB-накопичувачі з апаратним шифруванням можуть мати індивідуальні ідентифікатори продукту (PID), налаштовані під конкретну компанію: ці накопичувачі преміум-класу можуть містити запрограмований цифровий ідентифікатор. Тому, якщо накопичувач під'єднано до внутрішнього або зовнішнього брандмауера компанії, він може бути ідентифікований як накопичувач, випущений компанією. Наприклад, якщо співробітник втрачає накопичувач компанії та купує таку саму модель уроздріб, новий придбаний накопичувач не пройде перевірку в мережі компанії. Це налаштування підвищує рівень безпеки під час використання USB-накопичувачів.
4. Накопичувачі з апаратним шифруванням допомагають дуже швидко заощадити бюджет: саме зниження та усунення ризиків робить цикл окупності дуже коротким.

Kingston — найбільший у світі виробник USB-накопичувачів з шифруванням, що пропонує лінійки накопичувачів з різними функціями і ціновими категоріями. Зверніться безпосередньо до Kingston, щоб дізнатись, як ми можемо допомогти вам забезпечити дотримання вимог за допомогою USB-рішень з шифруванням для керівників, співробітників, підрядників тощо.

 MKF-956UA