Безшумна оборона.

Як передбачити наступну кібератаку?

Промислові системи управління (ICS) є серцевиною всіх промислових процесів – від генерації електроенергії до очистки стічних вод і промислового виробництва. ICS включають системи диспетчерського управління та збору даних (SCADA), розподілені системи управління (DCS), віддалені термінальні пристрої (RTU), програмовані логічні контролери (PLC). Несправність будь-якої з цих складових може привести до аварії промислового технологічного процесу з серйозними економічними втратами та загрозами для громадської безпеки.

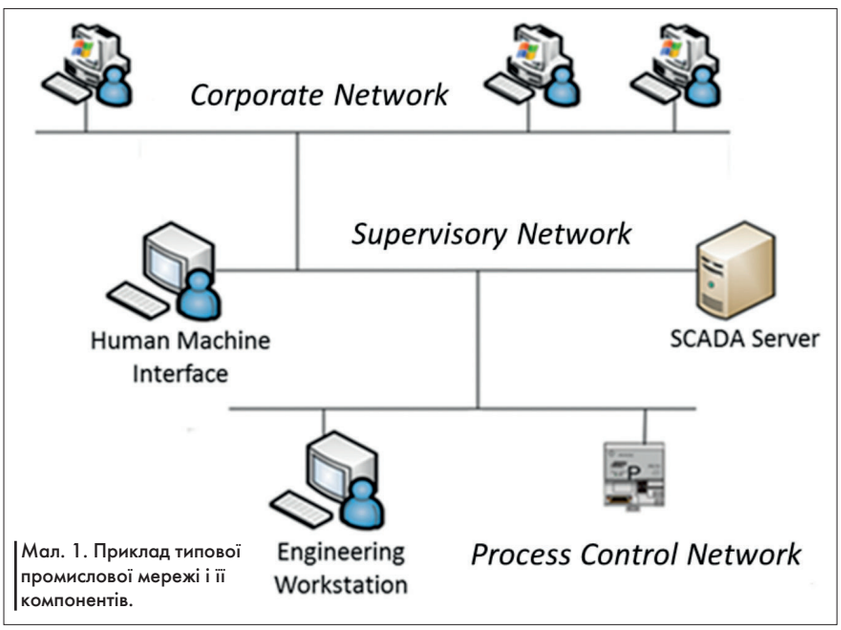
Павло Гірак, *pavel.girak@soliton.com.ua*

За матеріалами SecurityMatters: www.secmatters.com/resources

На необхідності моніторингу ICS та промислових комунікаційних мереж наголошується в рекомендаціях і стандартах, таких як Electricity Subsector Cybersecuirity Capability Maturity Model (ES-C2M2), NERC CIP, директива Європейського Союзу M/490, стандарт IEC 62443. Найбільш критичними активами підприємства є ті, що знаходяться в мережі диспетчерського та технологічного управління, оскільки вони забезпечують повне управління вразливими технологічними процесами (мал. 1).

Основними загрозами для промислових мереж є:

1. Зловмисні чи недбалі оператори;
2. Несподіване порушення конфігурації;
3. Цілеспрямована програмна атака невідомої вразливості;
4. Поширення шкідливих програм.



Мал. 1. Приклад типової промислової мережі і її компонентів.

Атака на промислові системи

Показовим прикладом атаки на промислову систему управління є інцидент в українських енергомережах, що відбувся 23 грудня 2015 року, відразу після Дня енергетика. Ця подія викликала серйозний резонанс в світовому інформаційному просторі. Одночасні атаки були здійснені на інформаційну інфраструктуру «Прикарпаттяобленерго», «Чернівціобленерго» та «Київобленерго». Перерва в електропостачанні склала від 1 до 3,5 годин. Загальний недовідпуск – 73 МВт*год (0,015% від добового обсягу споживання України) [1].

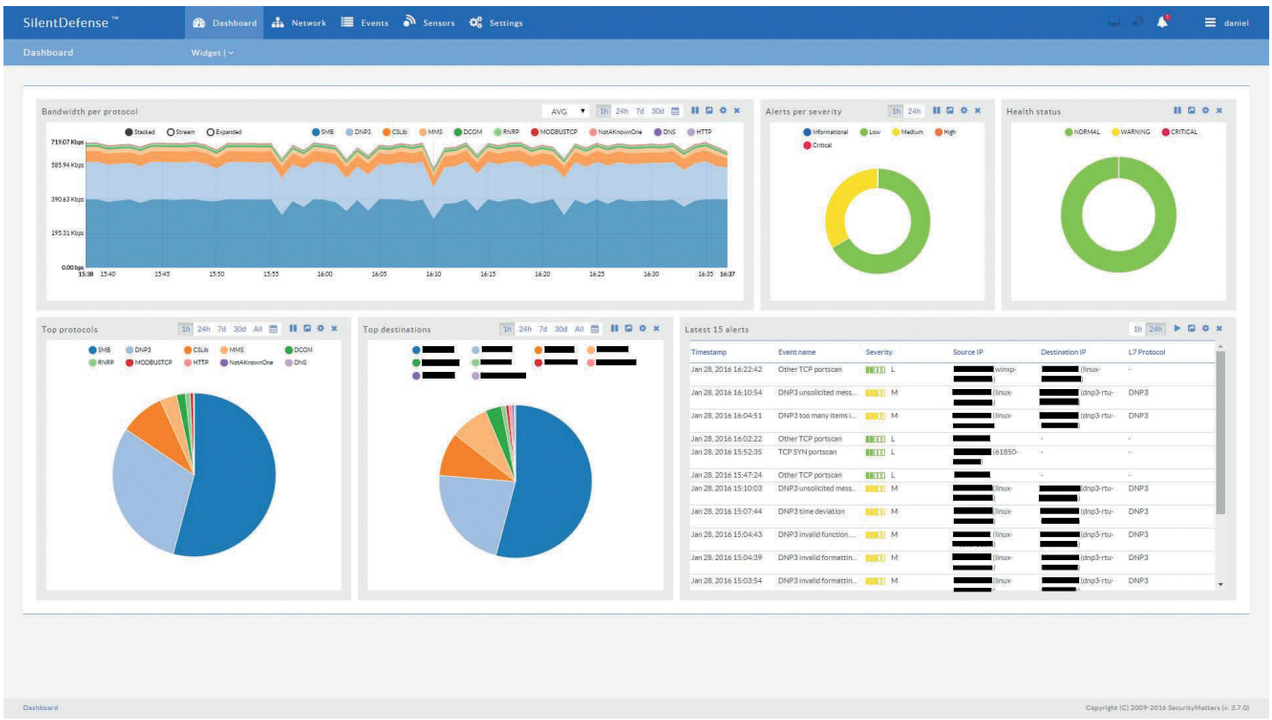
Незважаючи на те, що поки ще завчасно визначати точну динаміку інциденту, всі, хто приймають участь в аналізі погоджуються, що відключення є результатом надзвичайно добре скоординованої триступеневої атаки:

- шкідлива програма можливо мала доступ до мережі, щоб пошкодити систему SCADA;
- DDoS-атака контактного центру підприємства, щоб запобігти повідомленням клієнтів про проблеми;
- відкриття вимикачів підстанцій, швидше за все прямою командою, яка була надіслана нападниками, викликало відключення електропостачання.

З огляду на обставини, постачальники електроенергії були надзвичайно швидкими і ефективними у відновленні подачі електроенергії для своїх клієнтів. Оскільки дистанційне керування технологічним процесом через систему SCADA виявилося практично неможливим, експлуатаційний персонал на всіх вражених підстанціях включив всі відімкнені вимикачі вручну, та повернув систему до функціонуючого стану.

Чи можливо уникнути кібератаки?

Правильна відповідь – мабуть ні, але деякі симптоми атаки і дій атакуючих могли бути виявлені раніше в проце-



Мал. 2. Панель SilentDefense відображає набір попередньо сконфігурованих віджетів.

сі. Наприклад, антивірусні програми і системи запобігання вторгнень можуть виявити шкідливі програми, виявлені на українських підприємствах.

Два кроки атаки, які могли бути виявлені в той час, коли вона відбулась, це:

- обмін даними між інфікованими комп'ютерами та C&C (командно-контрольним) сервером шкідливої програми для повідомлення інформації через можливість перехоплення трафіку;
- дії, що виконуються атакуючими для дистанційного відкриття вимикачів, викликаючи реальне відключення.

Це виявлення було б можливим за умови контролю SCADA-мережі підприємства за допомогою платформи моніторингу SilentDefense компанії SecurityMatters.

SilentDefense

Вочевидь, що для протидії аналогічним атакам необхідні системи мережевого моніторингу, які враховують специфіку систем SCADA та інфраструктуру систем диспетчерського управління. І такі системи є на ринку. Передова інтелектуальна платформа мережевого моніторингу SilentDefense (тиха, мовчазна або безшумна оборона) використовується операторами критичної інфраструктури по всьому світу. Ця система вже довела свою ефективність проти спроб вторгнення і специфічних проблем ICS/SCADA на різних об'єктах критичної інфраструктури.

SilentDefense постійно стежить і аналізує мережеві комунікації, порівнює їх з базовою законною/бажаною (очікуваною) діяльністю. За допомогою інтелектуальної бібліотеки промислових загроз SecurityMatters вона повідомляє в реальному часі про проблеми і загрози для мережі ICS/SCADA, такі як:

- намагання і поточні вторгнення;
- помилкову поведінку і помилкові налаштування пристроїв;
- небажані операції в управлінні технологічним процесом;
- експлуатаційні помилки;
- атаки нульового дня і відомі атаки.

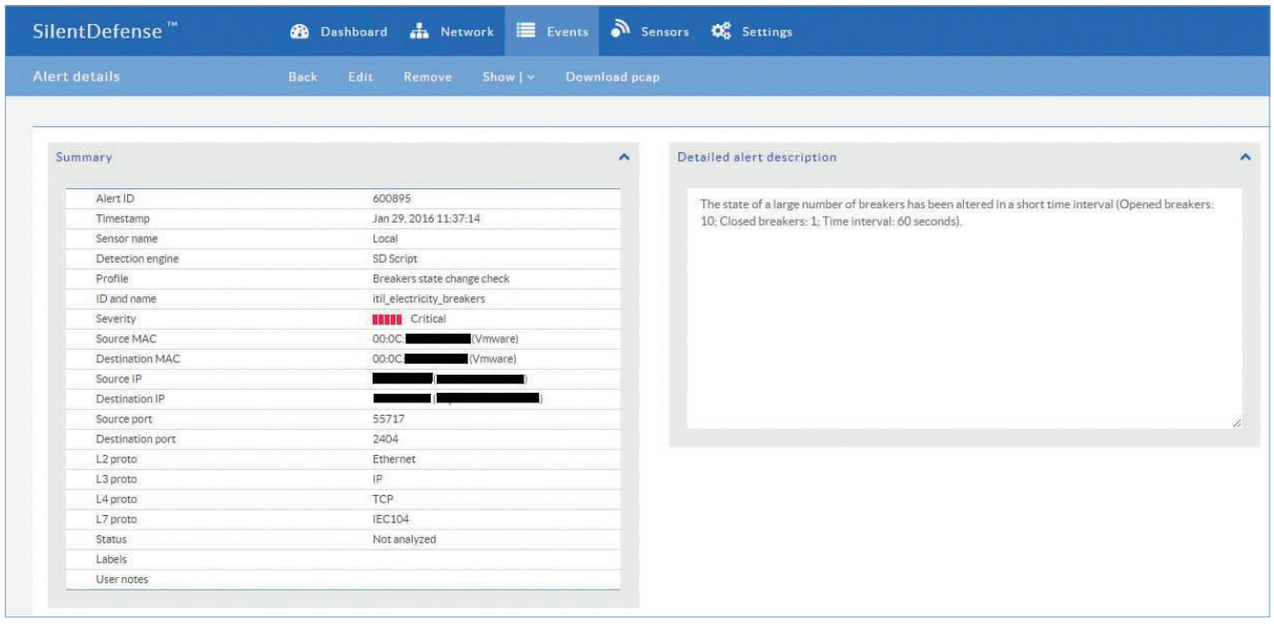
Ці загрози виявляються і представляються оператору в двох основних форматах:

- візуальна аналітика: «графічне представлення» мережі надає оператору можливість бачити/виявляти/аналізувати дивну поведінку мережі;
- сповіщення реального часу: про погану або неочікувану поведінку мережі, SilentDefense повідомляє оператора і надає йому всю необхідну інформацію для реагування на подію.

Система SilentDefense використовує алгоритми самонавчання, за рахунок цього вірогідність помилкового спрацювання є на порядки меншою, ніж в інших системах. Важлива перевага SilentDefense - те, що вона є прозорою для систем SCADA та інших інформаційних систем підприємства.

Розуміння промислових комунікаційних протоколів та інноваційний алгоритм SilentDefense забезпечує виявлення несанкціонованих команд в мережі ICS/SCADA. Система аналізує потоки даних на рівні комунікаційних протоколів управляючих контролерів, в тому числі протоколів IEC 104, DNP3, IEC 61850 (MMS & GOOSE), ICCP, Synchrophasor, Modbus/TCP, EtherNet/IP, MMS, OPC-DA, власних протоколів ABB та Siemens. Використовуючи алгоритми глибокого поведінкового контролю протоко-

Мал. 3. Приклад повідомлення SilentDefense про підозрілу зміну значень в технологічному процесі по протоколу Modbus/TCP.



Мал. 4. SilentDefense відображає згенероване сповіщення про те, що стан кількох вимикачів змінився за короткий час.

лу (DPBI), при неавторизованих діях та підозрілих спробах зміни значень SilentDefense автоматично генерує звіт (мал. 3).

Виявлення атаки

SilentDefense забезпечує виявлення проблем і вищезазначених загроз, використовуючи різні взаємодоповнюючі двигунці:

- вбудовані модулі для виявлення сканування портів, виявлення присутності, та перевірки відповідності протоколів;
- схеми комунікацій для виявлення невідомих мережевих пристроїв, небезпечних протоколів та небажаних операцій;
- схеми протоколів для виявлення несподіваних відхилень технологічних процесів;
- інтелектуальну бібліотеку промислових загроз для специфічних мережевих перевірок, наприклад, виявлення відкриття клапанів в небажані проміжки часу, верифікація, якщо певні вимикачі підстанції відкриваються, інші закриваються, і т.п.

Припускаючи, що, швидше за все, команда на відкриття вимикачів на підстанціях у наведеному вище прикладі атаки була видана нападниками з віддаленого робочого місця, ця команда зловмисників була б виявлена SilentDefense, якби ця система захисту була встановлена в українських Обленерго. І відразу ж після виявлення такої команди, оператори були б повідомлені і забезпечені зібраною інформацією, що дозволило б їм зрозуміти ситуацію та ініціювати заходи щодо виправлення становища.

Джерела:

[1] *http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245086886&cat_id=35109*