USAID
FROM THE AMERICAN PEOPLE

ОСНОВИ ОПЕРАЦІЙНИХ ТЕХНОЛОГІЙ, КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ІТ-ІНТЕГРАЦІЇ КІБЕРБЕЗПЕКИ

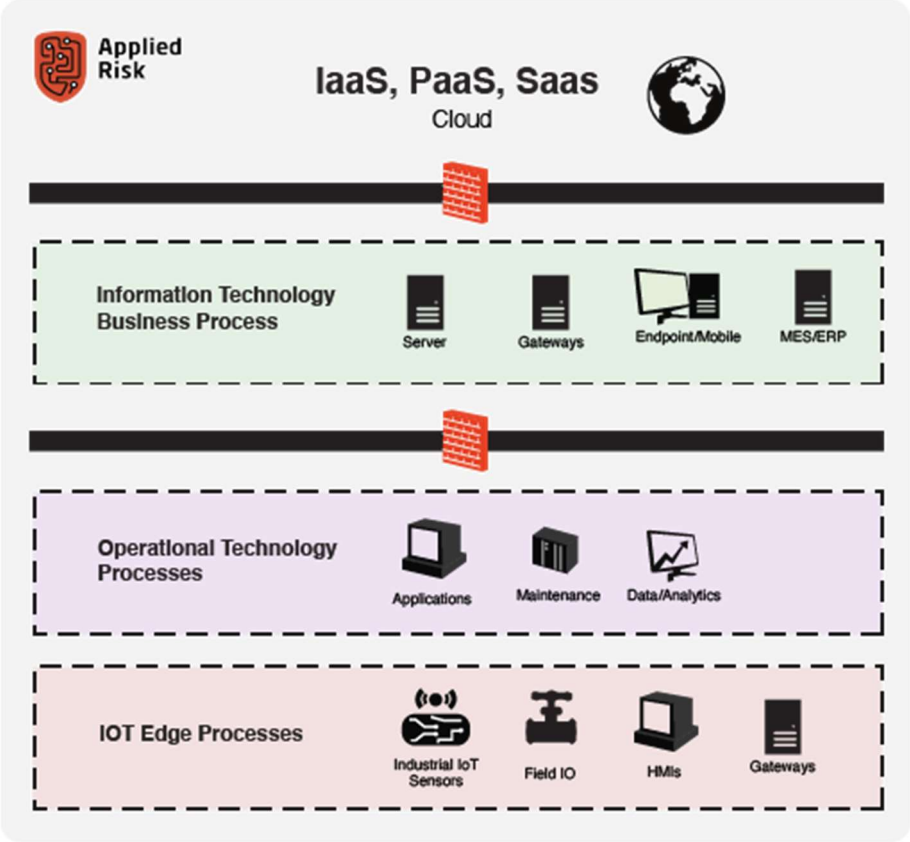
Цей документ підготовлений на замовлення USAID. Його самостійно підготував партнер-виконавець «Каталісто» для діяльності USAID «Кібербезпека критичної інфраструктури в Україні». Погляди авторів, висловлені в цьому документі, не обов'язково відображають погляди USAID або уряду Сполучених Штатів.

МОДУЛЬ 5 - ВСТУП

IT та OT (операційні технології) все більше перетворюються на одну і ту саму сутність і наближаються до спільного набору бізнес-цілей та завдань на майбутнє багатьох галузей. Мотивовані зростанням Промислового Інтернету Речей (Industrial IoT), Industry 4.0 та новими бізнес можливостями, представленими цифровою трансформацією, багато організацій вже розпочали інтеграції IT/OT та вже отримують переваги та аналізують ризики, пов'язані з такими моделями ведення бізнесу.

Ряд досліджень показує, що компанії частіше інтегрують OT-системи у свої бізнес-моделі, ніж у минулому. Однією з ключових переваг від конвергенції IT та OT є підвищення якості інформації для кращого прийняття рішень. Це дозволяє виробникам розпочати трансформацію даних, згенерованих машинами та процесами, у цінні інсайти, такі як прогнозне обслуговування.

Слід заохочувати та сприяти конвергенції IT та OT на рівнях технологій, безпеки та процесів (безпека як механізм підтримки бізнесу). В той час, як конвергенція та інтеграція OT приносить покращення, існуючі технологічні розробки потребують менеджерів, відповідальних за сферу OT, щоб розпочати дискусію про те, як підтримувати інфраструктури безпечними, гнучкими та сучасними. Однак, щоб це сталося, організації повинні визнати важливість середовищ IT та OT та їхню готовність до конвергенції, чого часто не вистачає, оскільки сьогодні для багатьох видів обладнання бракує необхідної інфраструктури.



IT/OT Architecture

КІБЕРБЕЗПЕКА ОТ (ОПЕРАЦІЙНИХ ТЕХНОЛОГІЙ)

Сфери ОТ та кібербезпеки досі розвиваються, і кількість задокументованих інцидентів досі є відносно невеликою. Категоризація є важливим кроком до визначення трендів і остаточного визначення вразливих місць та управління ризиками.

Цілісний підхід є необхідним для подолання додаткових випробувань, що являється передумовою конвергенції IT та ОТ, а також для захисту необхідної інфраструктури. Нижче наведені декілька важливих аспектів для обговорення:

Управління: Нові методи роботи вимагають значних інвестицій в культуру компанії, особливо у зміну управління IT/OT (ролей та відповідальності), в управління ризиками у сферах IT та ОТ, у подолання проблем у мережах постачання та управлінні залежностями та сервісами, такими як Cloud.

Еталонна архітектура IT/OT: Існує потреба у комплексній еталонній архітектурі IT/OT, що включає в себе повний набір компонентів та рівнів, від пристроїв до хмарних сервісів. Зони та канали передачі інформації повинні бути переглянуті.

Ризик та відповідність: Оцінка ризиків, моделей небезпек та мереж у кіберпросторі, що можуть вести до ваших найважливіших активів (включно з безпекою) є ключовим першим кроком для подолання кібератак. Крім цього, відповідність стандартам індустрії, таким як IEC 62443, та безпечне розділення інфраструктури на зони та канали передачі інформації, посилює безпеку. Відповідність регіональним і галузевим нормам, таким як Директива ЄС NIS, додає передбачуваність вашим основним послугам.

Обізнаність щодо ситуації та розвідка загроз: Нещодавні інциденти в галузі кібербезпеки, такі як атака на SolarWinds, підтвердили потребу впровадження нових стратегій для покращення обізнаності у сфері кібербезпеки та стійкості щодо загроз. Таким чином, це дасть вам можливість усвідомити небезпеку та відреагувати на неї швидко.

Обізнаність у сфері кібербезпеки та тренінги: Посилене впровадження IT -рішень у середовищах ОТ підкреслює необхідність навчання операторів та інженерів, аналітиків SOC та персоналу з управління кращим практикам та гігієні безпеки у конвергентному середовищі IT/OT. Треті сторони також потребуватимуть навчання, оскільки такі постачальники послуг часто відповідають за завдання, пов'язані з IT та ОТ.

Розуміння свого IT/OT середовища, знання нормативних вимоги та розробка правильного плану дій для підвищення безпеки вимагає значної технічної експертизи. Applied Risk надає індивідуальні та орієнтовані на клієнта рішення, котрі допомагають власникам активів, системним інтеграторам та постачальникам розробляти, розгортати та підтримувати кіберстійку інфраструктуру/сервіс, що неодмінно допоможе вам досягти ваших бізнес-цілей.

Якщо вам потрібна підтримка у будь-якому із згаданих у цій статті аспектів, або ви хотіли б проконсультуватися щодо ваших вимог по безпеці ОТ, не вагаючись звертайтеся до нас для отримання більш докладної інформації або поради від наших експертів.

ШІСТЬ КЛЮЧОВИХ ПРАВИЛ ЩОДО ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРЗАГРОЗ.

Критична інфраструктура визначається як активи, центральні системи та стратегічні мережі, як фізичні, так і цифрові, котрі є настільки важливими для країни, що їх вихід з ладу чи руйнування можуть мати негативний вплив на фізичну безпеку, далі на економіку, національну систему охорони здоров'я або на декілька з цих аспектів у будь-якій комбінації.

Агенція США з кібербезпеки та безпеки інфраструктури розглядає 16 секторів критичною інфраструктури, від комерційних об'єктів до ядерних реакторів. Щоб ці сектори вважалися частиною критичної інфраструктури, вони повинні бути настільки життєво важливими, що їхнє руйнування може призвести до помітної соціально-економічної кризи із потенційною безпекою для суспільства. Якщо ці сектори буде пошкоджено, складно буде підрахувати політичні та стратегічні наслідки, а також шкоду, завдану безпеці.

На рівні держави, щоб зменшити та протистояти загрозам критичній інформаційній інфраструктурі, потрібно підтримувати баланс між потребою у запобіганні, стримуванні, ідентифікації та викритті атаки з ефективною стратегією реагування, управління кризовими ситуаціями, контролем нанесеної шкоди та, у підсумку, протоколом повернення до звичайної роботи. Це завдання вимагає повного розуміння усіх точок перетину між зловмисниками та розширенням атакованого середовища.

УНІКАЛЬНІ ВИКЛИКИ ДЛЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПОРІВНЯНО З ІНШИМИ СЕКТОРАМИ

Те, що об'єднує ці важливі галузі, часто є поєднанням необхідного стратегічного планування для забезпечення базової кібербезпеки та спеціалізованих процесів ізоляції оперативної мережі, спеціальних протоколів безпеки та, здавалося б, нескінченної кількості критично важливих файлів, що вимагають постійної чистки.

Згідно нещодавнього звіту «Делойт»: «Програми для захисту найбільш необхідних частин інфраструктури спрямовані на подолання лише фізичних загроз, залишаючи країни вразливими до кібератак, починаючи від руйнування сервісів до зазіхання на безпеку усього суспільства»

Цей сегментований підхід до безпеки вимагає переоцінки мислення щодо ризиків, якщо він має намір керувати зростанням кіберризиків. Повторний розгляд має інтегрувати загальнодержавні інституції з державно-приватною співпрацею, щоб зосередитись на підвищенні обізнаності та формуванні єдиної відповіді на кіберзагрози.

Цей сегментований підхід до безпеки вимагає перегляду та змін у ставленні до ризиків. Без цього неможливо керувати кіберзагрозами, кількість яких зростає. Перегляд ставлення до ризиків повинен стосуватися загальнодержавних інституцій та співпраці між державою та приватним сектором, щоб зосередитись на підвищенні обізнаності та формуванні уніфікованого реагування на кіберзагрози.

КЛЮЧОВІ ПРОЦЕСИ ДЛЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У критичній інфраструктурі є певна кількість ключових процесів, які можуть сильно покращити кібербезпеку. Ці ключові інструкції прояснюють та модернізують систему захисту критичної інфраструктури.

Тут наведено деякі із найбільш важливих процесів:

ПРАВИЛА ТА ВІДПОВІДНІСТЬ ІНДУСТРІЇ

Загальногалузеві нормативні акти (наприклад, стандарти Північноамериканської корпорації з енергонадійності із захисту критичної інфраструктури (NERC CIP)) та штрафи підвищують рівень їх дотримання. І це навіть більш правильно, коли невідповідність вимогам індустрії та встановленим державою правилам, призводить до суттєвих фінансових наслідків. Для багатьох секторів критичної інфраструктури баланс між юридичними дозволами та новими технологічними рішеннями може залишити прогалини, що ще більше підкреслює важливість запровадження стандартизованого підходу щодо зменшення кіберризиків.

Ізолювання оперативної мережі

Ізолювання життєво-важливих систем (наприклад, управління енергопостачанням або відведенням стічних вод) від зовнішніх мереж зменшує атаковану поверхню, але ви також повинні врахувати, що загальносистемні оновлення можуть стати більш складними.

«Слабкі місця» чистки від зайвих файлів

У зв'язку із величезною кількістю важливих даних, а також зовнішньої інформації та файлів, що потребують інтеграції у ізольовані мережі, сектори необхідної інфраструктури повинні стандартизувати процедуру загального очищення системи для запобігання потрапляння вірусів та шкідливих елементів з мереж із недостатнім рівнем безпеки.

Інструменти для підтримання безпеки

Технічних рішень для зменшення кібер-ризиків наразі не бракує. Можливості варіюються від включення декількох рівнів рішень безпеки на основі пісочниці до ізоляції, від розширених мереж до обмеження доступу користувачів до життєво-важливих серверів до різних рівнів процесів шифрування.

Оскільки кожен із 16 секторів необхідної інфраструктури стикається з унікальним середовищем ризиків, інтегрування цих загальних процедур безпеки, а також SOAR (Координування, автоматизація та реагування у кібербезпеці) або SIEM (Інформація про кібербезпеку та управління подіями) може забезпечити найсильнішу технічну базу для кібербезпеки у багатьох із важливих індустрій.

Освіта

Згідно звіту компанії «Kaspersky» щодо стану кібербезпеки у 2019 році, "Помилки працівників та ненавмисні дії були причиною 52% інцидентів, що вплинули на OT та системи індустріального контролю (ICS) мереж протягом минулого року, як показали дослідження."

Оскільки такий великий сегмент інцидентів у кібербезпеці припадає на брак обізнаності працівників та розуміння того, що таке звичайний фішинг та інші подібні тактики, одним з перших кроків до захисту необхідної інфраструктури повинно стати виділення більшої кількості часу на поглиблення знань про кібербезпеку на рівні всієї організації.

Оновіть та застосуйте патчі для усього програмного забезпечення та технологій

Зупинка потоку вірусних програм до критичної інфраструктури не може бути здійснена без впровадження в систему оновлень та встановлення захистів всюди, включно із серверами та точками підключення (ендпоінтами).

За даними CIO, "57% жертв кібератак повідомляють, що цим порушенням цілісності систем безпеки можна було запобігти, встановивши доступний патч». Про це йдеться у новому дослідженні ServiceNow , проведеному Інститутом Понемон. 34% респондентів цього дослідження знали щодо наявності вразливих місць на момент атаки. В той час, як хакери створюють нові та більш токсичні вірусні програми, щоб знищити цілі сектори, багато хто використовує наявні віруси, о ведуть до драматичного результату.

Забезпечення цілісності критичної інфраструктури

У той час, як деякі сектори використовують проактивний підхід до кібербезпеки, зменшуючи ризики та шукаючи вразливі елементи своїх систем захисту, переважна більшість секторів критичної інфраструктури є неготовою до рівня і масштабів кібертероризму, який може вразити їхні життєво-важливі системи.

Коротко кажучи, щоб кібербезпека стала дійсно базовим елементом довготермінового захисту критичної інфраструктури, потрібно активно встановлювати захисти та оновлювати системи, навчати працівників та користувачів, підтримувати організації приватного сектору, створювати нові законопроекти для затвердження жорстких покарань та штрафів за невідповідність вимогам, впроваджувати різноманітні інструменти для підтримання безпеки та протоколи загального зменшення ризиків у кіберпросторі.

МАТЕРІАЛИ ТА ПОСИЛАННЯ

1. Модуль_5_Whitepaper1-integrating_cybersecurity_0
2. Модуль_5_Whitepaper2-deloitte-building-cyber-security-into-critical-infrastructure
3. Модуль_5_Whitepaper3-Comprehensive Guide to Operational Technology Cybersecurity
4. https://www.researchgate.net/publication/349969874_Understanding_the_Challenge_of_Cybersecurity_in_Critical_Infrastructure_Sectorshttps://www.cisecurity.org/white-papers/cis-controls-v8-mapping-to-nist-csf/