FORTINET | IT Solution FACTOR

Strategie zabezpieczania infrastruktury OT przed zaawansowanymi zagrożeniami

Spis treści

Streszczenie 3

Cel — infrastruktura OT 5

Segmentacja — minimalizowanie powierzchni ataku 6

Bezpieczna, scentralizowana kontrola dostępu — użytkownicy, urządzenia i aplikacje 8

Zaawansowane zagrożenia — ochrona i wykrywanie 9

Zaawansowane zagrożenia — ochrona, wykrywanie i reagowanie oparte na sztucznej inteligencji 10

Podsumowanie 12

FORTINET

Streszczenie

Technologia operacyjna (OT), czyli systemy kontrolujące sprzęt, maszyny i procesy mechaniczne w zakładach przemysłowych, elektrowniach, sieciach energetycznych i innej krytycznej infrastrukturze, coraz częściej jest celem cyberprzestępców. Po połączeniu ze sobą sieci OT i IT znika bariera, która niegdyś chroniła systemy OT przed zakusami hakerów. Ponadto atak na sieć OT może nieść poważne skutki, począwszy od zakłóceń lub przestojów w świadczeniu usług, a skończywszy na katastrofalnych zagrożeniach dla życia ludzkiego.

Cyberprzestępcy są coraz bardziej zaawansowani i biegli w wykorzystywaniu luk w zabezpieczeniach sieci OT. Tradycyjne zabezpieczenia sieci IT po prostu nie są zdolne do ochrony sieci OT przed zaawansowanymi zagrożeniami. Dyrektorzy ds. bezpieczeństwa infrastruktury informatycznej potrzebują zatem kompleksowej strategii ochrony przez znanymi i nieznanymi zagrożeniami, która przede wszystkim skupi się na neutralizowaniu skutków ataków nieudaremnionych przez stosowane mechanizmy zabezpieczeń. Strategia taka powinna obejmować rozwiązania, które zapewnią widoczność sieci OT oraz automatycznie i precyzyjnie ograniczą do niej dostęp, wykryją i powstrzymają ataki w czasie rzeczywistym, udaremnią atakującym działania w sieci wewnętrznej (ang. lateral movement) i zminimalizują powierzchnię ataku na sieć OT.

W ciągu ostatnich dwóch lat 90% przedsiębiorstw korzystających z systemów OT miało do czynienia z co najmniej jednym atakiem, który spowodował znaczne zakłócenia i przestoje[1].

Dyrektorzy ds. bezpieczeństwa infrastruktury informatycznej muszą zakładać, że zabezpieczenia sieci OT zostaną pokonane. Kluczowe znaczenie ma zatem wdrożenie środków, które uniemożliwią atakującym działania w sieci wewnętrznej, narażanie systemów na szwank i wywoływanie szkód.

Cel — infrastruktura OT

Od pewnego czasu cyberprzestępcy zaczynają kierować swoje ataki na systemy nadzorowania procesów technologicznych (SCADA) oraz przemysłowe systemy sterowania (ICS). Cele tych działań są różne i mogą na przykład obejmować przejęcie kontroli nad infrastrukturą krytyczną i żądanie okupu. Konkurenci przemysłowi, często za namową własnych rządów, mogą infiltrować systemy drugiej strony w celach szpiegostwa przemysłowego. W skrajnych przypadkach hakerzy chcą dokonać umyślnego sabotażu polegającego na przykład na odcięciu dostaw prądu dla dużej liczby ludności, aby osiągnąć określone cele polityczne lub wojskowe.

Determinacja cyberprzestępców przejawia się w zaawansowaniu stosowanych przez nich metod. Gdy tylko sforsują zabezpieczenia sieci, urządzeń lub aplikacji, stosują narzędzia informujące ich o wykryciu złośliwego oprogramowania oraz mechanizmy ukrywania lub uniemożliwiania analizy przeprowadzonego ataku, aby jak najbardziej utrudnić zbadanie ataku pod kątem jego metodologii, pochodzenia i celów[2].

Systemy OT są szczególnie podatne na zaawansowane zagrożenia, zwłaszcza ze względu na fakt, że często są to systemy stare (mają około 20-30 lat), rzadko aktualizowane (w porównaniu z systemami IT) oraz zróżnicowane pod kątem dostawców i stosowanych protokołów[3]. Ponadto wraz z rozwojem inicjatyw w zakresie transformacji cyfrowej (DX) i Internetu rzeczy (IoT) około 66% urządzeń OT zostało podłączonych albo do Internetu, albo do sieci przedsiębiorstwa[4]. O ile stosowanie zabezpieczeń przed zagrożeniami zewnętrznymi jest oczywiste, dyrektorzy ds. bezpieczeństwa infrastruktury informatycznej muszą zakładać, że zabezpieczenia sieci OT zostaną pokonane, i powinni się zapoznać z rozwiązaniami, technikami i praktykami, które pomogą chronić takie systemy przed zaawansowanymi zagrożeniami.

W poniższych sekcjach przedstawiono najważniejsze środki, które dyrektorzy ds. bezpieczeństwa infrastruktury informatycznej powinni traktować priorytetowo podczas opracowywania strategii zabezpieczenia infrastruktury OT przed zaawansowanymi zagrożeniami.

Wraz z rozwojem inicjatyw w zakresie transformacji cyfrowej (DX) i Internetu rzeczy (IoT) około 66% urządzeń OT zostało podłączonych albo do Internetu, albo do sieci przedsiębiorstwa[4].

Segmentacja — minimalizowanie powierzchni ataku

Gdy cyberprzestępca narusza zabezpieczenia działające na granicy sieci, konieczne jest wprowadzenie środków, które udaremnią mu działania w sieci wewnętrznej, narażanie systemów na szwank i wywoływanie szkód. Narażone na atak zasoby w środowisku OT wspólnie tworzą dużą powierzchnię ataku. Pierwszym zadaniem przedsiębiorstwa jest zatem jej zminimalizowanie.

Segmentacja oznacza oddzielenie lub odizolowanie od siebie krytycznych zasobów oraz zdefiniowanie zasad bezpieczeństwa, czyli zbudowanie w ramach całej sieci i infrastruktury chmury „drzwi i murów", których przekroczenie będzie wymagać określonego poziomu zaufania. Wspomniana segmentacja może przybierać różne formy:

- **Makrosegmentacja** polega na podzieleniu środowiska sieciowego na szereg segmentów funkcjonalnych (stref) dostępnych tylko dla autoryzowanych urządzeń, aplikacji i użytkowników.
- **Mikrosegmentacja** to proces tworzenia podstref na bardziej podstawowym poziomie z bardzo szczegółowymi mechanizmami kontroli dotyczącymi pojedynczych lub logicznie pogrupowanych zasobów.
- **Segmentacja oparta na celach biznesowych** dotyczy grupowania zasobów zgodnie z logiką biznesową na potrzeby segmentacji. Dynamiczne funkcje zaufania wbudowane w tego typu segmentację pozwalają na automatyczną aktualizację praw dostępu i reguł biznesowych na podstawie prowadzonych na bieżąco ocen wiarygodności[5].

Dzięki oddzieleniu od siebie współzależnych zasobów, segmentacja taka skutecznie zmniejsza powierzchnię ataku w ramach infrastruktury OT (a także infrastruktury IT) i ogranicza ruch wschód-zachód (wewnątrz sieci). W efekcie zagrożenie, które przedostało się do sieci, nie uzyska dostępu do uruchomionych aplikacji, na przykład programowalnych sterowników logicznych (PLC).

Segmentacja ułatwia również wykrywanie naruszeń; każda próba nieautoryzowanego dostępu wskazuje bowiem na potencjalne włamanie, a zapory następnej generacji (NGFW) blokują takie próby i automatycznie ostrzegają wszystkie narażone na atak aplikacje o obecności zagrożenia. Działania takie są szczególnie ważne, ponieważ cyberprzestępcy skracają czas między momentem włamania a uaktywnieniem się złośliwego działania (na przykład zakłócenia lub zatrzymania działania systemu, żądania okupu lub kradzieży danych).

Sieci przedsiębiorstw korzystających z systemów OT są słabo posegmentowane, przy czym 45% użytkowników systemów ICS/SCADA nie korzysta z funkcji zarządzania tożsamościami uprzywilejowanymi6.

Determinacja cyberprzestępców przejawia się w zaawansowaniu stosowanych przez nich metod.

Bezpieczna, scentralizowana kontrola dostępu — użytkownicy, urządzenia i aplikacje

Bez względu na zastosowane zabezpieczenia najsłabszym punktem każdej infrastruktury zabezpieczeń jest najczęściej człowiek. Wiele szkodliwych naruszeń bezpieczeństwa było wynikiem przejęcia przez cyberprzestępców kont i haseł użytkowników lub niewłaściwych poziomów dostępu[7].

Urządzenia, użytkownicy i aplikacje trzeba uwierzytelniać przed udzieleniem im dostępu do środowiska OT lub wchodzących w jego skład posegmentowanych zasobów. Dyrektorzy ds. bezpieczeństwa infrastruktury informatycznej potrzebują rozwiązań, które mogą dokładnie zweryfikować, kto lub co próbuje uzyskać dostęp do chronionych zasobów. Są to zarówno mechanizmy kontroli dostępu oparte na rolach, które ograniczają dostęp na podstawie przydzielonych użytkownikom obowiązków, jak również mechanizmy zarządzania uprawnieniami w czasie rzeczywistym. Segmentacja oparta na celach biznesowych może również pomóc w ograniczeniu dostępu do określonych segmentów sieci do konkretnych osób na podstawie logiki biznesowej. Dzięki mechanizmom kontroli dostępu opartym na rolach (NAC) zespoły zajmujące się siecią OT mogą wdrażać odpowiednie zasady dostępu do urządzeń i użytkowników.

Ponadto sieci OT coraz częściej wykorzystują łączność bezprzewodową na potrzeby zdalnego monitorowania i zarządzania (polega to na łączeniu chmurowych kontrolerów z czujnikami i wbudowanymi urządzeniami, które obsługują urządzenia i generują dane). Łączność taka z pewnością zwiększa sprawność operacyjną i automatyzację, dodaje też jednak nowy poziom podatności na zagrożenia. Do ochrony sieci OT przed zaawansowanymi zagrożeniami niezbędne są zatem odpowiednie mechanizmy zabezpieczające ruch bezprzewodowy, bezprzewodowe punkty dostępu i przełączniki, służące do blokowania ataków prowadzonych za pośrednictwem łączy bezprzewodowych.

Urządzenia, użytkownicy i aplikacje trzeba uwierzytelniać przed udzieleniem im dostępu do środowiska OT lub wchodzących w jego skład posegmentowanych zasobów.
Dyrektorzy ds. bezpieczeństwa infrastruktury informatycznej potrzebują rozwiązań, które mogą dokładnie zweryfikować, kto lub co próbuje uzyskać dostęp do chronionych zasobów.

Zaawansowane zagrożenia — ochrona i wykrywanie

W miarę jak podejmowane przez cyberprzestępców działania stają się coraz trudniejsze do wykrycia i coraz bardziej zamaskowane dyrektorzy ds. bezpieczeństwa infrastruktury informatycznej muszą wdrażać coraz bardziej zaawansowane rozwiązania, które sobie z takimi działaniami poradzą. Wiele rozwiązań może powstrzymać znane typy ataków, zespoły zajmujące się siecią OT potrzebują jednak mechanizmów wykrywania i udaremniania nieznanych zagrożeń i ataków typu „zero-day", zwłaszcza ataków wykorzystujących luki w zabezpieczeniach, które to luki właśnie odkryto, ale jeszcze ich nie usunięto.

Techniki „oszukiwania" zagrożeń mogą pomóc w neutralizacji i minimalizacji szkód wynikających ze wspomnianych zagrożeń i ataków[8]. „Oszustwo" polega tu na wdrożeniu w infrastrukturze pozornych maszyn wirtualnych lub aplikacji, które zwabią, zaangażują i powstrzymają atakujących. Jest to ważna metoda wykrywania nieznanych zagrożeń i ataków typu „zero-day". Narzędzia „oszustwa" służą jako system wczesnego ostrzegania, który dokładnie monitoruje i śledzi nieautoryzowany ruch wschód-zachód, często pozwalając na dokonanie ataku pod ścisłą obserwacją oraz przekazując informacje o zagrożeniach na potrzeby adekwatnej reakcji mechanizmów bezpieczeństwa.

Skuteczną bronią w walce z nieznanymi zagrożeniami i atakami typu „zero-day" jest również korzystanie z bezpiecznego środowiska testowego (ang. sandboxing). W tym przypadku chodzi o odizolowanie podejrzanej aktywności od głównego ruchu i obserwowania jej w symulowanym środowisku, aby najpierw sprawdzić, czy jest ona złośliwa, a jeśli tak, to automatycznie zacząć ją neutralizować. W celu skutecznej ochrony sieci OT bezpieczne środowisko testowe musi obsługiwać systemy operacyjne właściwe dla danego środowiska OT. Będzie wówczas bardzo cennym uzupełnieniem struktury zabezpieczeń służącym do znajdowania zaawansowanych zagrożeń, którym udało się uniknąć tradycyjnych mechanizmów wykrywania złośliwego oprogramowania.

„Dobra przynęta musi być wiarygodna. Nie może mieć ani zbyt dobrych zabezpieczeń, których nie da się naruszyć, ani też zbyt słabych zabezpieczeń, które będą sugerować pułapkę. Jeśli cyberprzestępca rozpozna pułapkę, uniknie jej, musi ona zatem działać i wyglądać jak pozostałe elementy sieciowe"[9].

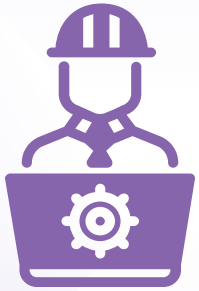
Zaawansowane zagrożenia — ochrona, wykrywanie i reagowanie oparte na sztucznej inteligencji

W zaawansowanych atakach coraz częściej używa się mechanizmów sztucznej inteligencji (AI) i uczenia maszynowego (ML). Za pomocą sztucznej inteligencji cyberprzestępcy mapują sieci, szukają luk w zabezpieczeniach i przygotowują niestandardowe ataki, w tym ataki na sieć OT[10]. Doskonale zdają sobie przy tym sprawę z niedostatecznych zasobów i kadr przewidzianych do ochrony takich sieci. W odpowiedzi na te zagrożenia przedsiębiorstwa muszą zatem korzystać z mechanizmów sztucznej inteligencji, uczenia maszynowego i automatyzacji. Mechanizmy te mogą poprawić skuteczność działania zespołów zajmujących się ochroną sieci, zwiększając ich zdolność do wykrywania zagrożeń, umożliwiając im określanie priorytetów badań oraz minimalizując liczbę fałszywych alarmów[11].

Kompleksowe strategie powinny również przewidywać wdrożenie zintegrowanych i zautomatyzowanych funkcji wymiany informacji o zagrożeniach. Dyrektorzy ds. bezpieczeństwa infrastruktury informatycznej potrzebują rozwiązań, które będą automatycznie przesyłać dane dotyczące wszelkich wykrytych zagrożeń między środowiskami IT i OT oraz w ramach każdego elementu zabezpieczeń — od centrum danych i główny kampus po brzeg sieci.

Przedsiębiorstwa muszą również scentralizować procesy reagowania na incydenty bezpieczeństwa i zarządzanie zdarzeniami. Strategia bezpieczeństwa nie będzie skuteczna, jeśli stosowane w jej ramach rozwiązania będą działać w sposób nieskoordynowany. Integracja całej infrastruktury bezpieczeństwa jest niezbędna, aby umożliwić automatyczną agregację danych pochodzących z systemów wykrywania zagrożeń i zapobiegania im. Agregacja ta jest z kolei niezbędna w celu podjęcia odpowiednich działań w obliczu pojawiających się zagrożeń dla środowiska OT.

Strategia wykrywania zaawansowanych zagrożeń i łagodzenia ich skutków powinna wreszcie uwzględniać zastosowanie mechanizmów analizy zachowań użytkowników i urządzeń (UEBA) stosowanych zazwyczaj do identyfikacji zagrożeń wewnętrznych. Osoby mające dostęp do informacji poufnych odpowiadają za istotny odsetek włamań, zazwyczaj wskutek zaniedbań, ale czasami też wskutek działań umyślnych. W badaniu Deloitte z 2019 r. na temat ryzyka cybernetycznego w sektorze energetycznym za „najbardziej pospolite zagrożenia" uznano błędy ludzkie i działania niezadowolonych pracowników[12]. Aby odpowiednio reagować na te problemy, mechanizmy UEBA muszą korzystać z technologii uczenia maszynowego i zaawansowanych narzędzi analitycznych w celu automatycznej identyfikacji niezgodnych z przepisami, podejrzanych lub odbiegających od normy zachowań oraz przesyłać ostrzeżenia dotyczące przejętych kont użytkowników.



Kompleksowe strategie powinny również przewidywać wdrożenie zintegrowanych i zautomatyzowanych funkcji wymiany informacji o zagrożeniach. Operatorzy sieci OT potrzebują rozwiązań, które będą automatycznie przesyłać dane dotyczące wszelkich wykrytych zagrożeń między środowiskami IT i OT oraz w ramach każdego elementu zabezpieczeń.

Podsumowanie

Rosnąca liczba i stopień zaawansowania ataków znacznie utrudnia pracę dyrektorów ds. bezpieczeństwa infrastruktury informatycznej i dotyczy zarówno środowiska IT, jak i OT. Ataki na środowisko OT mogą okazać się tragiczne w skutkach nie tylko dla przedsiębiorstw przemysłowych i operatorów kluczowej infrastruktury, ale również dla ogółu społeczeństwa. Dyrektorzy ds. bezpieczeństwa infrastruktury informatycznej muszą znać zaawansowane metody włamań, weryfikować stan bezpieczeństwa chronionych zasobów, identyfikować luki w zabezpieczeniach oraz znajdować rozwiązania służące do neutralizowania pojawiających się zagrożeń. W tym celu powinni zadać sobie następujące pytania:

- Czy nasza infrastruktura zabezpieczeń jest zintegrowana tak, aby informacje o zagrożeniach były współdzielone w czasie rzeczywistym przez wszystkie elementy tej infrastruktury?
- Czy nasz system informowania o zagrożeniach korzysta z mechanizmów sztucznej inteligencji i uczenia maszynowego do identyfikacji nieznanych zagrożeń i ataków typu „zero-day”?
- Czy mamy wdrożone zautomatyzowane procesy reagowania na incydenty i zarządzania zdarzeniami umożliwiające łagodzenie skutków udanych włamań, zanim się rozprzestrzenią i wyrządzą szkody?
- Czy mamy wdrożone mechanizmy wykrywania zaawansowanych zagrożeń i naruszeń takie jak bezpieczne środowiska testowe i przynęty?
- Czy stosujemy środki służące szybszemu wykrywaniu ataków i blokowaniu dostępu do zasobów sieciowych już po dokonaniu włamania?

[1] „Cybersecurity in Operational Technology: 7 Insights You Need to Know", Ponemon Institute, marzec 2019 r.

[2] „Threat Landscape Report Q2 2019", Fortinet, 7 sierpnia 2019 r.

[3] „Operational technology cybersecurity: A vision for the industrial sectors", EY, sierpień 2018 r.

[4] Barbara Filkins, „The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns", SANS Institute, 18 lipca 2018 r.

[5] „Reducing Complexity with Intent-base Segmentation: Best Practices for CIOs", Fortinet, 5 kwietnia 2019 r.

[6] „Independent Study Pinpoints Significant SCADA/ICS Security Risks", Fortinet, 28 czerwca 2019 r.

[7] Paul Yung, „Security Think Tank: Many breaches down to poor access controls", ComputerWeekly, 8 marca 2016 r.

[8] Gary S. Miliefsky, „Why Deception Technology Will Change the Game in Our Favor Against Cyber Crime and Breaches", Cyber Defense Magazine, 30 czerwca 2019 r.

[9] Kevin Townsend, „How Deception Technology Can Defend Networks and Disrupt Attackers", SecurityWeek, 5 czerwca 2019 r.

[10] Derek Manky, „The Evolving Threat Landscape—Swarmbots, Hivenets, Automation in Malware", CSO, 29 sierpnia 2018 r.

[11] „Using AI to Address Advanced Threats That Last-Generation Network Security Cannot", Fortinet, 8 czerwca 2019 r.

[12] Steve Livingston, et al., „Managing cyber risk in the electric power sector", Deloitte Insights, 31 stycznia 2019 r.

FORTINET

www.fortinet.com

448135-0-A-PL

5 lutego, 2021 1:00 PM

eb-Advanced-threat-landscape-for-OT-CISO_PL-foximo