Joanna Chmielak, Fortinet

Bezpieczeństwo systemów przemysłowych

w sektorze energetycznym

Systemy technologii operacyjnych (*Operational Technologies*, OT) służą do kontrolowania infrastruktury przemysłowej i krytycznej w sektorze energetycznym, przy produkcji przemysłowej, w komunikacji i transporcie, obronności, a także w placówkach świadczących usługi użyteczności publicznej. Z uwagi na obszary, w których systemy te są wykorzystywane, mają one kluczowe znaczenie dla bezpieczeństwa publicznego i gospodarczego. We wszystkich tych sektorach szeroko wdrażane są również rozwiązania cyfrowe. W efekcie sieci OT są coraz częściej podłączane do sieci informatycznych (IT), a te z kolei mają łączność z Internetem. W ten sposób OT stają się podatne na zagrożenia, które wcześniej ich nie dotyczyły.

fot: Pixabay.com

Konsekwencje łączenia IT/OT

Łączenie sieci IT i OT powoduje, że maszyny i całe procesy produkcyjne są narażone na cyberzagrożenia. Mogą one skutkować utratą danych, przestojami w produkcji, uszkodzeniem sprzętu lub innych zasobów, a nawet zagrożeniem bezpieczeństwa i życia ludzi. Wiele systemów OT nigdy nie było zaprojektowanych z myślą o zdalnym dostępie, więc ryzyko z nim związane nie było brane pod uwagę. Zamiast kompletnie przeprojektować te środowiska, zaczęto stosować takie rozwiązania jak segmentacja i zaawansowana analiza danych, co - częściowo skutecznie - miało zapewnić bezpieczeństwo urządzeń oraz procesów fizycznych. Dodatkowo w ostatnim czasie z sieciami OT integrowane są takie technologie informatyczne, jak uczenie maszynowe (ML) i Big Data, co zwiększa cyfrową powierzchnię ataku i ryzyko włamań.

Do niedawna najlepszym sposobem ochrony sieci OT było ich całkowite odizolowanie od sieci IT (ang. *air gapping*). Jednak obecnie, według badania przeprowadzonego przez Fortinet w 2018 r.[1], prawie trzy czwarte przedsiębiorstw zgłasza, że posiada przynajmniej podstawowe połączenia między swoimi środowiskami IT i OT.

Oznacza to, że ochrona będąca efektem wspomnianej izolacji, praktycznie znika i sieci OT są narażone na te same zagrożenia co sieci IT. W obliczu konieczności ich obrony przed rosnącą falą zaawansowanych ataków, centra zarządzania siecią znalazły się pod ogromną presją, aby w tym samym czasie zapewnić zarówno bezpieczeństwo, jak i jej operacyjną dostępność. W związku z tym muszą na nowo przeanalizować istniejący system zabezpieczeń.

Problemy te są widoczne dla osób zajmujących się cyberbezpieczeństwem w firmach produkcyjnych. Prawie wszystkie (97%) dostrzegają wyzwania związane z zapewnieniem ochrony w połączonych środowiskach IT oraz OT[2].

OT na celowniku cyberprzestępców

Według opublikowanego przez Fortinet w 2019 r. „Raportu o stanie technologii operacyjnej i cyberbezpieczeństwa", trzy czwarte badanych operatorów systemów OT odnotowało w ciągu ostatnich 12 miesięcy włamanie do nich. Co więcej, połowa firm doświadczyła w tym czasie od 3 do 10 włamań. Naruszenie bezpieczeństwa skutkowało zwykle utratą danych, zakłóceniami lub przerwą w działalności operacyjnej oraz narażeniem reputacji marki.

> Łączenie sieci IT i OT powoduje, że maszyny i całe procesy produkcyjne są narażone na cyberzagrożenia. Mogą one skutkować utratą danych, przestojami w produkcji, uszkodzeniem sprzętu lub innych zasobów, a nawet zagrożeniem bezpieczeństwa i życia ludzi

Wrażliwa energetyka

Sektor energetyczny należy do szczególnie zagrożonych atakami na systemy operacyjne, a w dodatku skutki naruszenia bezpieczeństwa przedsiębiorstw w nim działających mogą być bardzo dotkliwe dla bezpieczeństwa publicznego. O tym, że cyberprzestępcy szczególnie interesują się tym obszarem świadczą już dokonane z powodzeniem ataki.

W 2003 r. wirus Slammer/SQL Slammer sparaliżował pracę elektrowni jądrowej Davis-Besse w amerykańskim stanie Ohio. Inne głośne przypadki to naruszenie bezpieczeństwa operatora elektrowni jądrowej w Korei Południowej z 2014 r., czy dwa ataki na ukraiński sektor energetyczny - w 2015 i 2016 r. Warto podkreślić, że najczęściej pierwotnym celem ataku były firmy współpracujące z elektrowniami.

Warto również dodać, że w ostatnim czasie cyberprzestępcy przeprowadzali ataki typu ransomware (polegające na zaszyfrowaniu plików i żądaniu wpłaty okupu w zamian za ich odzyskanie, bądź odblokowanie systemów), w których próbowali podszywać się pod rosyjskie spółki naftowo-gazowe, w szczególności „PAO NGK Slavneft". Ich prawdopodobnym celem było uderzenie w część tego segmentu przemysłu.

W tym kontekście ważna jest wypowiedź Karola Okońskiego, Wiceministra Cyfryzacji odpowiedzialnego za cyberbezpieczeństwo. W maju tego roku zapowiadał on, że polski rząd zamierza przeprowadzić symulację cyberataku na wybrany sektor, aby sprawdzić działanie w praktyce krajowego systemu cyberbezpieczeństwa. Wiceminister cytowany przez PAP stwierdził: *pewnie wybierzemy sektor, który jest na tyle obszerny i w ramach którego nastąpiło najwięcej zmian, czy najwięcej wyzwań się pojawia. Wydaje się, że jest nim sektor energetyczny.*

Widoczność kluczem do bezpieczeństwa

Zgodnie z prawdą, że nie da się ochronić tego, czego się nie widzi, kluczowym elementem zapewnienia bezpieczeństwa połączonych środowisk

> Właściwe podejście do tematu zabezpieczenia sieci OT powinno uwzględnić wdrożenie zintegrowanej, poddanej segmentacji wielowarstwowej architektury ochronnej

IT/OT jest maksymalizacja dostępu do informacji o nich. Jednak firmy mają z tym problem. Aż 82% z nich przyznało, że nie jest w stanie zidentyfikować wszystkich urządzeń podłączonych do swojej sieci.

Zagwarantowanie odpowiedniego działania systemu OT wymaga zapewnienia ciągłej widoczności każdego podłączonego do niego urządzenia przewodowego i bezprzewodowego. Należy przy tym uwzględnić fakt, że są one na bieżąco podłączane i odłączane od sieci lub zmieniają swoją lokalizację.

Obecnie powszechne jest stosowanie w środowiskach OT najróżniejszych urządzeń bezprzewodowych i związanych z Internetem rzeczy (*Internet of Things*, IoT). Są to na przykład inteligentne czujniki parametrów środowiskowych. Ze względu na fakt, że łączą się z zewnętrzną siecią informatyczną w celu zapewnienia dodatkowych funkcji, mogą stanowić potencjalne „tylne wejście" podczas ataków ukierunkowanych na niezabezpieczone systemy OT.

Zintegrowane środowisko ochronne może zapewnić przejrzystą, scentralizowaną widoczność całej infrastruktury OT. W tym celu powinna ona udostępniać wbudowane interfejsy API oraz otwarte interfejsy API REST, aby przedsiębiorstwo mogło wykorzystać je do połączenia ze swoimi rozwiązaniami ochronnymi. Procesowi zapewnienia widoczności może towarzyszyć wdrożenie takich rozwiązań, jak mechanizmy kontroli dostępu do sieci (NAC), które ułatwią pasywną inwentaryzację punktów końcowych i urządzeń związanych z Internetem rzeczy oraz zarządzanie nimi bez zakłócania działania wrażliwych systemów OT.

Należy jednak przyznać, że w organizacjach korzystających z systemów OT rośnie nacisk na cyberbezpieczeństwo. 70% z nich planuje powierzenie w przyszłym roku nadzoru nad tymi kwestiami menedżerom ds. zabezpieczeń infrastruktury informatycznej (CISO), 62% organizacji zwiększyło nakłady na tę dziedzinę, a 38% deklaruje, że utrzyma je na dotychczasowym poziomie[3].

Ankietowani zwracali również uwagę na problem luki kompetencyjnej, który dotyka całą branżę cyberbezpieczeństwa. Na rynku brakuje również odpowiedniej liczby specjalistów zajmujących się zabezpieczeniami systemów przemysłowych. Skutkuje to problemami we wdrożeniu bardziej złożonych cyberzabezpieczeń, standardów bezpieczeństwa, czy elastyczności operacyjnej.

Jak chronić systemy OT?

Właściwe podejście do tematu zabezpieczenia sieci OT powinno uwzględnić wdrożenie zintegrowanej, poddanej segmentacji wielowarstwowej architektury ochronnej. Zapewni to odpowiednią widoczność wszystkich urządzeń, możliwość analizy kontekstu w czasie rzeczywistym oraz oparte na regułach mechanizmy zapewniające integralność urządzeń lub systemów, przy jednoczesnym zabezpieczeniu innych, krytycznych elementów środowiska OT. Ważna jest również segmentacja sieci według kryteriów biznesowych, która określa typ użytkownika, urządzenia i potrzeby biznesowe, aby kontrolować ich dostęp do określonych zasobów sieci.

Rozwiązaniem spełniającym powyższe wymagania jest Fortinet ICS Layered Defense Model. Platforma ATP umożliwia wykrywanie i neutralizowanie zaawansowanego szkodliwego oprogramowania. Podejście *Defense-in-Depth* zapewnia ściśle zintegrowaną, wielowarstwową ochronę. Z kolei funkcja wewnętrznej segmentacji umożliwia wykrywanie i blokowanie w sieci wewnętrznej szkodliwego kodu, który zdołał pokonać zewnętrzne zabezpieczenia. Pozwala to ograniczyć zakres ataku i potencjalne szkody. Biorąc pod uwagę lawinowy wzrost liczby urządzeń IoT w przemysłowych systemach sterujących oraz konieczność ochrony infrastruktury krytycznej, jest to obszar, w którym należy wprowadzić najbardziej zaawansowane rozwiązania ochronne.

Warto również przyjrzeć się rozwiązaniom stosowanym przez firmy, które w przywołanym wcześniej raporcie Fortinet wypadły jako najlepiej zabezpieczone i nie zgłosiły żadnych przypadków włamań przez minione 12 miesięcy. Stosowały one uwierzytelnianie wieloskładnikowe w celu uzyskania dostępu do danych i systemów (każda z nich), mechanizm kontroli oparty na rolach, monitorowały i analizowały zdarzenia dotyczące bezpieczeństwa oraz wdrożyły segmentację sieci. □

1) „Raport z niezależnego badania cyberbezpieczeństwa systemów SCADA/ICS", Fortinet 2019 r.
2) Tamże.
3) „Raport o stanie technologii operacyjnej i cyberbezpieczeństwa", Fortinet, 2019 r.