fot. © panandrii / Adobe Stock

Ochrona łańcuchów dostaw przed cyberatakami

Mike Mullane

Odporność cybernetyczna może zostać osiągnięta jedynie dzięki skupieniu się na technologii informacyjnej i operacyjnej

W ostatnich miesiącach w wielu badaniach i raportach podkreślano alarmujący wzrost liczby cyberataków na łańcuchy dostaw. Jedno z takich badań, przeprowadzonych w obu Amerykach, Azji i Europie, sugeruje, że w ostatnim roku dwie trzecie firm doświadczyło cyberataku na ich łańcuch dostaw.

Łańcuch dostaw to droga, jaką produkty i usługi muszą przejść od dostawcy do klienta. To system, który obejmuje organizacje, ludzi, działania, informacje i zasoby. Łańcuchy dostaw są szczególnie wrażliwe ze względu na ich złożone interakcje m.in. z działaniami zakładu, pracownikami, klientami i spedytorami. Trudno poznać te mechanizmy, nie mówiąc już o ich kontroli oraz procedurach bezpieczeństwa wykorzystywanych wzdłuż całego łańcucha.

Inną kwestią wskazaną przez raport Departamentu Obrony Stanów Zjednoczonych jest to, że bezpieczeństwo w przemyśle wytwórczym koncentruje się na usługach w chmurze, zarządzaniu danymi i innych rodzajach technologii informacyjnych (IT), jednocześnie nie uwzględniając bezpieczeństwa łańcucha dostaw, z których wiele działa na podstawie technologii operacyjnej (OT). Głównym problemem Pentagonu jest oczywiście amerykański przemysł obronny, ale kwestie uwzględnione w raporcie dotyczą wszystkich sektorów przemysłowych i infrastruktury krytycznej na całym świecie.

Cyberbezpieczeństwo IT i OT

Programy cyberbezpieczeństwa zbyt często bazują na rozwiązaniach IT. W rzeczywistości ograniczenia operacyjne w sektorach przemysłu takich jak produkcja, energetyka, ochrona zdrowia i transport oznaczają, że podejście zaadaptowane w kwestii cyberbezpieczeństwa wymaga zabezpieczenia OT.

IT koncentruje się głównie na danych i ich zdolności do swobodnego i bezpiecznego przepływu. Istnieje w świecie wirtualnym, w którym dane są przechowywane, pobierane, przesyłane i edytowane. IT jest płynny i ma wiele ruchomych części i bram, co czyni go podatnym na ataki. Obrona przed nimi polega na zabezpieczeniu każdej warstwy oraz ciągłym identyfikowaniu i korygowaniu słabości, aby zapewnić ciągłość przepływu danych.

OT przeciwnie, należy do świata fizycznego. Podczas gdy dział IT musi chronić każdą warstwę systemu, OT obejmuje utrzymanie kontroli nad systemami: włączania i wyłączania, zamykania lub otwierania. OT zapewnia poprawne wykonanie wszystkich działań. Wszystko w OT jest nastawione na fizyczny ruch i kontrolę urządzeń i procesów, aby system działał zgodnie z przeznaczeniem, ze szczególnym naciskiem na bezpieczeństwo i zwiększoną wydajność. Na przykład OT pomaga zagwarantować, że generator włącza się w tryb online, w sytuacji wzrostu zapotrzebowania na energię elektryczną lub że zawór przelewowy otwiera się, gdy zbiornik chemikaliów jest pełny, aby uniknąć wycieków niebezpiecznych substancji.

W przeszłości IT i OT miały odrębne role. Zespoły OT pracowały z zamkniętymi systemami zależnymi od fizycznych mechanizmów bezpieczeństwa zapewniającymi ciągłość działania. Wraz z pojawieniem się Przemysłowego Internetu Rzeczy (Industrial Internet of Things - IIoT) oraz integracją fizycznych maszyn z czujnikami i oprogramowaniem w sieci, granice między tymi dwoma technologiami zacierają się. Ponieważ coraz więcej obiektów łączy się, komunikuje ze sobą i wchodzi w interakcje, nastąpił wzrost liczby punktów końcowych i potencjalnych sposobów dostępu cyberprzestępców do sieci i systemów infrastruktury.

Ochrona łańcuchów dostaw

To prowadzi nas z powrotem do łańcuchów dostaw, skąd prawdopodobnie bierze się ogromna większość cyberprzestępstw. I znowu, istnieją istotne różnice pomiędzy IT i OT.

Łańcuch dostaw IT definiuje się jako „zbiór organizacji z powiązanymi zbiorami zasobów i procesami, z których każdy działa jako nabywca, dostawca lub obie te osoby, aby tworzyć kolejne relacje z dostawcami ustanowione w momencie złożenia zamówienia, podpisania umowy lub innej formalnej umowy zaopatrzeniowej".

Definicja łańcucha dostaw dla inteligentnych zakładów produkcyjnych obejmowałaby nie tylko IT, lecz także łańcuch dostaw OT. Dotyczy to osób (programistów, dostawców, sprzedawców i pracowników pracujących w OT) oraz procesów i produktów: elementów i systemów centralnych dla OT, takich jak automatyka przemysłowa i systemy kontroli (IACS), a także coraz częściej elementy Internetu Rzeczy (IoT).

W ochronie łańcucha dostaw kluczowe znaczenie ma zainstalowanie bezpiecznej technologii. Stara technologia jest poważnym problemem, zwłaszcza gdy zagrożone urządzenia stają się bramą do systemów kontroli przemysłowej lub kontroli nadzorczej i systemów gromadzenia danych (SCADA). Naukowcy niedawno korzystali z linii faksu, aby uzyskać dostęp do urządzeń sieciowych podłączonych do drukarki wielofunkcyjnej.

Znaczenie zarządzania ryzykiem

Bezpieczna technologia stanowi tylko część wyzwania; sama w sobie nie zapewni odporności. Najbezpieczniejsze podejście polega na zrozumieniu i zmniejszeniu ryzyka w celu zastosowania właściwej ochrony w odpowiednich punktach systemu. Dotyczy to zarówno IT, jak i OT.

Istotne jest, że ten proces jest ściśle powiązany z celami organizacyjnymi, ponieważ decyzje dotyczące ograniczeń mogą mieć poważny wpływ na działalność. Idealnie byłoby, gdyby proces bazował na podejściu systemowym angażującym interesariuszy z całej organizacji.

fot. © Alex / Adobe Stock

Gdy organizacja zrozumie system i określi, co jest wartościowe i potrzebuje największej ochrony, należy podjąć trzy kroki, aby poradzić sobie z ryzykiem i konsekwencjami ataku cybernetycznego:

- zrozumieć znane zagrożenia poprzez modelowanie zagrożeń i ocenę ryzyka;
- zająć się zagrożeniami i wdrożeniem ochrony za pomocą Norm Międzynarodowych odzwierciedlających najlepsze światowe praktyki;
- zastosować odpowiedni poziom oceny zgodności – testowanie i certyfikacja – wobec wymogów.

Podejście oparte na analizie ryzyka zwiększa zaufanie wszystkich zainteresowanych stron, demonstrując nie tylko stosowanie środków bezpieczeństwa uwzględniających najlepsze praktyki, lecz także skuteczne wdrożenie odpowiednich środków przez organizację.

Normy i ocena zgodności w ochronie łańcuchów dostaw

IEC opracowało wiele norm w celu ochrony infrastruktury przemysłowej i krytycznej, mające zastosowanie do wielu różnych sytuacji oraz wyspecjalizowanych norm, na przykład dla elektrowni jądrowych lub ochrony zdrowia. Jednocześnie IEC pracuje także nad oceną zgodności (CA) oraz globalnymi schematami certyfikacji poprzez grupy robocze (WG) powołane przez Radę ds. Oceny Zgodności (CAB) oraz Komitet ds. Zarządzania Certyfikacją (Certification Management Committee - CMC) w IECEE.

Oprócz grupy norm ISO/IEC 27000 obejmującej zarządzanie usługami IT oraz serii norm IEC 62443 horyzontalnych publikacji obejmujących przemysłowe sieci komunikacyjne oraz IACS, wiele komitetów (TC) i podkomitetów technicznych (SC) IEC opracowało normy, specyfikacje techniczne (TS) oraz wymagania dla poszczególnych sektorów.

IEC CAB powołało WG 17, aby prześledzić potrzeby rynku i ramy czasowe usług CA (globalnych schematów certyfikacji) dla produktów, usług, personelu i zintegrowanych systemów w obszarze cyberbezpieczeństwa. Nie obejmuje to automatyki przemysłowej, którą zajmuje się IECEE CMC WG 31. CAB WG 17 informuje również inne sektory przemysłu o ogólnym podejściu w zakresie cyberbezpieczeństwa przyjętym przez IECEE CMC WG 31 oraz jak może ono dotyczyć tych sektorów.

Głównym zadaniem IECEE CMC WG 31 jest „stworzenie wyjątkowego podejścia CA do serii norm IEC 62443". W tym celu powstał OD-2061 opublikowany w czerwcu 2018 roku przewodnik *Operational Document* (Dokument Operacyjny), opisujący jak ocena zgodności może być wykorzystywana i stosowana wobec niektórych norm z serii IEC 62443.

OD-2061 wyjaśnia również, pod jakimi warunkami można uzyskać IECEE *Cyber Certificates of Conformity – Industrial Cyber Security Capability*. Certyfikaty są ważne tylko gdy „podpisze je uznane Laboratorium Certyfikujące oraz dołączone do certyfikatu wydanego przez krajową jednostkę certyfikującą (NBC – National Certification Body)".

Obecnie te certyfikaty są określone dla następujących ocen, z których każda ma zastosowanie do jednej lub więcej norm z serii IEC 62443:

- wydajności produktu (*Product capability*);
- wydajności procesu (*Process capability*);
- możliwości zastosowania produktu (*Product application of capabilities*);
- możliwości zastosowania procesów (*Process application of capabilities*);
- możliwości zastosowania rozwiązań (*Solution application of capabilities*).

Wraz z normami IEC obejmującymi bezpieczeństwo cybernetyczne niedawne wprowadzenie kompleksowych systemów certyfikacji CA powinno zapewnić lepszą ochronę systemów bazujących na przemysłowych sieciach komunikacyjnych oraz IACS (w tym łańcuchów dostaw) przed cyberzagrożeniami.

Źródło: IEC e-tech magazine, Issue 6/2018
Tłum. I. P.