yubico

БІЛА КНИГА

Захист енергії та природних ресурсів від сучасних кіберзагроз

Модернізуйте MFA і перейдіть на безпарольний захист критично важливих інфраструктур та потоку ресурсів

Зміст

Критична потреба у безпеці та ефективності організацій, що займаються енергетикою та природними ресурсами

$4.72 мільйони

вартість витоку даних в енергетиці [1]

$442 мільйони

це приблизно сума, на яку очікується зростання ринку кіберстрахування для енергетики до 2030 року [6]

Енергетичні та природні ресурси є безцінною частиною критично важливих національних і міжнародних інфраструктур, що робить їх ідеальною мішенню для кібератак, які можуть призвести до збоїв у роботі. Кібератаки не лише коштують організаціям, що займаються енергетикою та природними ресурсами, у середньому 4,72 мільйона доларів,[1] але також можуть призвести до втрати виробничого часу, інтелектуальної власності, цілісності продукту та потенційно вплинути на життя. Унікальний ландшафт інформаційних технологій (IT) та операційних технологій (OT), який існує у висхідному, проміжному та низхідному потоках природних ресурсів, лише посилює безліч точок дотику та передачі, які необхідно захистити від сучасних кіберзагроз. Крім того, цей сектор є ключовим цільовим об'єктом, тому що багато комунальних підприємств можуть опинитися за межею бідності у сфері кібербезпеки, що стосується тих, хто перебуває за межею бідності і не має достатнього бюджету або людських ресурсів для реалізації заходів безпеки.[2]

Атаки в цьому секторі стали звичним явищем у всьому світі. Атака Colonial Pipeline 2021 року, яка завдала збитків на десятки мільйонів доларів США та вплинула на мільйони людей у Східній частині Сполучених Штатів через один зламаний пароль,[3] лише підкреслила, що енергетичні та природні ресурси є основними цілями для складних програм-здирників і передових постійних загроз (APT) — таких негараздів, як фішинг, обмін SIM-картами та атак «людина посередині» (MiTM). У лютому 2022 року кібератака на європейські нафтопереробні центри Амстердам-Роттердам-Антверпен (ARA) порушила завантаження та розвантаження вантажів нафтопродуктів на тлі континентальної енергетичної кризи.[4]

Атака Colonial Pipeline разом із атакою SolarWinds у 2020 році також стали рушійними силами нормативних змін, які передбачили використання стійкої до фішингу багатофакторної автентифікації (MFA). Оскільки енергетична галузь підпадає під сферу компетенції кількох федеральних відомств, це призвело до необхідності дотримання безлічі стандартів та правил, таких як Директиви з безпеки Управління транспортної безпеки (TSA): Директиви безпеки TSA 2021-01 та 2021-02. Вони вимагають від власників і операторів трубопроводів впроваджувати спеціальні заходи для захисту від програм-здирників та інших кіберзагроз. Багато з цих практик, викладених у директивах, розроблені для систем інформаційних технологій, які знаходяться в традиційних комп'ютерних мережах, а не для операційних технологій – апаратного чи програмного забезпечення, яке моніторить або контролює обладнання, таке як запобіжні клапани трубопроводів та водяні насоси.[5] Це означає, що оператори, які покладаються на ці спільні ресурси OT, не отримують адекватних інструкцій для впровадження суворих заходів безпеки.

Крім того, Координаційна рада нафтогазового сектора (ONG SCC) та Федеральна комісія з регулювання енергетики (FERC) рішуче підтримують відповідність вимогам Національного інституту стандартів і технологій (NIST), у яких зазначено, що застарілі форми MFA, такі як SMS, повинні бути оголошені застарілими.

То чому підвищена увага саме до MFA? Відповідь полягає в тому, що поточні застарілі рішення автентифікації та безпеки, такі як імена користувачів і паролі та мобільні автентифікатори, більше не ефективні для захисту організацій від сучасних кіберзагроз. Дослідження Google, Нью-Йоркського університету (NYU) та Каліфорнійського університету у Сан-Дієго (UCSD), засноване на 350 000 реальних спроб зламу, показало, що одноразовий пароль (OTP) на основі SMS заблокував лише 76% цільових атак, а push-додаток заблокував лише 90%.[5] Як мінімум, коефіцієнт проникнення 10 %. При такому підході питання не в тому, чи буде на вас напад, а в тому — коли.

Крім того, сьогодні більшість постачальників кіберстрахування вимагають розгортання MFA, а також деяких стійких до фішингу MFA. Очікується, що ринок кіберстрахування в енергетичному секторі до 2030 року зросте до 442 мільйонів доларів США при середньорічному темпі зростання (CAGR) 18%.[6] Стає очевидним, що без потужного МЗС кіберстрахування буде неможливо отримати.

Поширені сценарії автентифікації та пов'язані з ними вразливості

У трьох секторах енергетики та природних ресурсів унікальний набір проблем і загальних сценаріїв автентифікації призвели до того, що безпека не встигає за ландшафтом атак на кібербезпеку, як показано в таблиці нижче.

Висхідний потік | Середній потік | Спадаючий потік

- Привілейовані користувачі та облікові записи в IT- та OT-середовищах
- Підрядники, контрактники, відряджені та спільні підприємства
- Спільне середовище робочої станції
- OT та середовища безпеки фізичного доступу з обмеженим мобільним доступом
- Польові пристрої IoT
- Безпека фізичного доступу

Привілейовані користувачі та облікові записи з доступом до критично важливих IT- та OT-систем

Кожна організація з енергетики та природних ресурсів має підмножину користувачів або облікових записів із привілейованим доступом до критично важливих IT- та OT-систем. Привілейований користувач або обліковий запис – це будь-який користувач або облікові дані для входу з розширеним доступом до критично важливих даних або систем у мережі або до критичної інфраструктури. Привілейовані користувачі та облікові записи повинні мати різні рівні доступу залежно від того, що вони повинні бачити та робити в цих системах, в ідеалі – мінімальний рівень доступу. Принцип найменших привілеїв означає надання найменшого можливого доступу (хто до чого має доступ) і найменшого можливого привілею (дії, які хтось може виконувати), пов’язані з цим доступом. Згідно з дослідженням, проведеним Ponemon Institute, в середньому 23% співробітників в організації можуть вважатися привілейованими користувачами.[7]

Ім'я користувача та пароль

- Розгортається всюди
- Відомі прогалини в юзабіліті
- Дорого, важко підтримувати
- Загальна ціль для фішингу облікових даних

Привілейований користувач також може бути користувачем, який не є штатним працівником, тобто підрядником, відрядженим, постачальником ланцюжка постачання тощо. Нещодавнє опитування показало, що до 97% організацій мали порушення кібербезпеки в результаті слабкості в ланцюжку постачання.[8] Організації повинні ідентифікувати та автентифікувати кожного користувача, який має доступ до вхідних даних, IP або до систем, задіяних у всьому ланцюжку постачання. Навіть системи SCADA, які моніторять і контролюють передачу електроенергії, транспортування газу та нафти по трубопроводах та інші функції,[9] потребують моніторингу доступу, тому що якщо можливості та контроль потрапляють до рук користувача зі зловмисними намірами, результат може бути катастрофічним. Таким чином, життєво важливо надавати доступ лише цим користувачам до програм і служб, пов'язаних із обліковими даними певного користувача, одночасно проводячи швидку та надійну автентифікацію для підтримки продуктивності.

Типи привілейованих користувачів

Нерегулярні користувачі

Доступ до чутливих/конфіденційних даних або систем для підрядників або для конкретних завдань

Привілейовані бізнес-користувачі

Доступ до чутливих/конфіденційних даних: C-suite, HR, фінанси, продажі

Привілейовані IT-користувачі

Доступ до систем, ПЗ та даних: IT-адміністратори, адміністратори безпеки, адміністратори мереж і адміністратори баз даних

Кібератаки, спрямовані на системи ICS та SCADA

Зараз енергетичні організації отримують попередження про зловмисне програмне забезпечення, націлене на пристрої промислової системи управління (ICS)/системи диспетчерського контролю та збору даних (SCADA), які можуть бути розгорнуті через фішинг або скомпрометований віддалений доступ. Зловмисники можуть отримувати контроль, скомпрометувати уражені пристрої, підвищувати привілеї та переміщатися всередині середовища OT, а також порушувати критичні пристрої чи функції.[10] Це зловмисне програмне забезпечення також відоме як «Pipedream», оскільки воно може «порушити, погіршити та потенційно зруйнувати промислове середовище і процеси» згідно зі звітом Dragos.[11]

Підрядники, контрактники, відряджені, та спільні підприємства

В енергетичному секторі не всі мають доступ до наданих компанією пристроїв, які використовуються для автентифікації. Порівняно з працівниками, які можуть мати пристрій, наданий організацією, — підрядники, працівники за контрактом, відряджені та спільні підприємства, — швидше за все, його не мають. Підрядники можуть нараховуватися десятками тисяч або більше, а також можуть змінюватися щомісяця за кількістю та окремими користувачами. Люди в цих ролях використовують застарілу автентифікацію, імена користувачів і паролі, і таким чином створюють ризик, оскільки якщо ці облікові дані скомпрометовано, ризик збільшується. Це підвищує потребу в надійній автентифікації, яка не піддаватиметься фішингу. Серед нетехнічної спільноти також слід враховувати потребу в освіті та навчанні, щоб люди могли розпізнавати загрози та вразливі місця.

Спільне середовище робочої станції

Спільні робочі станції – це пристрої, кіоски або обчислювальні середовища, якими користуються кілька користувачів, які іноді називають «пересувними користувачами», де кілька людей проходять автентифікацію на одній робочій станції. Ці системи є критично важливими для повсякденних операцій і часто мають прямий зв'язок із критично важливими системами та даними, що посилює внутрішню загрозу, будь то зловмисну чи недбалу, і створює додаткові ризики безпеці при використанні в місцях із високим трафіком.

Mobile-restricted environments

Call centers

Airgap environments

High-security sites

Industrial (no connection, oil rigs, etc)

OT та середовища з обмеженим доступом до мобільних пристроїв

Середовище з обмеженим доступом до мобільного зв'язку – це сценарій, за якого мобільні пристрої не можна використовувати через фактори, пов'язані з самим середовищем, як-от спеціальне обладнання (з повітряним проміжком або SCADA) або ізольовані мережі, суворе середовище офлайн або офшорні місця, веб-сайти з високим рівнем безпеки або через обмеження, накладені нормативними актами, профспілками, або коли мобільні пристрої просто не рекомендовані політикою компанії. Також може існувати підгрупа користувачів в організації, які не бажають використовувати персональні мобільні пристрої для робочих цілей, вимагаючи іншого методу автентифікації. Мобільні обмежені середовища часто включають спільні робочі станції, і ці станції можуть мати спеціальні вимоги до входу та виходу.

Організаціям, що займаються енергетикою та природними ресурсами, щоб забезпечити безпечні робочі процеси в середовищах з обмеженим доступом до мобільних пристроїв і одночасно прискорити бізнес, — їм необхідно розглянути рішення MFA, яке легко подолає унікальні проблеми безпеки та продуктивності.

Польові IoT-пристрої

Інтернет речей (IoT) перетворює цю галузь, підвищуючи автоматизацію та ефективність обладнання, що використовується у видобутку нафти та газу, до інструментів, які використовуються для моніторингу споживання кінцевих користувачів. Завдяки використанню пристроїв IoT і даних, зібраних з них, енергетичний сектор зміг створити інтелектуальні мережі, «розумні мережі», що дозволяє оптимізувати пристрої та активи, підключені до мережі, забезпечуючи підвищену гнучкість керування системами. Контроль суворого доступу до цих мереж має важливе значення, тому що якщо будь-хто зможе отримати доступ до зібраних даних або отримати контроль, це може завдати серйозної шкоди, порушивши роботу служб.

Безсумнівно, ця мережа підключених кінцевих точок, включаючи дані, що збираються через неї, має бути безпечною та зашифрованою протягом усього наскрізного циклу. Ось чому для захисту пристроїв Інтернету речей потрібні апаратні рішення, такі як апаратні модулі безпеки (HSM), які забезпечують максимальну безпеку навіть у найбільш агресивних середовищах.

Безпека фізичного доступу

Загрози можуть бути кібернетичними або фізичними, тому також слід враховувати внутрішні загрози. Зважаючи на величезну кількість дуже дорогого обладнання та конфіденційної інформації, фізична безпека все ще є основною проблемою. Наприклад, цілеспрямована снайперська атака на енергосистему у Каліфорнії спричинила збитки на суму близько 15 мільйонів доларів США, що призвело до перебоїв у роботі служби.[14] Контроль за тим, хто має доступ до фізичного місцезнаходження, є життєво важливим для забезпечення того, щоб конфіденційна інформація та доступ надавалися лише тим особам, чия робота цього вимагає.

Зростання кількості кібератак і розширення повноважень різних федеральних і державних установ підкреслюють величезну потребу інвестувати в безпеку, яка забезпечує комплексний захист для всієї критичної інфраструктури та систем у сфері енергетики та природних ресурсів. Щоб захиститися від зловмисного програмного забезпечення, наприклад «Pipedream», і фішингових атак, важливо розуміти роль і вплив якісної автентифікації.

Безпечний доступ за допомогою сучасної, захищеної від фішингу багатофакторної автентифікації

94%

витоків даних в енергетиці пов'язані з обліковими даними – це більше, ніж у будь-якій іншій галузі [15]

Недоліки застарілої автентифікації

Не всі форми MFA створені однаковою мірою для захисту від кібератак або з точки зору забезпечення оптимального балансу надійної безпеки зі швидким і простим інтерфейсом користувача (UX), що забезпечує високу продуктивність. Важливо відзначити, що хоча будь-яка форма двофакторної або багатофакторної автентифікації забезпечує більшу безпеку, ніж одні тільки паролі, застаріла автентифікація, як і раніше, спирається на паролі як на перший фактор — все ще небезпечний, все ще неефективний, який, як і раніше, є джерелом розчарування співробітників. Небезпечні методи роботи з обліковими даними лише посилюють ці ризики витоку даних.

У застарілому MFA другий фактор часто пов'язаний із мобільним пристроєм. Мобільні автентифікатори збільшують кількість кроків у процесі автентифікації, вимагаючи від користувачів очікування одноразового пароля або надсилання кодів додатків, або, у випадку з користувачами в енергетичних і газових організаціях, зняття важких рукавичок для процесу автентифікації. Питання безпеки є однією з найважливіших причин, чому мобільні телефони не можна використовувати в певних ситуаціях на борту нафтової вишки,[16] і багато компаній і місцеві закони забороняють використання особистих телефонів та інших розумних пристроїв на нафтових вишках.[17] Серед цих проблем є багато червоних прапорців, включаючи аспекти, перелічені нижче:

- Можуть бути проблеми з доступністю мобільних пристроїв, які своєчасно надсилають коди через погане з'єднання або ненадійні служби.
- Немає реальної гарантії, що приватний ключ опиниться на безпечному елементі мобільного пристрою.
- OTP або приватний ключ може бути перехоплено якимось чином (наприклад, через заміну SIM-карти)

Заміна застарілої однофакторної автентифікації (ім'я користувача та пароль) і автентифікації на основі мобільних пристроїв на стійку до фішингу MFA є першим кроком у покращенні практик безпеки для захисту IT- та OT-середовищ.

Стійкий до фішингу – це процес автентифікації, захищений від зловмисників, які перехоплюють або навіть обманом змушують користувачів розкрити інформацію про доступ. Не всі MFA вважаються стійкими до фішингу. Стійкий до фішингу MFA кваліфікується лише як PIV/Smart Card і FIDO2/WebAuthn, як зазначено в Меморандумі з Управління та бюджету M-22-09.

Ризик захоплення облікового запису

0%

FIDO ключ безпеки (YubiKey)

10%

Підказка на пристрої

21%

Додатковий email

24%

SMS-код

50%

Номер телефона

YubiKey

- Доведено, що запобігає 100% захоплень облікових записів[18]
- Забезпечує зручність роботи
- Вхід у 4 рази швидший, ніж OTP[19]
- Не прийдеться покладатися на стільникову мережу або акумулятор
- Висока міцність — сертифікація IP68: пилонепроникність, стійкість до роздавлювання та водонепроникність

Майбутнє без пароля

Зрештою, дії користувача є найбільшою слабкістю застарілої автентифікації, а багатоетапна автентифікація значною мірою сприяє незадоволенню користувачів, тому найкраща світова практика рухається до автентифікації без пароля – автентифікації, яка не вимагає від користувача надання пароля при вході.

Традиційні смарт-карти дійсно забезпечують високий рівень безпеки, але зазвичай потребують великих капітальних витрат (CapEx) для пристроїв для зчитування смарт-карток, фізичних карток, на додаток до серверних платформ керування. Завдяки цьому галузь у цілому рухається до процесу входу до системи без пароля з використанням сучасних стандартів автентифікації, таких як FIDO2/WebAuthn, які добре працюють із хмарою, що призводить до зниження поточних витрат, навіть якщо підприємства розширюються.

Сучасний стандарт автентифікації FIDO (Fast IDentity Online) забезпечує надійну двофакторну, багатофакторну та безпарольну автентифікацію. FIDO2/WebAuthn – це найновіша версія стандарту FIDO, яка використовує криптографію з відкритим ключем для забезпечення високого рівня безпеки, де закриті ключі ніколи не залишають автентифікатор, що забезпечує сучасну двофакторну, багатофакторну та навіть безпарольну автентифікацію. Для організацій, що займаються енергетикою та природними ресурсами, які мають застарілі системи OT і низьку толерантність до непродуктивних завдань, апаратні ключі безпеки FIDO2, такі як YubiKey, пропонують багатофакторну автентифікацію без пароля з високим рівнем безпеки та винятковим інтерфейсом для організацій, що займаються енергетикою і природними ресурсами, які мають застарілі системи OT і низьку стійкість до невиробничих завдань, і забезпечують підтримку кількох протоколів для SmartCard, OTP, OpenPGP, FIDO U2F і FIDO2/WebAuthn на одному ключі.

Сучасна захищена від фішингу автентифікація та безпарольна автентифікація за допомогою YubiKey

YubiKey від Yubico забезпечує сучасну надійну автентифікацію в масштабах усього ланцюжка постачання, допомагаючи організаціям та їхнім постачальникам запроваджувати надійну, просту у використанні автентифікацію для будь-якого користувача, який має висхідний доступ до мережі або при передачі важливих IP-адрес.

За допомогою YubiKey організації, що займаються енергетикою та природними ресурсами, можуть розгорнути стійку до фішингу багатофакторну автентифікацію без пароля в будь-якому масштабі, за допомогою апаратного ключа безпеки, що захищає приватні секрети на захищеному елементі, який неможливо легко зламати. YubiKey пройшов перевірку на відповідність згідно з Федеральним стандартом з обробки інформації FIPS 140-2 і стійкий до імітації особи, що робить його вельми придатним для регульованих середовищ і перевершує вимоги нових нормативних актів, таких як Указ 14028, Меморандум M-22-09 та Управління та бюджету (OMB), для посилення кібербезпеки зі структурами з «нульовою довірою», включаючи розгортання MFA, стійкої до фішингу.

YubiKey доступний у різноманітних форм-факторах, і один ключ можна використовувати на кількох пристроях, різноманітних сучасних і застарілих IT- та OT-середовищах, а також із сотнями програм і сервісів. Вони спеціально розроблені для роботи в деяких із найсуворіших місць, як то: спільна робоча станція, середовища з обмеженим мобільним зв'язком, ізольовані території та морські бурові установки. Користувачі можуть отримати вигоду від легкого робочого процесу автентифікації – підключіть YubiKey до порту USB і натисніть кнопку для автентифікації або просто торкніться до пристрою YubiKey за допомогою NFC (добре підходить для середовищ без іскри).

Для подальшого покращення користувальницького досвіду та швидкості автентифікації Yubico також пропонує серію YubiKey Bio — FIDO Edition з підтримкою FIDO U2F і FIDO2, яка забезпечує фірмову безпеку, якою відомі всі YubiKey з новим безпарольним інтерфейсом на основі біометричних даних.

> «Ми впровадили YubiKey у наші системи SCADA, які працюють з електроенергією, щоб підвищити безпеку за допомогою MFA. Цей процес дозволяє оператору приходити на зміну, швидко автентифікуватися і вживати необхідних заходів без будь-яких збоїв у роботі системи. MFA гарантує, що лише автентифіковані користувачі можуть отримати доступ до керування системою».
>
> –Чад Ллойд, Директор з архітектури кібербезпеки управління енергоспоживанням, Schneider Electric

Забезпечення безпеки ланцюжка постачання та критично важливих систем

В організаціях, що займаються енергетикою та природними ресурсами, безперервний рух найважливіших ресурсів має вирішальне значення для доставки цих ресурсів світу. Одним із ризиків, властивих безпеці ланцюжка постачання, є можливість порушення цілісності, якості або надійності продукту, програмного забезпечення або послуги, що постачається. Можливість автентифікації обладнання та машин також є невід'ємним компонентом забезпечення безпеки операцій. Взаємозв'язок між трьома основними секторами — висхідним, середнім і низхідним — і великими організаціями, що існують між усіма, впливає на якість безпеки, оскільки вони настільки ж безпечні, наскільки безпечна їхня найслабша ланка.

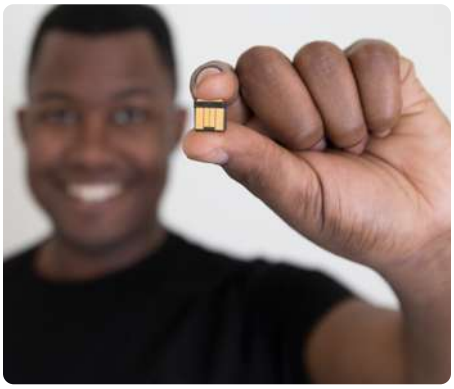
Забезпечення найвищої цілісності деталей і пристроїв Інтернету речей

Щоб уникнути небажаного тиражування та крадіжки, а також для забезпечення якості, вкрай важливо переконатися, що всі компоненти, задіяні в наскрізному процесі, є автентичними. Як наслідок, завжди має бути готове рішення для захисту цілісності та інтелектуальної власності всіх компонентів і ресурсів у всіх процесах на вищому, середньому та нижчому рівнях.

Традиційний підхід до захисту інтелектуальної власності (IP) і запобігання підробкам передбачає використання цифрових криптографічних ключів та шифрування. Криптографічні ключі зберігаються або в програмному забезпеченні, яке є дуже вразливим, або в апаратній моделі безпеки (HSM). На жаль, традиційні стелажні HSM і HSM на основі карт є великими та дорогими, що робить їх непрактичними на нафтових вишках, промислових об'єктах, у центрах обробки даних або для пристроїв IoT. При розгляді пристроїв IoT різні дані, включаючи інформацію про навколишнє середовище та облікові дані, що зберігаються всередині них, необхідно контролювати та захищати за допомогою шифрування та дешифрування. Якщо зловмисник порушує або змінює потік даних між IoT-пристроями, це може спричинити проблеми з регулюванням або поставити компанію у важкий чи скомпрометований стан. Як наслідок, ці пристрої потребують заходів безпеки, які захищають ці дані та захищають ці потенційні точки збою.

Захист зовнішнього коду та даних

Організації, які використовують програмне забезпечення у своїх продуктах, повинні мати метод безпечного підпису коду для прийому коду або даних із зовнішніх джерел. Потреба в рішеннях для безпечного підпису коду зросла останнім часом, як продемонстрували наслідки атаки SolarWinds. Під час цієї атаки хакери скористалися проломом у системі підпису коду SolarWinds, що дозволило їм шахрайським шляхом поширювати шкідливий код як законні оновлення для понад 18 000 установок продукту SolarWinds Orion по всьому світу.[20] Крім того, потужність криптографічного рішення, яке ви використовуєте, настільки ж надійна, як і метод атестації вашого партнера в ланцюжку постачання. Тому дуже важливо, щоб ці партнери могли продемонструвати ланцюжок контролю над кодом, який повертається до комп'ютера початкового розробника.



Захист інтелектуальної власності, продуктів та пристроїв за допомогою YubiHSM 2

Важлива не тільки автентифікація користувачів, а й автентифікація між IT- та OT-системами, включаючи частини продукту і машини. Yubico створила ультрапортативний і недорогий YubiHSM 2, найменший у світі модуль HSM, виконаний у нано-форм-факторі. YubiHSM 2 забезпечує безпечне, захищене від несанкціонованого доступу зберігання та роботу ключів, запобігаючи копіюванню та розповсюдженню криптографічних ключів, а також дистанційній крадіжці ключів, що зберігаються у програмному забезпеченні. YubiHSM 2 можна застосовувати до будь-якого процесу, де необхідно керувати секретами та автентичністю компонентів, а також де необхідно запобігти несанкціонованому втручанню. Це рішення захищає облікові дані та повноваження, що зберігаються на пристроях IoT, і захищає їх за допомогою шифрування, що створює додаткові рівні безпеки. Компактний розмір YubiHSM2, мінімальні вимоги до живлення та той факт, що його можна підключати безпосередньо до обладнання, не вдаючись до монтажу на стелажі, роблять його гнучким у використанні та розгортанні.

YubiHSM 2 може захистити та бути легко розгорнутим на будь-яких:				
USB-роз'є-мах на серверах	Базах даних	Роботизованих складальних лініях	Додатках	Пристроях IoT у польових умовах

YubiHSM 2 гарантує, що тільки сертифіковані станції програмування можуть взаємодіяти з передбачуваними компонентами або робити цифрові підписи на кожен компонент для забезпечення цілісності. В обох сценаріях додаткова безпека YubiHSM2 допомагає підтримувати репутацію компанії і дає їй душевний спокій. Він ідеально підходить для захисту ключів підпису та сертифікатів як для коду підпису, так і для створення цифрових підписів, допомагаючи підтримувати секрети, якими спільно користуються в ланцюжку постачання. Але навіть окрім цих варіантів використання, організації отримують можливість впроваджувати інновації та вирішувати більш широкий спектр бізнес-сценаріїв за допомогою YubiHSM2, ніж будь-коли раніше. Для організацій, яким необхідно відповідати вимогам FIPS 140-2, також є опція YubiHSM 2 FIPS із перевіркою FIPS 140-2, рівень 3, щоб забезпечити найвищий рівень захисту даних на додаток до суворих рівнів відповідності.

Важливо відзначити, що криптографічні ключі, які використовуються для підпису та/або сертифікації компонентів, ніколи не розкриваються за межами обладнання YubiHSM 2, що забезпечує високий рівень надійності та безпеки. Щоб проілюструвати це на прикладі, навіть якщо віддалений зловмисник зможе скомпрометувати мережу або конкретно комп'ютер, підключений до пристрою, все одно немає очевидних векторів атаки, оскільки ключі не можуть бути вилучені. З іншого боку, якщо той самий зловмисник зможе отримати повний базовий доступ до еквівалента програмного забезпечення, він може принаймні запустити аналіз пам'яті, підключеної бази даних або навіть локальних файлів на потенційні слабкі місця чи шаблони.

ПРИКЛАД З ПРАКТИКИ

Забезпечення безпеки систем та ланцюжка постачання у Schneider Electric

Schneider Electric є лідером у галузі цифрової трансформації управління енергоспоживанням та автоматизації, виробництва електричних деталей та систем управління живленням, включаючи систему диспетчерського управління та збору даних (SCADA), що використовується для віддаленого управління критично важливою інфраструктурою (наприклад, центрами обробки даних, лікарнями, нафтовими та газовими підприємствами).

YubiKey дозволив Schneider Electric інтегрувати MFA в ізольовану систему, не покладаючись на Інтернет або менш безпечну автентифікацію на основі SMS, спростивши автентифікацію під час передачі робочої зміни. YubiKey також використовується в ситуаціях управління, коли потрібні дії блокування нагляду. Сучасний MFA через YubiKey був частиною процесу успішного проходження сертифікації IEC-62443 SL2.

«Безпека та захищеність мають першорядне значення для Schneider Electric і знаходять відображення у всьому, що ми робимо», — зазначає Чад Ллойд, Директор з архітектури кібербезпеки управління енергоспоживанням у Schneider Electric. «У рамках нашої сертифікації IEC SL2 ми включили MFA до нашої системи управління енергоспоживанням, що дозволить нам відповідати вимогам SL3 у майбутньому. Тепер це відмінна риса Schneider Electric», — сказав Ллойд.

На додаток до інтеграції YubiKey у свої системи SCADA, які використовуються клієнтами в критичній інфраструктурі, Schneider Electric вжила заходів для забезпечення якості та цілісності свого ланцюжка постачання, використовуючи апаратний модуль безпеки YubiHSM для інтеграції з ключовими постачальниками у виробничому процесі. Криптографічне апаратне забезпечення високого рівня безпеки YubiHSM допомагає підтримувати процеси ретельного тестування та виробництва всіх оригінальних продуктів Schneider Electric.

> «Щоб заздалегідь захистити наш ланцюжок постачання, ми тісно співпрацюємо з ключовими постачальниками для створення подвійного шифрування, оскільки і постачальник, і Schneider Electric використовують модулі YubiHSM, вбудовані у виробничий процес».
>
> Чад Ллойд, Директор з архітектури кібербезпеки управління енергоспоживанням, Schneider Electric

Yubico пропонує просту закупівлю та розповсюдження стійких до фішингу засобів захисту у будь-якому масштабі

Yubico також пропонує послуги YubiEnterprise Services, які складаються з Підписки YubiEnterprise та Доставки YubiEnterprise, щоб допомогти спростити придбання та розповсюдження ключів YubiKey для співробітників у різних місцях у будь-якому масштабі.

Підписка YubiEnterprise

Завдяки YubiEnterprise Subscription організації отримують доступну модель придбання YubiKey на основі послуг із такими перевагами, як передбачувані витрати, оновлення до останніх пропозицій, підтримка клієнтів тощо. Це особливо важливо для організацій, у яких спостерігається часта плинність кадрів.

Доставка YubiEnterprise

Завдяки YubiEnterprise Delivery організації отримують автентифікацію «під ключ» з доставкою YubiKey, відстеженням та обробкою повернення продуктів Yubico, які безперешкодно обробляються експертами з логістики, тому організації можуть зосередитись на найважливішому – забезпеченні безпеки робочої сили.

Команда Професійних послуг Yubico може надати технічне та операційне керівництво, щоб допомогти оптимізувати впровадження та розгортання YubiKey із послугами, які відповідають вашим потребам.

Економічні переваги YubiKey

Крім технологічних і безпекових переваг YubiKey також має економічні переваги. У цьому розділі демонструється приклад проблеми автентифікації та запропоновані розрахунки, які організації, що займаються енергетикою та природними ресурсами, можуть використати для отримання очікуваних економічних вигод від розгортання YubiKey для надійної двофакторної, багатофакторної або безпарольної автентифікації.

СИТУАЦІЯ

Розглянемо компанію X, що займається виробництвом енергії та природних ресурсів:

Структура компанії: 10 000 співробітників і 10 000 підрядників (які змінюються щомісяця), котрі працюють над процесом виробництва та розподілу енергії у висхідному, середньому та низхідному потоках. На відміну від співробітників, підрядники не мають доступу до мобільних пристроїв, що надаються компанією, тому вони не мають доступу до мобільних МФА, якими в даний час користуються співробітники. У процесі виробництва та розподілу енергії існує кілька критичних систем, яким потрібний безпечний доступ для операцій з даними та управління системою.

Що не дає їм спати вночі: Зростаюче занепокоєння щодо повторюваних кібератак, а також звітів про погану роботу користувача з автентифікацією, що ставить під сумнів продуктивність працівників, підвищує витрати на підтримку, що також може бути пов'язано з більш тривалим часом виходу на ринок.

Непродуктивна автентифікація: У відгуках співробітників говориться, що поточний процес двофакторної автентифікації, який використовується в корпоративному IT-середовищі, який включає ім'я користувача та пароль, а також код токена TOTP, є неефективним для кількох разів протягом робочого дня, коли співробітники повинні проходити автентифікацію, щоб використовувати IT- та OT-системи і робочі станції. Крім того, однофакторна автентифікація на основі імені користувача та пароля, яку використовують підрядники, не забезпечує захист від сучасних кібератак і призводить до затримок у виробництві та збільшення витрат на IT, коли працівники забувають свій пароль і потребують зв'язку зі службою підтримки.

КІНЦЕВИЙ СТАН: ПЕРЕХІД НА БЕЗПАРОЛЬНУ АВТЕНТИФІКАЦІЮ

Офіс CISO зараз вивчає засоби переходу на середовище автентифікації без пароля як для співробітників, так і для підрядників з двох основних причин. По-перше, щоб зменшити вплив зовнішніх загроз, які зазвичай добре фінансуються внутрішніми кібер-зловмисниками, а також відомими національними державами, і призначені для порушення критичної інфраструктури та ланцюжка постачання. Друга причина полягає в покращенні взаємодії з користувачем, щоб підвищити ефективність і продуктивність.

Через небезпечні ризики, пов'язані з використанням мобільних телефонів у середовищах OT, таких як нафтові вишки чи енергетичні установки, автентифікація на основі мобільних пристроїв тут не підходить, тому компанія X шукає рішення, яке пропонує високий рівень захисту від сучасних загроз, простий користувальницький досвід і високу довговічність середовища операційних технологій. Стратегічним пріоритетом компанії X є запровадження безпарольної стратегії на основі FIDO2 із використанням апаратного ключа безпеки, такого як YubiKey, що додасть значну додаткову цінність організації як у IT-, так і в OT-середовищах для її працівників, а також для підрядників, працівників за контрактом, відряджених і для спільних підприємств. Для цілей цієї вправи на рентабельність інвестицій (ROI) нижче термін «користувач» використовуватиметься для позначення власних працівників, підрядників, контрактних працівників, відряджених або спільних підприємств.

ПРОГНОЗ ТА ЦІЛІ ROI

Передбачається, що перехід на YubiKey від Yubico з можливостями NFC, який підтримує сучасний протокол автентифікації FIDO2, вирішить усі вищезазначені проблеми.

Мета полягає в тому, щоб обчислити розумну, досяжну та правдоподібну віддачу від інвестицій (ROI), яка була підтверджена концепцією та позитивно відображає зобов'язання та інвестиції в довгострокову стратегію автентифікації. Для цілей цієї вправи це означає стандартний для всього підприємства метод перевірки ідентичності користувача без використання пароля. Розрахунки рентабельності інвестицій покажуть річну віддачу від процесів на вищому, середньому та нижчому рівнях, від YubiKey порівняно з автентифікацією за іменем користувача та паролем, яка часто використовується підрядниками та контрактними працівниками, а також віддачу YubiKey від рішення автентифікації TOTP, яке часто використовують працівники підприємства.

Після порівняння витрат на придбання YubiKey з використанням постійного ліцензування та YubiKey з використанням ліцензування на основі передплати прогнозується, що перехід на розширений рівень YubiEnterprise Subscription (YES) Yubico, включаючи YubiKey з можливостями NFC, які підтримують сучасний протокол автентифікації FIDO2, вирішить усі вищезазначені проблеми та забезпечить найкращу віддачу від інвестицій.

КОРОТКИЙ ОГЛЯД ROI

Покращений досвід автентифікації та підвищення продуктивності: Завдяки простому входу в систему натисканням/дотиком і простоті використання YubiKey це спонукає очікувати, що середній час автентифікації/входу для користувачів різко скоротиться з розрахунку на кожного користувача, який понаднормово виконує вхід до IT- та OT-систем, що дозволяє їм переорієнтувати свою продуктивність на інші задачі. Зважаючи на різні місця розташування підрядників, контрактників, відряджених співробітників та спільних підприємств (корпоративний офіс, робота в польових умовах), їм необхідне завжди доступне рішення MFA.

Зменшення витрат на службу підтримки: Більшість дзвінків до служби підтримки IT компанії X пов'язані зі скиданням пароля. IT-менеджмент хотів би зменшити витрати та час, витрачений на дзвінки для скидання пароля, перейшовши до моделі самообслуговування та, зрештою, до середовища без пароля.

Усунення загроз і втрата безперервності бізнесу: Враховуючи той факт, що найбільший обсяг викрадення облікових даних відбувається в результаті успішних фішингових атак, компанія X очікує значного скорочення витрат, пов'язаних з усуненням кіберзагроз та зусиллями щодо усунення наслідків, включаючи аналіз загроз, тим самим знижуючи витрати на штат аналітиків центру операцій із безпеки (SOC), що важливо для зниження ризиків впливу на бренд. Крім того, закриття об'єкта через атаку може призвести до втрати бізнесу, критичних збоїв у роботі кінцевих клієнтів, регулятивних штрафів і пов'язаних з атаками юридичних витрат і витрат на судові виплати.

РОЗРАХУНКИ ROI

Після всебічного аналізу наведених вище випадків використання компанія X вирішила рухатися далі з YubiKey. До кінця 2024 року компанія X прийде до однорідної безпарольної стратегії на основі FIDO2. Обрана пропозиція YubiEnterprise Subscription включає Пріоритетні послуги підтримки, а також 25% накладних витрат YubiKey на відтік співробітників.

Зараз компанія X використовує автентифікацію на основі імені користувача та пароля, а також автентифікацію на основі TOTP у своїй організації. Заміна автентифікації на основі імені користувача та пароля на FIDO2 без пароля з використанням YubiKey з ліцензуванням передплати для підрядників, контрактних працівників, відряджених та спільних підприємств призведе до річного прибутку приблизно 6 208 333,33 доларів США. Заміна автентифікації TOTP для співробітників призведе до річного прибутку приблизно 17 617 333,33 доларів США. Обидва сценарії передбачають значне скорочення часу автентифікації, перенаправлення часу співробітників на інші пріоритети (підвищення продуктивності), зменшення кількості дзвінків у службу підтримки та, таким же чином, зменшення успішних фішингових загроз для кінцевих користувачів, у результаті центру операцій із забезпечення безпеки доводиться вирішувати менше справ. Річний дохід обох сценаріїв автентифікації не включає витрати на прибуток, пов'язані з перерозподілом часу користувача на результати з більш високим пріоритетом. Вважається, що одержані економічні дані, як показано нижче, є консервативною передбачуваною оцінкою.

РОЗРАХУНКИ ROI

У таблиці 1 наведено зведення кожного оціненого економічного впливу, розрахованого на основі цілей індивідуального варіанту використання.

Таблиця 1: Резюме рентабельності інвестицій

ПРИКЛАД ВИКОРИСТАННЯ: ПРОЦЕС ВИРОБНИЦТВА ТА РОЗПОДІЛУ ЕНЕРГІЇ | АВТЕНТИФІКАЦІЯ				
Подробиці	Кількість користувачів	Вартість поточного логіна та пароля	Поточна вартість TOTP	Вартість з YubiKey
Досвід автентифікації та підвищення продуктивності перенаправлених користувачів	10,000	$5,692,000.00	$11,386,000.00	$2,846,000.00
Витрати на службу підтримки	—	$58,333.33	$58,333.33	—
Витрати на усунення загроз	—	$864,000.00	$864,000.00	$0.00
Загальна річна вартість	—	$6,614,333.33	$12,308,333.33	$2,846,000.00
Вартість ліцензування YubiKey (безстрокова)				$1,110,000.00
Річна вартість ліцензування YubiKey (підписка)				$420,000.00
Передбачуваний річний дохід YubiKey (безстроковий) порівняно з ім'ям користувача та паролем				$5,518,333.33*
Розрахунковий річний дохід від передплати YubiKey у порівнянні з ім'ям користувача та паролем				$6,208,333.33**
Очікуваний річний дохід YubiKey (безстроковий) порівняно з TOTP				$17,127,333.33*
Розрахунковий річний прибуток від передплати YubiKey у порівнянні з TOTP				$17,617,333.33**

*Поточна вартість + Приріст продуктивності - (Вартість з YubiKey + Вартість безстрокової ліцензії YubiKey)

**Поточна вартість + Приріст продуктивності - (Вартість з YubiKey + Вартість ліцензії на підписку YubiKey)

У таблиці 2 наведено вхідні дані та розрахунки переходу від автентифікації за іменем користувача, паролем і TOTP до FIDO2 або без пароля на основі смарт-картки з YubiKey, зокрема порівняння поточного часу, необхідного для цих процесів, і його порівняння з оновленою автентифікацією YubiKey разом із економією коштів, і переваги підписки.

Таблиця 2: Вхідні дані та обчислення досвіду автентифікації

КОМПАНІЯ X ВХОДИ		
Кількість користувачів у сценарії	10,000	Вхідне значення
Середня погодинна ставка оплати (користувач)	50	Вхідне значення
Середня хвилинна ставка оплати (користувач)	0.83	Вхідне значення
Робочих днів на рік	200	Вхідне значення
Кількість годин у робочому дні	8	Вхідне значення
Час входу в програму (у хвилинах) на користувача на рік лише з ім'ям користувача та паролем	1,253	Тест Forrester: 1253 хвилини на рік дорівнюють у середньому 3,43 хвилинам на день, витраченим на доступ до програм
Час входу в програму (у хвилинах) на користувача на рік із TOTP	2,506	Припустимо, що це подвоює час від базового часу введення імені користувача та пароля, тобто 1253×2
Час входу в програму (у хвилинах) на користувача на рік з YubiKey	626.5	Google Stat: YubiKey у 4 рази швидше, ніж введення OTP (Google Authenticator)

ВАРТІСТЬ АВТЕНТИФІКАЦІЇ	Поточна вартість імені користувача та пароля	Поточна вартість TOTP	Вартість з YubiKey	
Час входу в програму (у хвилинах) на користувача на добу	3.43	6.86	1.715	Введіть значення зверху
Вартість автентифікації/працівник/день	$2.846	$5.693	$1.423	хвилинна швидкість користувача* загальний середньодобовий час авторизації
Загальна щоденна вартість автентифікації (на загальну кількість користувачів у разі використання)	$28,460.00	$56,930.00	$14,230.00	вартість за авторизацію / співробітник/день * #кількість користувачів
Загальна річна вартість досвіду автентифікації	$5,692,000.00	$ 11,386,000.00	$2,846,000.00	загальна щоденна вартість автентифікації * робочі дні на рік

РОЗРАХУНКОВА ВАРТІСТЬ YUBIKEY БЕЗТЕРМІНОВО		
Вартість ліцензування YubiKey для 10 000 користувачів	$1,100,000.00	Ліцензія YubiKey (YubiKey 5C NFC $110 за 2 упаковки)
Річна вартість послуг підтримки з урахуванням Пріоритетної підтримки	$10,000.00	Вартість Пріоритетної підтримки Yubico
Загальні розрахункові витрати YubiKey (безстрокове ліцензування)	$1,110,000.00	Ліцензування YubiKey + витрати на підтримку

РІЧНА РОЗРАХУНКОВА ВАРТІСТЬ ПІДПИСКИ YUBIKEY		
Річна вартість ліцензування YubiKey для 10 000 користувачів (первинний ключ)	$240,000.00	Вартість підписки на YubiKey (YubiKey 5C NFC) $24
Річна вартість ліцензування YubiKey для 10 000 користувачів (резервний ключ)	$180,000.00	Вартість підписки YubiKey на резервний ключ (знижка 25%)
Річна вартість послуг підтримки з урахуванням Пріоритетної підтримки	—	Безкоштовно при ліцензуванні за підпискою
Total Annual Estimated YubiKey Costs (subscription licensing)	$420,000.00	Річна вартість первинних ключів для всіх користувачів + річна вартість резервних ключів для всіх користувачів

У таблиці 3 показано вхідні дані та розрахунки переходу від автентифікації за іменем користувача, паролем і TOTP до FIDO2 або безпарольного використання смарт-картки за допомогою YubiKey, а також результат значно покращеного досвіду користувача, який повертає час назад на кожну спробу автентифікації/вхід, кілька разів на день у процесі виробництва та розподілу енергії.

Таблиця 3. Вхідні дані та розрахунки підвищення продуктивності перенаправлених користувачів

ВАРТІСТЬ АВТЕНТИФІКАЦІЇ	Поточна вартість логіна та пароля	Поточна вартість TOTP	Вартість з YubiKey	
Час входу в програму (у хвилинах) на користувача на добу	3.43	6.86	1.715	Введіть значення зверху
Кількість робочих хвилин на рік		96,000		Кількість робочих днів на рік* кількість годин на робочий день* кількість хвилин на годину
Час входу в програму (у хвилинах) на користувача на рік	686	1,372	343	Час входу в програму (у хвилинах) на користувача за добу* кількість робочих днів
Час входу в програму (у годинах) на користувача на рік	11.43	22.86	5.71	Час входу в програму (у годинах) на користувача на рік / 60
Загальний відшкодований час (години) на користувача на рік YubiKey порівняно з ім'ям користувача та паролем	–	–	5.72	Час входу в програму (у годинах) на користувача на рік [ім'я користувача та пароль – YubiKey]
Загальний відшкодований час (години) на користувача на рік YubiKey порівняно з TOTP	–	–	17.15	Час входу в програму (у годинах) на користувача на рік [TOTP – YubiKey]
Загальний відшкодований час (години) на рік YubiKey порівняно з ім'ям користувача та паролем	–	–	57,200	Загальний відшкодований час на користувача на рік * кількість користувачів
Загальний відшкодований час (години) на рік YubiKey порівняно з TOTP	–	–	171,500	Загальний відшкодований час на користувача на рік * кількість користувачів
Річна вартість продуктивності YubiKey порівняно з ім’ям користувача та паролем	–	–	$2,860,000.00	Загальний відшкодований час (години) на рік * середня погодинна ставка оплати (користувач) [ім’я користувача та пароль - YubiKey]
Вартість продуктивності на рік YubiKey порівняно з TOTP	–	–	$8,575,000.00	Загальний відшкодований час (години) на рік * середня погодинна ставка оплати (користувач) [TOTP - YubiKey

Організації можуть використовувати наведені нижче формули для розрахунку передбачуваної економії витрат з метою варіанта використання: скорочення витрат на службу підтримки та економія на усуненні загроз.

Зменшення витрат на службу підтримки:

Вхідні дані та розрахунки щодо переходу від автентифікації за іменем користувача, паролем і TOTP до FIDO2 або без пароля на основі смарт-картки за допомогою YubiKey, а також усунення запитів на «скидання пароля», скорочення кількості нових кадрів для навчання та постійна підтримка всіх користувачів, що мають відношення до досвіду покращеної автентифікації. Використані значення вхідних даних дивіться у додатку.

Загальна вартість = Погодинна вартість FTE повністю завантаженого працівника служби підтримки × кількість співробітників служби підтримки, які звертаються до запитів пароля/автентифікації × час на одного працівника на заявку × кількість заявок на працівника.

Витрати на усунення загрози:

Вхідні дані та обчислення переходу від автентифікації на основі імені користувача і пароля та автентифікації TOTP до FIDO2 або автентифікації без пароля на основі смарт-картки за допомогою YubiKey, а також їх вплив на кіберзагрози та усунення загроз через асинхронні методи без використання загального секрету, які зупиняють фішинг облікових даних, зловмисне програмне забезпечення і кібератаки, керовані людиною посередині. Автентифікація на основі TOTP не вважається стійкою до фішингу відповідно до вказівок NIST, тому витрати на усунення загрози за допомогою автентифікації на основі імені користувача і пароля та автентифікації на основі TOTP будуть однаковими з урахуванням того, що TOTP може бути підданий фішингу. Поточна розрахована вартість не включає порушення даних, пов'язане з простоєм виробництва, юридичні збори, виплати програм-здирників, внески кіберстрахування чи штрафи регуляторів. Використані значення вхідних даних дивіться у додатку.

Загальна вартість FTE на аналіз/виправлення (або кілька виправлень) = Погодинна вартість FTE повністю завантаженого аналітика безпеки × кількість аналітиків, які беруть участь у зусиллях з усунення передбачуваної крадіжки облікових даних, про яку було повідомлено або яку було виявлено × кількість годин, витрачених на розслідування.

Додаток

Кількість співробітників служби підтримки (у випадку використання)	10	Вхідні дані
Середній погодинний FTE працівника служби підтримки	50	Вхідні дані
Середній похвилинний FTE працівника служби підтримки	0.83	Вхідні дані
Кількість робочих днів на рік робітника служби підтримки	200	Вхідні дані
Вартість роботи одного працівника служби підтримки за день	29.17	Загальна кількість годин на день одного працівника* погодинна ставка
Загальна вартість скидання пароля за день	291.67	Вартість одного співробітника служби підтримки в день* кількість співробітників служби підтримки
Загальна річна вартість скидання пароля	58,333.33	Загальна вартість скидання пароля за день* кількість робочих днів на рік
Кількість запитів на скидання пароля в службу підтримки на день	5	Вхідні дані
Середня кількість хвилин, необхідних для запиту на скидання пароля	7	Вхідні дані
Загальна кількість хвилин на день, необхідних для запитів на скидання пароля	35	#запити * хвилин у середньому
Загальна кількість годин на день, необхідних для запитів на скидання пароля	.58	#щоденні хвилини / 60
Кількість співробітників аналітиків SOC (у випадку використання)	10	Вхідні дані
Середня погодинна ставка аналітика SOC для усунення загроз	90	Вхідні дані
Середня (у хвилинах) швидкість аналітика SOC у виправленні загрози	1.50	Вхідні дані
Робочі дні (на рік) аналітика SOC для усунення загроз	200	Вхідні дані
Кількість невирішених спроб фішингу на день	6	Вхідні дані
Середня кількість хвилин, необхідних для аналізу та виправлення	48	Вхідні дані
Загальна кількість хвилин на день на аналітика SOC	288	#невирішених на день * середня кількість хвилин на аналіз
Загальна кількість годин на день на аналітика SOC	4.80	всього хвилин / 60
Щоденна вартість аналітика SOC	432.00	Загальна кількість годин на день на одного аналітика SOC * Середня погодинна ставка аналітика SOC для усунення загроз
Загальна щоденна вартість аналітика SOC	4,320.00	Щоденна вартість аналітика SOC * кількість співробітників аналітики SOC
Загальна річна вартість усунення загроз	864,000.00	Загальна щоденна вартість аналітика SOC * робочі дні/рік усунення загроз аналітика SOC

Забрати

The YubiHSM 2 і YubiHSM 2 FIPS

Зліва направо: YubiHSM 2 і YubiHSM 2 FIPS

The YubiKey 5 Series

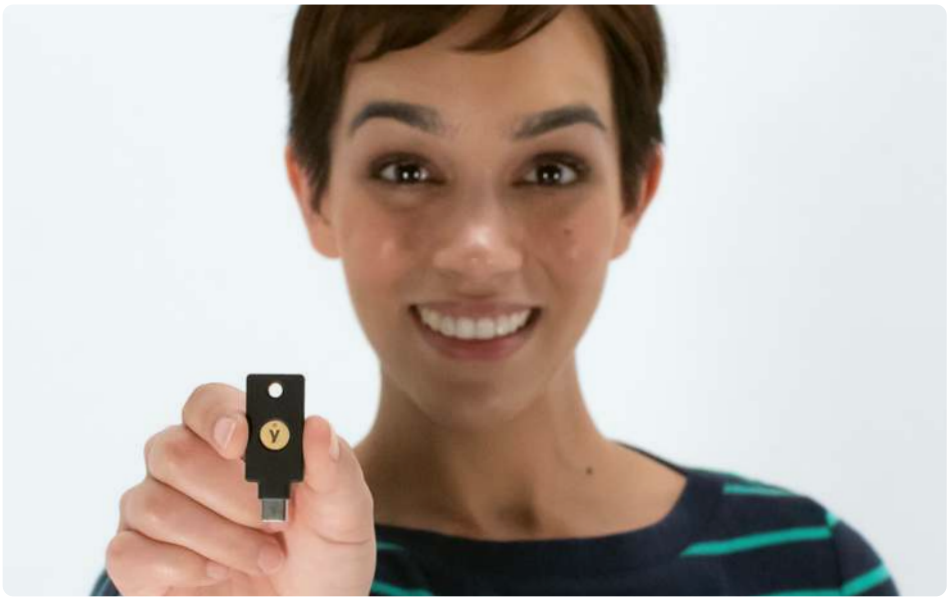
Зліва направо: YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano та YubiKey 5C Nano

Через постійний розвиток складності кібератак потреба в модернізації автентифікації як ніколи своєчасна і необхідна. У результаті провідні організації розгортають автентифікацію без пароля та ультрапортативний і гнучкий HSM для захисту від сучасних кіберзагроз. Ці рішення мають бути зручними для користувача та економічно ефективними в масштабі, водночас дуже довговічними, щоб відповідати різноманітним робочим середовищам, у яких перебувають користувачі, наприклад, у польових умовах, у корпоративному середовищі чи на нафтовій платформі.

Проактивність і захист ваших даних, людей і критичної інфраструктури за допомогою правильного рішення безпеки може допомогти вам пом'якшити атаки, мінімізувати рівень проникнення атак і захистити ваші безцінні ресурси, які впливають на світ.

Сучасні кіберзагрози вимагають рішень безпеки Yubico. YubiKey і YubiHSM2 — це безпечні, портативні, адаптовані та прості у використанні рішення, розроблені для задоволення різноманітних потреб енергетичних і природних організацій, де вони знаходяться, допомагаючи безперебійно підтримувати застарілу інфраструктуру, а також сприяти її інтеграції в сучасні хмарні системи.

Будьте попереду серед загроз, що постійно розвиваються, завдяки найкращій у своєму класі безпеці, яка забезпечить вам успіх не лише зараз, а й у майбутньому.



Виноски

[1] IBM, Звіт про вартість витоку даних за 2022 р. (станом на 31 жовтня 2022 р.)
[2] Bloomberg, Хакери зламали колоніальний трубопровід, використовуючи скомпрометований пароль (4 червня 2021 р.)
[3] Industrial Cyber, WEF оцінює кібератаки, спрямовані на європейський енергетичний сектор (8 лютого 2022 р.)
[4] Politico, «TSA облажалося»: правила трубопровідної кібербезпеки стикаються з серйозними перешкодами (17 березня 2022 р.)
[5] Курт Томас, Анжеліка Мосціцкі, Нове дослідження: Наскільки ефективна базова гігієна облікового запису при запобіганні зламу (17 травня 2019 р.)
[6] PR Newswire, Guidehouse Insights прогнозує, що ринок кіберстрахування для енергетики зростатиме із сукупним річним темпом зростання майже 18% до 2030 р. (10 березня 2022 р.
[7] Інститут Ponemon, Звіт про стан безпеки паролів і автентифікації за 2020 р. (лютий 2020 р.)
[8] BlueVoyant, Управління кіберризиками в розширеній екосистемі постачальників 2021 (1 червня 2022)
[9] Onlogic, Що таке система SCADA і як вона працює? (20 квітня 2022 р.)
[10] CISA, Alert (AA22-103A), APT Cyber Tools, націлені на пристрої ICS/SCADA (25 травня 2022 р.)
[11] CHERNOVITE PIPEDREAM проти зловмисного програмного забезпечення, націленого на промислові системи контролю (ICS) (13 квітня 2022 р.)
[12] Trusted Computing Group, захист промислового Інтернету речей в енергетичному секторі (24 січня 2022 р.)
[13] Nexus Integra, IoT в енергетичному секторі: моніторинг і аналіз змінних (станом на 1 липня 2022 р.)
[14] Річ Кастанья, Безпека енергетичної мережі стає ще складнішою завдяки IoT (18 серпня 2020 р.)
[15] Verizon, Звіт про розслідування витоку даних за 2021 рік (станом на 18 травня 2022 р.)
[16] Арнольд та Іткін, «Як офшорні працівники спілкуються з близькими» (станом на 25 травня 2022 р.)
[17] Арнольд та Іткін, «Як офшорні працівники спілкуються з близькими» (станом на 25 травня 2022 р.)
[18] Курт Томас, Анжеліка Мосціцкі, Нове дослідження: наскільки ефективна базова гігієна облікового запису в запобіганні викраденню (17 травня 2019 р.)
[19] Курт Томас, Анжеліка Мосціцкі, Нове дослідження: наскільки ефективна базова гігієна облікового запису в запобіганні викраденню (17 травня 2019 р.)
[20] SEC, Форма 8-K SolarWinds Corporation (14 грудня 2020 р.)

yubico

Про Yubico

Як винахідник YubiKey, Yubico робить безпечний вхід простим і доступним для всіх. Компанія є лідером у встановленні глобальних стандартів безпечного доступу до комп'ютерів, мобільних пристроїв тощо. Yubico є творцем і основним учасником стандартів FIDO2, WebAuthn і FIDO Universal 2nd Factor (U2F) і відкритих стандартів автентифікації.

YubiKey є золотим стандартом стійкої до фішингу багатофакторної автентифікації (MFA), що дозволяє одному пристрою працювати з сотнями споживчих і корпоративних програм і сервісів.

Yubico є приватною компанією, яка представлена по всьому світу. Для отримання додаткової інформації відвідайте: www.yubico.com.