Ochrona operacji produkcyjnych w kontekście zwiększającej się powierzchni ataku

Krytyczne elementy złożonej architektury zabezpieczeń

Spis treści

Streszczenie 3

Wprowadzenie — potrzeba modernizacji rozwiązań zabezpieczających w przedsiębiorstwach przemysłowych 4

- Wdrożenie skutecznych mechanizmów kontroli dostępu do sieci 6
- Minimalizowanie powierzchni ataku 8
- Eliminowanie silosów w celu zwiększenia skuteczności zabezpieczeń 10
- Zwiększenie widoczności i automatyzacja 12
- Zapewnienie zgodności rozwiązań zabezpieczających z siecią OT 13

Podsumowanie — właściwa architektura zabezpieczy sieci OT i IT 15

FORTINET

Streszczenie

Operacje produkcyjne korzystające z technologii operacyjnej (OT) coraz częściej stają się obiektem cyberataków. Prawie 75% przedsiębiorstw korzystających z systemów OT miało w ciągu ostatniego roku do czynienia z co najmniej jednym włamaniem dokonanym za pomocą złośliwego oprogramowania[1]. W ramach działań podejmowanych w celu zapewnienia lepszej ochrony tych operacji wspomniane przedsiębiorstwa powinny oceniać potencjalne rozwiązania zabezpieczające w kontekście kilku kluczowych kryteriów.

Po pierwsze osoby nadzorujące wspomniane operacje muszą mieć pewność, że stosowane przez nie technologie zabezpieczeń skutecznie kontrolują dostęp do sieci, uniemożliwiając jednocześnie nieautoryzowane działania w sieci wewnętrznej (ang. lateral movement) między poszczególnymi segmentami sieci. Po drugie osoby te powinny szukać rozwiązań zabezpieczających, które można ze sobą zintegrować w celu wyeliminowania silosów informacyjnych i zmniejszenia liczby roboczogodzin poświęcanych na zarządzanie bezpieczeństwem. Po trzecie osoby te muszą się upewnić, że każde rozważane przez nie rozwiązanie będzie zdolne do obsługi protokołów i funkcji stosowanych w ramach wspomnianych operacji produkcyjnych.

Wprowadzenie — potrzeba modernizacji rozwiązań zabezpieczających w przedsiębiorstwach przemysłowych

Nawet jak na standardy zmian technologicznych, przedsiębiorstwa produkcyjne doświadczają niespotykanego dotąd tempa rozwoju. Aby odpowiednio zarządzać procesami przemysłowymi wiele z tych przedsiębiorstw korzysta z systemów nadzorowania procesów technologicznych (SCADA). Systemy te zbierają dane z czujników, a następnie przesyłają je do przemysłowych systemów sterowania (ICS) służących do zarządzania systemami operacyjnymi przedsiębiorstwa, które zazwyczaj obejmują złożone zestawy generatorów, wentylatorów, robotów przemysłowych i innych urządzeń.

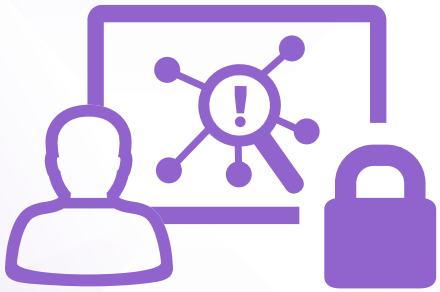
Systemy SCADA i ICS rozwijano bardzo szybko pod kątem zdolności do wykorzystania danych z różnych typów czujników. Systemy te są również coraz częściej stosowane przez firmy zewnętrzne (64% przedsiębiorstw korzystających z systemów OT zapewnia zewnętrznym dostawcom rozwiązań IT pełny lub duży dostęp do swoich systemów SCADA lub ICS[2]). W wyniku tych tendencji wielu producentów podłącza obecnie swoje systemy OT, w tym urządzenia ICS i SCADA, do korporacyjnej sieci IT. Podłączenie takich urządzeń do sieci IT, w skład której wchodzą m.in. wysokiej klasy procesory i pamięci masowe, pozwala na efektywniejsze zarządzanie danymi produkcyjnymi.

Ponadto rosnąca liczba specjalistów ds. operacji produkcyjnych wdraża systemy sterowania online. Na ostatnim webinarium 35% jego uczestników stwierdziło, że ponad połowa ich systemów i urządzeń OT jest podłączona do Internetu, a prawie 10% podało, że wszystkie ich systemy i urządzenia OT są podłączone do Internetu[3].

Prawie dwie trzecie (64%) przedsiębiorstw korzystających z systemów OT z trudem nadąża za tempem zmian dotyczących OT[4]. Bezpieczeństwo jest głównym obszarem, który wymaga tutaj uwagi. Na szczęście odpowiednia kombinacja technologii zabezpieczeń może pozwolić wspomnianym specjalistom na zarządzanie tym ryzykiem.

Poniżej przedstawiono pięć kwestii, o których specjaliści ds. operacji produkcyjnych muszą pamiętać.

„Połączenie środowisk IT i OT pozwala przedsiębiorstwom dostarczać bardziej wydajne i nowoczesne rozwiązania[5]”.



Niestety tylko 55% przedsiębiorstw korzystających z systemów SCADA i ICS stosuje mechanizmy kontroli dostępu oparte na rolach obejmujące wszystkich swoich pracowników[6].

Wdrożenie skutecznych mechanizmów kontroli dostępu do sieci

Urządzenia i systemy OT są coraz bardziej atrakcyjnymi celami dla cyberprzestępców, którzy chcą zakłócić operacje biznesowe, wykraść tajemnice handlowe i zdobyć okup[7]. Niemal 60% przedsiębiorstw korzystających z systemów SCADA i ICS doświadczyło w ciągu ostatniego roku przypadku naruszenia bezpieczeństwa tych systemów, podczas gdy tylko 11% z nich nigdy nie miało do czynienia z takim przypadkiem[8]. Jest to ogromny problem, ponieważ wspomniane systemy często nie mają wbudowanych zabezpieczeń.

Wiele stosowanych obecnie systemów OT zostało zaprojektowanych kilkadziesiąt lat temu w czasach, gdy środowiska IT były oddzielone od środowisk OT, co dotyczyło również operacji produkcyjnych. Podczas projektowania tych systemów okoliczność cyberataków nie była w ogóle brana pod uwagę. W rezultacie wielu systemom OT brakuje nowoczesnych funkcji, które mogłyby je lepiej chronić po połączeniu z systemami IT.

Pierwszą linią obrony systemów SCADA, ICS i innych systemów obsługujących operacje produkcyjne przed cyberprzestępcami, są informacje o wszystkich elementach, które są lub mają zostać podłączone do sieci przedsiębiorstwa. W tym kontekście kluczowe znaczenie mają mechanizmy kontroli dostępu do sieci (NAC). Zważywszy na fakt, że wiele urządzeń OT nie posiada monitorów, typowych systemów operacyjnych lub mocy obliczeniowej (ang. headless), a tym samym nie jest zdolna do przyjmowania poprawek i aktualizacji, tradycyjne podejścia do zabezpieczania punktów końcowych są niewystarczające.

Specjaliści ds. operacji produkcyjnych powinni również stosować mechanizmy kontroli dostępu oparte na rolach, aby zapewnić użytkownikom dostęp tylko do tych urządzeń i aplikacji, do których mają uprawnienia dostępu. Zaufanie musi być stale monitorowane i weryfikowane przez odpowiedni aparat zintegrowany z szerszą platformą zabezpieczeń. Przyjmując w kontekście dostępu do sieci zasadę minimalnego uprzywilejowania, typową dla modelu zabezpieczeń dostępu opartego na zasadzie zerowego zaufania, można jednak lepiej zapobiegać nieautoryzowanemu dostępowi do systemów OT.

Wyniki badań wskazują, że zapewnienie użytkownikom bezpiecznego dostępu do sieci IT i OT ma istotne znaczenie. To właśnie tam wirtualna sieć prywatna (VPN) stosująca uwierzytelnianie wieloskładnikowe zapewnia użytkownikom ochronę podczas dostępu do obszarów sieci korporacyjnej.



„Systemy ICS nie są odporne na skoordynowane ataki... Zważywszy, że systemy ICS projektowano w czasach, gdy nie rozważano nawet możliwości cyberataków, zabezpieczenie tych systemów będzie coraz szerszym obszarem uwzględnianym w kontekście wojny cybernetycznej i badań inżynieryjnych”[9].

Minimalizowanie powierzchni ataku

Obserwowane ostatnio łączenie systemów OT i IT stwarza ryzyko w obu kierunkach. Udany atak na systemy IT może dać przestępcom dostęp do danych i aplikacji OT, potencjalnie zagrażając operacjom i procesom produkcyjnym. Udany atak na systemy ICS lub SCADA może natomiast potencjalnie zmienić działanie sprzętu, co może spowodować uszkodzenie tego sprzętu lub obrażenia wśród pracowników[10]. W najbardziej skrajnych przypadkach złośliwe oprogramowanie atakujące operacje produkcyjne może zagrozić życiu ludzi.

Jednocześnie udany atak na systemy ICS, SCADA i inne systemy OT może otworzyć dostęp do zasobów sieciowych. Niektóre systemy operacyjne stosowane w ramach operacji produkcyjnych nie są zdolne do obsługi standardowego klienckiego oprogramowania zabezpieczającego i nie zapewniają środków służących do neutralizacji luk w zabezpieczeniach. Nawet w przypadku operacji produkcyjnych korzystających z oprogramowania zabezpieczającego neutralizacja luk w zabezpieczeniach jest zazwyczaj trudna, ponieważ systemy OT muszą działać 24 godziny na dobę przez 7 dni w tygodniu i nie można ich przenieść do trybu offline w celu aktualizacji zabezpieczeń.

Z powyższych przyczyn operacje produkcyjne są często bardziej podatne na zagrożenia niż typowy wdrożony przez dział IT serwer, system pamięci masowej lub punkt końcowy. W miarę wzrostu skuteczności rozwiązań zabezpieczających w blokowaniu złośliwego oprogramowania niektórzy cyberprzestępcy zaczynają zwracać uwagę na operacje produkcyjne jako alternatywną i łatwiejszą ścieżkę dostępu do sieci przedsiębiorstw.

Specjaliści ds. operacji produkcyjnych powinni wdrożyć zapory następnej generacji (NGFW) zarówno na granicach sieci, jak i między wewnętrznymi segmentami sieci. Przeprowadzana przez te zapory weryfikacja uprawnień powinna mieć charakter dynamiczny: sygnatury używane do weryfikacji tożsamości użytkowników, kontroli aplikacji i blokowania wykrytych ataków powinny być na bieżąco aktualizowane. Ponadto zapory NGFW powinny obsługiwać różne formaty, aby optymalizować nakłady na sprzęt w przypadku, gdy wspomniane zapory będą wdrażane w celu ochrony segmentów o różnych rozmiarach i różnym natężeniu ruchu. Jeszcze jednym ważnym aspektem jest zdolność do prowadzenia inspekcji danych szyfrowanych przy użyciu protokołu Secure Sockets Layer (SSL) / Transport Layer Security (TLS) bez narażania na szwank wydajności zapór NGFW.

„Cyberatak, który udanie narusza zabezpieczenia systemu OT lub podłączonych do sieci urządzeń, takich jak zawory, wskaźniki lub przełączniki, może przynieść katastrofalne skutki dla najważniejszych usług i infrastruktury, środowiska, a nawet życia ludzkiego”[11].

Eliminowanie silosów w celu zwiększenia skuteczności zabezpieczeń

W przypadku większości operacji produkcyjnych stosuje się rozwiązania zabezpieczające pochodzące od wielu dostawców. Wskutek wybierania najlepszych w swojej klasie zabezpieczeń dla danego urządzenia powstają jednak silosy. Ma to kilka negatywnych skutków. Jednym z nich jest brak komunikacji między różnymi mechanizmami zabezpieczeń w kontekście wykrytych zagrożeń. Jeśli określone rozwiązanie w jednym obszarze sieci wykryje lub udaremni próbę ataku, złośliwe oprogramowanie może odnieść sukces w innym miejscu. Problem pogłębi się, gdy okaże się, że zabezpieczenia sieci OT nie mogą zostać zintegrowane z funkcjami ochrony poczty elektronicznej, punktów końcowych, przełączników lub punktów dostępu bezprzewodowego lub zaporami następnej generacji.

Przedsiębiorstwa korzystające z systemów OT powinny szukać rozwiązań zabezpieczających, które będą mogły zostać zintegrowane w celu wymiany informacji o wykrytych zagrożeniach i odpowiedniej reakcji na te zagrożenia. Integracja może również zapewnić personelowi technicznemu większą widoczność w kontekście wykrywania zagrożeń i reagowania na nie we wszystkich systemach OT i IT w całym przedsiębiorstwie oraz stanu bezpieczeństwa całej sieci.

56%

przedsiębiorstw korzystających z systemów OT doświadczyło w ciągu ostatnich 12 miesięcy przypadku naruszenia bezpieczeństwa[12].

Zwiększenie widoczności i automatyzacja

Dla 45% przedsiębiorstw korzystających z systemów OT niedobór wykwalifikowanych specjalistów ds. IT i cyberbezpieczeństwa jest dużym wyzwaniem[13] i może zmniejszyć zdolność do wdrażania u siebie zaawansowanych technologii zabezpieczeń i praktyk z dziedziny bezpieczeństwa. Zespoły zajmujące się operacjami produkcyjnymi muszą zatem wdrażać rozwiązania automatyzujące czynności ręczne, aby usprawnić procesy w obliczu wspomnianych braków kadrowych.

Oceniając rozwiązania zabezpieczające, specjaliści ds. operacji produkcyjnych powinni szukać produktów, które nie tylko dadzą się zintegrować z resztą architektury zabezpieczeń, ale także zautomatyzują procesy wykrywania zagrożeń i reagowania na zagrożenia zarówno w sieci OT, jak i w sieci IT. Połączenie automatyzacji i orkiestracji może skrócić z dni do minut czas reakcji sieci na konkretne zagrożenie. Może również znacznie zmniejszyć liczbę roboczogodzin przeznaczonych na zarządzanie infrastrukturą, ponieważ nie będzie już wówczas konieczne czasochłonne sporządzanie raportów dotyczących różnych rozwiązań zabezpieczających i ręczne kompilowanie uzyskanych w ten sposób informacji.

Zintegrowana i zautomatyzowana infrastruktura zabezpieczeń może wreszcie uprościć audyt i wymaganą przepisami sprawozdawczość, jeszcze bardziej zmniejszając obciążenie pracą ręczną zbyt małego personelu informatycznego.

Dla 45% przedsiębiorstw korzystających z systemów OT brak wykwalifikowanych pracowników jest dużym wyzwaniem[14].

Zapewnienie zgodności rozwiązań zabezpieczających z siecią OT

Między innymi ze względu na dotychczasowe oddzielenie systemów ICS i SCADA od sieci IT, wiele stosowanych w sieciach IT rozwiązań zabezpieczających nie obsługuje niektórych protokołów OT. Przedsiębiorstwa łączące systemy OT z sieciami IT muszą zatem upewnić się, że kluczowe elementy ich infrastruktury zabezpieczeń będą takie protokoły OT obsługiwać.

Na przykład niektóre bezpieczne środowiska testowe (ang. sandbox) nie są zgodne z niektórymi systemami operacyjnymi OT. Środowiska te służą do identyfikacji nieznanych zagrożeń i ataków typu „zero-day" w drodze testowania pakietów potencjalnie zainfekowanych złośliwym oprogramowaniem, zanim zostaną one wpuszczone do sieci. Jeśli jednak takie środowisko nie będzie zdolne do uruchomienia konkretnego protokołu OT, nie przeprowadzi wspomnianego testowania. Specjaliści ds. operacji produkcyjnych muszą zatem upewnić się, że stosowane przez nich bezpieczne środowiska testowe mogą obsługiwać i chronić konkretne urządzenia OT takie jak programowalne sterowniki logiczne (PLC) firmy Siemens lub zdalne terminale (RTU) firmy Schneider.

W celu zapewnienia wspomnianej zgodności należy w ten sam sposób zweryfikować działanie każdego zabezpieczenia sieci.



Rozwiązania zabezpieczające sieć OT muszą obsługiwać wszystkie protokoły stosowane w odniesieniu do używanych przez dane przedsiębiorstwo technologii SCADA, ICS, RTU, PLC i innych technologii operacyjnych.

Podsumowanie — właściwa architektura zabezpieczy sieci OT i IT

Specjaliści ds. operacji produkcyjnych, którzy nie dysponują odpowiednimi rozwiązaniami zabezpieczającymi narażają swoje organizacje na ryzyko. W kontekście połączenia sieci OT i IT oraz wzrostu liczby systemów i urządzeń OT wyzwania i zagrożenia nigdy nie były większe, a tradycyjne zabezpieczenia po prostu nie są zdolne do ochrony tak zwiększonej powierzchni ataku.

W odpowiedzi na te zagrożenia specjaliści ds. operacji produkcyjnych muszą zmodernizować swoją architekturę zabezpieczeń tak, aby oferowała kompleksowe mechanizmy kontroli dostępu do sieci, uniemożliwiała nieautoryzowane działania w sieci wewnętrznej, zapewniała dobrą widoczność i scentralizowane mechanizmy kontroli oraz była w pełni zgodna ze środowiskami OT.

Połączenie sieci OT i IT przyczyniło się do zwiększenia ryzyka związanego ze zwiększającą się powierzchnią ataku na operacje produkcyjne. Specjaliści ds. operacji produkcyjnych nie mogą zatem już dłużej zwlekać z reakcją na takie rosnące zagrożenie dla bezpieczeństwa zarządzanych przez nich środowisk OT.

[1] „State of Operational Technology and Cybersecurity Report", Fortinet, 15 marca 2019 r.

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

[3] „Webinar: Securing the Future of Industrial Control Systems", Fortinet, dostęp z dnia 9 września 2019 r.

[4] „State of Operational Technology and Cybersecurity Report", Fortinet, 15 marca 2019 r.

[5] „Causes and Consequences of IT and OT Network Convergence", Fortinet, 25 lipca 2019 r.

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

[7] Joe Weiss, „Industrial control systems: The holy grail of cyberwar", The Christian Science Monitor, 24 marca 2017 r.

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

[9] Joe Weiss, „Industrial control systems: The holy grail of cyberwar", The Christian Science Monitor, 24 marca 2017 r.

[10] John Maddison, „Resolving the Challenges of IT-OT Convergence", CSO, 21 czerwca 2018 r.

[11] Ibid.

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

[13] „State of Operational Technology and Cybersecurity Report", Fortinet, 15 marca 2019 r.

[14] Ibid.

www.fortinet.com

Copyright © 2019 Fortinet, Inc. Wszelkie prawa zastrzeżone. Fortinet®, FortiGate®, FortiCare®, FortiGuard® oraz niektóre inne znaki są zastrzeżonymi znakami towarowymi spółki Fortinet, Inc. Pozostałe nazwy związane z Fortinet zawarte w niniejszym dokumencie również mogą być znakami towarowymi lub zastrzeżonymi znakami towarowymi Fortinet. Wszelkie inne nazwy produktów lub spółek mogą być znakami towarowymi ich odpowiednich właścicieli. Przedstawione w niniejszym dokumencie parametry wydajności i inne dane uzyskano podczas testów laboratoryjnych w warunkach idealnych, faktyczna wydajność może być zatem inna. Na wartość parametrów wydajności mogą mieć wpływ zmienne sieciowe, różnorodne środowiska sieciowe i inne uwarunkowania. Żadne ze stwierdzeń zawartych w tym dokumencie nie stanowi wiążącego zobowiązania ze strony Fortinet, a Fortinet odrzuca wszelkie wyraźne lub dorozumiane gwarancje i rękojmie, z wyjątkiem gwarancji udzielonych przez Fortinet na mocy wiążącej umowy z kupującym podpisanej przez głównego radcę prawnego Fortinet, w której Fortinet zagwarantuje, że określony produkt będzie działać zgodnie z wyraźnie wymienionymi w takim dokumencie parametrami wydajności, a w takim przypadku wyłącznie określone parametry wydajności wyraźnie wskazane w takiej wiążącej umowie pisemnej będą wiązać Fortinet. Wszelka tego typu gwarancja będzie dotyczyć wyłącznie wydajności uzyskiwanej w takich samych warunkach idealnych, w jakich Fortinet przeprowadza wewnętrzne testy laboratoryjne. Fortinet w całości odrzuca wszelkie wyraźne lub dorozumiane przyrzeczenia, oświadczenia i gwarancje związane z tym dokumentem. Fortinet zastrzega sobie prawo do zmieniania, modyfikowania, przenoszenia lub innego korygowania niniejszej publikacji bez powiadomienia (zastosowanie ma najnowsza wersja publikacji).

443523-0-0-PL

23 kwietnia, 2020 11:31 AM

eb-protecting-plant-manufacturing-operations_PL