Кібербезпека промислової автоматизації: бачення Trend Micro

Захист систем АСУ/ОТ пов'язаний зі специфічними проблемами, вирішення яких потребує особливих інструментів.

У листопаді фірма Mandiant, дочірня компанія Google з кібербезпеки, оприлюднила результати розслідування інциденту, спричиненого 10 жовтня 2022 року в Україні злочинним гравцем Sandworm, який діє в інтересах російського ГРУ. Тоді одночасно з масованим ракетним ударом, якого завдала країна-агресор, хакери здійснили вплив на автоматичні вимикачі однієї з підстанцій, що призвело до знеструмлення, а згодом запустили в IT-середовище жертви програму-вайпер.

Фахівці Mandiant встановили, що Sandworm отримав доступ до OT-середовища через гіпервізор, який містив копію системи SCADA. Початкову точку входу вони знайти не змогли, але з дослідження можна виснувати, що SCADA не була ізольованою від Інтернету, а загалом, як часто буває, енергетична система не мала ні периметрального захисту з контролем промислових протоколів, ані рішень, які здійснюють кореляцію даних і пов'язують інциденти в мережі у єдиний ланцюжок атаки.

Іншою проблемою є використання на промислових об'єктах застарілих версій ОС Windows. У січні 2023 року Microsoft припинила випуск оновлень безпеки для Windows 7 у рамках платної програми розширеної підтримки і водночас перестала оновлювати Windows 8.1, для якої ця програма не планувалась. Проте ці ОС поширені в промисловості, і далеко не завжди є можливість замінити їх на новіші версії.

За даними дослідження, що його провів у 2023 році SANS Institute, 25% організацій вважають загрози безпеці АСУ серйозними або критичними, ще 43% ризик високим, і цей тренд посилюється з року в рік. Респонденти виділили три найпроблемніші місця: видимість в мережі специфічних для АСУ/ОТ протоколів; можливість оцінювання і розуміння ризиків; і виявлення загроз, що можуть поширюватись в АСУ через зовнішні пристрої (ноутбуки тощо), які підключаються для виконання різних завдань. При цьому, зазначають дослідники, ешелонований захист конкретно для АСУ є не просто приємним бонусом, а необхідністю, але водночас треба виходити за межі реагування і діяти на випередження.

Компанія ELKO Ukraine має в своєму арсеналі рішення, які роблять все це можливим.

Vision One: від реагування до випередження

Платформа кібербезпеки Trend Micro Vision One поєднує функції розширеного виявлення і усунення загроз (XDR) і управління ризиками, спричиненими поверхнею атаки (ASRM). Платформа не лише захищає різноманітні IT-ресурси (електронну пошту, кінцеві точки, хмари тощо), а й охоплює промислові мережі, OT-системи і пристрої IoT, розділяючи корпоративну мережу і виробниче середовище і убезпечуючи ресурси, які не можуть бути захищені стандартними агентами. Мережеві сенсори, які входять до складу платформи, «розуміють» промислові протоколи та вміють аналізувати трафік IT– й OT-систем.

XDR здійснює кореляцію даних, отриманих з різних джерел (робочих станцій, серверів, мобільних пристроїв, хмарних навантажень і т. ін.), використовуючи як власні сенсори, так і глобальні ресурси кіберрозвідки і сторонні джерела даних. Єдина інформаційна панель дає змогу виявляти і розслідувати підозрілу поведінку, зловмисне ПЗ, програми-здирники та інші серйозні атаки, і реагувати на них. Trend Micro має 250 млн сенсорів по всій земній кулі і дослідницькі центри практично у всіх регіонах, де знаходяться злочинні організації і відбуваються атаки. Опираючись на дані цієї кіберрозвідки, Vision One забезпечує наскрізну видимість усього «життєвого циклу» атакувальної кампанії, здійснює профілювання зловмисників, ідентифікує відомі та новопосталі кіберзлочинні угруповання, що дає змогу залишатися на крок попереду хакерів.

До складу платформи входить віртуальний помічник на базі генеративного ШІ, який зрозумілими словами пояснює тривожні сповіщення, від простих до найскладніших, а також прискорює пошук загроз, перекладаючи текстові питання у формальні пошукові запити.

Понад те, Vision One виходить за рамки виявлення загроз і реагування на них, забезпечуючи ідентифікацію потенційних ризиків і їх усунення ще до того, як станеться злам або інший інцидент. Платформа дає змогу визначити усю

Рис. 1. Контроль поверхні атаки в системі Vision One

можливу поверхню атаки, тобто мати список усіх пристроїв, облікових засобів, IoT-обладнання тощо. Наступними кроками є оцінювання ризиків і автоматичне закриття вразливостей для скорочення поверхні атаки. Це спрямовано, з одного боку, на зменшення ймовірності успішної атаки, а з іншого – на мінімізацію наслідків (**рис. 1**).

Поєднання XDR і ASRM створює синергію, яка покращує захист. Дані, зібрані в XDR, вдосконалюють пріоритезацію ризиків, а дії щодо реагування на інциденти використовуються для усунення вразливостей, що виключає повторення цих інцидентів. ASRM же надає дані про потенційні шляхи атак для розслідування інцидентів, а випереджальне закриття дір скорочує число інцидентів і зменшує «втому від сповіщень».

Stellar: промисловий EDR для робочих станцій

Традиційні антивіруси погано пристосовані до використання в АСУ промислових об'єктів. По-перше, вони вимагають постійного оновлення бази сигнатур, а для цього потрібне постійне підключення до Інтернету. По-друге, сканування файлів відбирає частину ресурсів процесора і пам'яті і може впливати на роботу АСУ. Система захисту кінцевих точок у виробничому середовищі має свої пріоритети: вона не повинна в жодному разі заважати виробничим процесам, обчислення не повинні сповільнюватися, а прийняття рішень – затримуватися.

З огляду на це компанія TXOne (спільне підприємство Trend Micro і Moxa) створила рішення Stellar, яке є системою виявлення і знешкодження загроз у кіберфізичних системах (CPSDR) – аналогом EDR для промислових середовищ. В її основі знаходяться агенти, які збирають телеметрію щодо пристроїв, операційних систем, мереж і програм, формуючи «цифрові відбитки» базового стану. Надалі агенти постійно порівнюють поведінку пристроїв з базовими параметрами і блокують несподівані зміни. На наступному етапі більш докладний аналіз визначає причину зміни (зовнішня загроза, помилка оператора чи щось інше).

В партнерстві з виробниками обладнання TXOne підтримує базу даних, яка містить інформацію про понад 8 тис. застосунків, пристроїв та сертифікатів. Своєю чергою, Stellar може передавати дані в XDR (**рис. 2**).

Агент Stellar розроблений спеціально для пристроїв з обмеженими ресурсами, тож і займає мало місця. Окрім того, завдяки інтелектуальній фільтрації даних він споживає на 90% менше трафіку без зменшення точності та ефективності роботи. Агенти є автономними, тому ізольовані пристрої також захищені, а оновлення здійснюються через USB-носії (підключення таких носіїв теж контролюється). Підтримка різних версій ОС – як актуальних, так і застарілих, починаючи з Windows 2000, – гарантує захист існуючого обладнання впродовж його життєвого циклу.

Захисна «флешка»

Додатково для захисту ізольованих систем TXOne пропонує рішення Portable Inspector – USB-пристрій, який підключається до обладнання і виявляє та знищує зловмисне ПО. Встановлювати захисні програми або перезавантажувати систему при цьому не потрібно. Паралельно зі скануванням Portable Inspector проводить інвентаризацію системи (інформація про комп'ютер, статус оновлень Windows, список програм тощо). Апаратний засіб шифрування AES-256 дає змогу безпечно переносити в ізольоване середовище важливі файли. Portable Inspector сумісний з різними платформами, зокрема Windows і Linux, і забезпечує захист навіть для застарілих версій, таких як Windows XP та Windows 7.

Щоб убезпечити роботу з самими знімними пристроями, TXOne створила рішення Safe Port, яке має два роз'єми USB і сенсорний дисплей для відображення процесу й результатів сканування. Safe Port сканує носії інформації зі швидкістю 7200 файлів за хвилину. Уся історія перевірених пристроїв доступна фахівцям з кібербезпеки.

Дані з Portable Inspector і SafePort передаються у платформу централізованого управління ElementOne. Завдяки їй організація може бачити усі свої ресурси і пов'язані з ними ризики. Зведення показує тип кожного ресурсу, його ОС, 10 останніх відсутніх патчів та інші критичні вразливості. Також за допомогою ElementOne адміністратори можуть конфігурувати Portable Inspector під потреби різних груп: кожна отримує доступ до конкретних ресурсів, що мінімізує ризик витоку даних.

Отримати консультацію та придбати рішення Trend Micro та TXOne можна в компанії ELKO Ukraine. Як офіційний дистриб'ютор комплексних рішень, ELKO надає партнерам усі необхідні ресурси для успішного розвитку бізнесу: активну підтримку в питаннях захисту інвестицій партнера у проєкті; бізнес-кейси та рекомендації з розвитку бізнесу; можливість придбати сервісну підтримку і отримати консультації інженерів; демо-ліцензії; допомогу у проведенні пілотних проєктів та при проєктуванні; навчання співробітників компаній-партнерів; та багато іншого.

+38 044 461 9670,
elko@elko.ua,
https://www.elko.ua

Рік який ми прожили, був повним новин. Вийшли нові продукти та технології, з'явились нові виробники рішень інформаційної безпеки, нові цікаві звіти команд Threat Hunting.
Ми мали змогу відчути кібератаки та їхні наслідки на собі та своєму житті. Відчуваю, що в новому році нам ще не один раз доведеться проявити стійкість.
Отже, бажаю всім у прийдешньому році стати кращими та мати більшу стійкість, адже випробувань для нас завжди буде вистачати!

Роман ЧОРНЕНЬКИЙ,
керівник напрямку кібербезпеки ELKO Ukraine

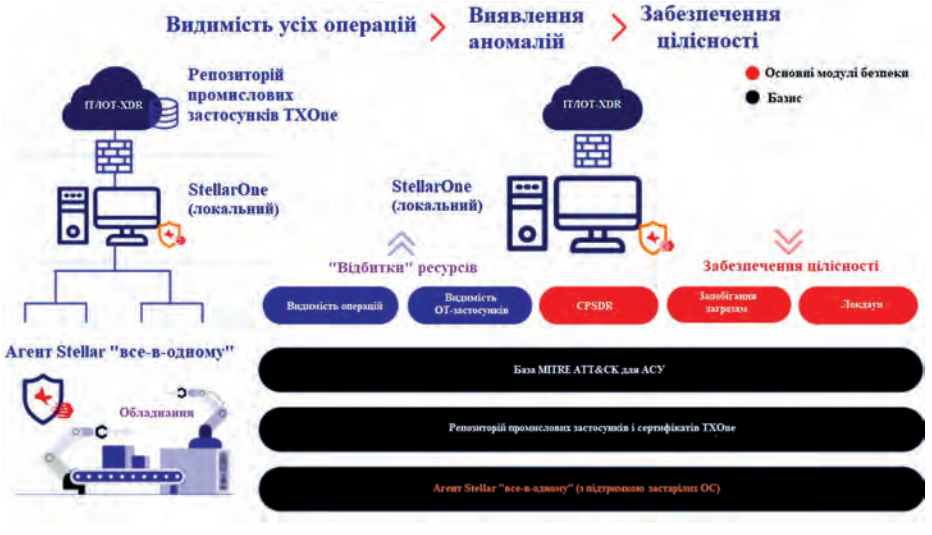

Рис. 2. Технологічний стек TXOne Stellar