Zabezpieczenie sieci OT zaczyna się od zapewnienia widoczności

Większa przejrzystość sieci w infrastrukturze przemysłowej i krytycznej

Spis treści

Streszczenie 3

01 Obrona rozszerzającej się powierzchni ataku w sieci OT 4

02 Nowe rozwiązanie zabezpieczające sieć OT 6

03 Widoczność całej powierzchni ataku 8

04 Kontrola dostępu, aktualizacje zabezpieczeń itp. 10

05 Informacje o środowisku 11

06 Większa przejrzystość sieci w infrastrukturze przemysłowej i krytycznej 12

FORTINET

Streszczenie

Systemy technologii operacyjnych (OT) kontrolują infrastrukturę przemysłową i krytyczną w sektorach takich jak energetyka, usługi użyteczności publicznej, produkcja przemysłowa, komunikacja, transport i obrona. We wszystkich tych sektorach w coraz szerszym zakresie wdrażane są nowe technologie cyfrowe, co sprawia, że sieci OT są coraz częściej podłączane do sieci technologii informatycznych (IT) podłączonych z kolei do Internetu. W rezultacie takiego podłączenia stale powiększająca się powierzchnia ataku na sieci IT naraża również odizolowane wcześniej systemy OT na wszystkie możliwe zagrożenia dotyczące sieci IT. Ze względu na fakt, że tradycyjne strategie zabezpieczeń nie zostały opracowane z myślą o szczególnych i wrażliwych potrzebach sieci OT, specjaliści ds. zarządzania siecią muszą szukać rozwiązań zabezpieczających, które zapewnią widoczność i kontrolę oraz informacje pozwalające lepiej zrozumieć środowisko OT.

01: Obrona rozszerzającej się powierzchni ataku w sieci OT

Do niedawna najlepszym sposobem ochrony sieci OT było ich całkowite odizolowanie od sieci IT (ang. „air gapping"). Obecnie jednak prawie trzy czwarte przedsiębiorstw zgłasza posiadanie przynajmniej podstawowych połączeń między swoimi środowiskami IT i OT[1]. Oznacza to, że wynikająca ze wspomnianej izolacji ochrona praktycznie znika i sieci OT są narażone na te same zagrożenia co sieci IT.

W obliczu konieczności obrony sieci OT przed rosnącą falą zaawansowanych ataków mogących wykorzystać nieskończenie większą powierzchnię ataku centra zarządzania siecią znalazły się pod ogromną presją, aby w tym samym czasie zapewnić zarówno bezpieczeństwo, jak i operacyjną dostępność sieci OT. W związku z tym muszą na nowo rozważyć istniejący system zabezpieczeń.

Trzy czwarte przedsiębiorstw zgłasza posiadanie przynajmniej podstawowych połączeń między swoimi środowiskami IT i OT.

97%

przedsiębiorstw dostrzega problemy związane z zapewnieniem bezpieczeństwa w połączonych środowiskach IT i OT[2].

02: Nowe rozwiązanie zabezpieczające sieć OT

W kontekście łączenia środowisk OT i IT wdrożenie skutecznej strategii zabezpieczenia środowiska OT wymaga pewnych specjalistycznych rozważań. Próby przeciwdziałania zagrożeniom polegające na wdrożeniu w środowisku OT standardowych zapór, bezpiecznych środowisk testowych i systemów ochrony przed włamaniami (IPS) wiążą się z niedopuszczalnymi i niedającymi się przewidzieć rezultatami, ponieważ narzędzia zabezpieczające środowiska OT powinny być specjalnie dostosowane do protokołów, metod komunikacji i usług właściwych dla tych wrażliwych środowisk.

Zamiast zatem wdrażać punktowe zabezpieczenia służące ochronie nowo wykrytych luk, przedsiębiorstwo powinno umieścić zabezpieczenia na najbardziej podstawowych poziomach środowiska OT, aby uwzględnić szerszą perspektywę. Należy również pamiętać, że poszczególne części infrastruktury zabezpieczeń organizacji muszą ze sobą współdziałać w ramach spójnego i skoordynowanego systemu.

Właściwe podejście do problemu zapewnić może wdrożenie zintegrowanej, poddanej segmentacji wielowarstwowej architektury zabezpieczeń. Takie kompleksowe rozwiązanie może zapewnić ochronę wykraczającą poza zwykłe zablokowanie potencjalnie zaatakowanego systemu wentylacji podłączonego wcześniej do Internetu. Zintegrowane rozwiązanie zabezpieczające może zapewnić przejrzystą widoczność wszystkich urządzeń, możliwość analizy kontekstu w czasie rzeczywistym oraz oparte na zasadach mechanizmy zapewniające integralność urządzeń lub systemów przy jednoczesnym zabezpieczeniu innych krytycznych elementów środowiska OT.

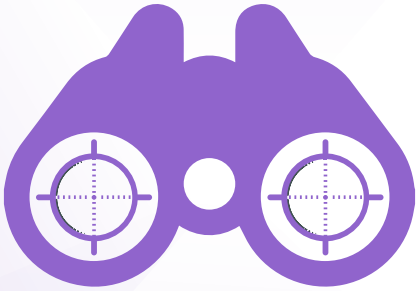


65% przedsiębiorstw korzystających z systemów OT nie ma mechanizmów kontroli dostępu opartych na rolach, co daje atakującym większą swobodę poruszania się w środowiskach OT[3].

03: Widoczność całej powierzchni ataku

Zagwarantowanie dobrego działania systemu OT wymaga zapewnienia nieprzerwanej widoczności każdego podłączonego do niego urządzenia przewodowego i bezprzewodowego (przy uwzględnieniu faktu, że urządzenia takie są na bieżąco podłączane i odłączane od sieci lub zmieniają swoją lokalizację). Obecnie bardzo powszechne jest stosowanie w środowiskach OT najróżniejszych urządzeń bezprzewodowych i urządzeń związanych z Internetem rzeczy (IoT) (takich jak inteligentne czujniki parametrów środowiskowych). Ze względu na fakt, że urządzenia te łączą się z zewnętrzną siecią informatyczną w celu uzyskania dodatkowych możliwości, mogą tym samym stanowić potencjalne „tylne wejście" dla ataków ukierunkowanych na niezabezpieczone systemy OT.

Zintegrowana architektura zabezpieczeń może zapewnić przejrzystą, scentralizowaną widoczność całego środowiska OT. W celu zapewnienia tego rodzaju ochrony, architektura taka powinna mieć wbudowane połączenia interfejsów API oraz otwarte interfejsy API REST, aby przedsiębiorstwo mogło w ten sposób połączyć z nią swoje rozwiązania zabezpieczające. Procesowi zapewnienia widoczności może również 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).



Nie da się ochronić tego, czego się nie widzi. 82% organizacji przyznało, że nie jest w stanie zidentyfikować wszystkich urządzeń podłączonych do swojej sieci[4].

04: Kontrola dostępu, aktualizacje zabezpieczeń itp.

Sprawowanie kontroli w środowisku OT polega na określeniu zwykłego ruchu i wstępnym zdefiniowaniu zatwierdzonych funkcji, aby przypadki wykrycia odstępstw od normy zostały rozpoznane i zabezpieczenia odpowiednio na nie zareagowały w czasie rzeczywistym. Na szczęście zachowania urządzeń w środowiskach OT mają zazwyczaj charakter statyczny i mieszczą się w dającym się przewidzieć zakresie, prawdopodobieństwo natychmiastowego wykrycia anomalii jest tam zatem większe niż w przypadku tradycyjnych środowisk IT.

Mechanizmy kontroli powinny obejmować funkcje przełączania, segmentacji sieci (typu „północ-południe" i „wschód-zachód") oraz mikrosegmentacji zasobów sieciowych. Kolejną krytyczną funkcją wymaganą w środowiskach OT jest zdolność do wymuszania ruchu z przestarzałych urządzeń przez zaporę następnej generacji (NGFW).

Ponadto przedsiębiorstwo musi być w stanie stosować i egzekwować zasady dostępu na podstawie typu użytkownika i urządzenia podłączonego do sieci. Dynamiczne, oparte na rolach mechanizmy kontroli dostępu muszą być zdolne do tworzenia w ramach sieci segmentów grupujących aplikacje, łączących dane i ograniczających dostęp do określonych grup w celu lepszego zabezpieczenia środowiska OT. Ten rodzaj szczegółowej kontroli jest czasami określany mianem **segmentacji opartej na celach biznesowych** (ang. intent-based segmentation), w ramach której kontrola dostępu jest dostosowywana zależnie do dokonywanej na bieżąco oceny zaufania[5].

Dawniej mechanizmy kontroli dostępu przyjmowały statyczne wartości zaufania dla użytkowników, urządzeń i aplikacji. Wiarygodność może jednak ulegać wahaniom z powodu zwykłych zmian zachodzących w działalności biznesowej lub w wyniku pojawienia się zagrożeń. Segmentacja oparta na celach biznesowych łączy w sobie funkcje kontroli dostępu ze stale aktualizowanymi ocenami zaufania na podstawie danych pozyskanych ze źródeł wewnętrznych i zewnętrznych.

Segmentacja oparta na celach biznesowych określa typ użytkownika, urządzenia i potrzeby biznesowej, aby kontrolować dostęp urządzeń i użytkowników do sieci na podstawie określonych potrzeb biznesowych.

05: Informacje o środowisku

Specjaliści ds. zarządzania siecią mogą codziennie otrzymywać tysiące alertów bezpieczeństwa. Po uzyskaniu informacji o podejrzanej aktywności na konkretnym adresie IP ręczne określenie lokalizacji podejrzanego urządzenia i uzyskanie wszystkich innych informacji o danym zdarzeniu w celu stwierdzenia, czy jest to atak, czy zwykła anomalia, może zająć wiele godzin. Niedobór wykwalifikowanych pracowników potęguje ten problem.

Ilekroć urządzenie w środowisku OT jest atakowane, przedsiębiorstwo musi natychmiast otrzymać odpowiedni alert wraz z kontekstem zagrożenia, aby móc szybko stwierdzić, jakie konkretne działania musi podjąć. Rozwiązanie oferujące mechanizm zarządzania informacjami i zdarzeniami dotyczącymi bezpieczeństwa (SIEM) może przyspieszyć analizę zagrożenia, zautomatyzować reakcję i przyspieszyć działania naprawcze dzięki funkcjom jednolitej korelacji zdarzeń i zarządzania ryzykiem.

W przypadku wykrycia podejrzanego urządzenia próbującego uzyskać dostęp do sieci, zintegrowane mechanizmy kontroli dostępu mogą automatycznie przesłać specjaliście ds. zarządzania siecią powiadomienie o tym zagrożeniu wraz z odpowiednim kontekstem w czasie rzeczywistym. W rezultacie specjalista taki może szybko zlokalizować i rozwiązać zaistniały problem (co zajmie już nie kilka dni, ale kilka sekund).

64% osób odpowiedzialnych za system OT stwierdziło, że nadążenie za zmianami jest dla nich największym wyzwaniem, a 45% z nich uznało, że ma ograniczone możliwości ze względu na brak wykwalifikowanych pracowników[6].

06: Większa przejrzystość sieci w infrastrukturze przemysłowej i krytycznej

Ochrona rozszerzającej się powierzchni ataku na systemy OT bez uszczerbku dla ich działania stanowi nie lada wyzwanie. Połączenie ze sobą sieci OT i IT zapewnia duże korzyści, ale oznacza również nowe zagrożenia, które mogą nie być znane specjalistom ds. zabezpieczeń i zarządzania siecią.

Przedsiębiorstwo musi mieć kompleksową widoczność każdego użytkownika i urządzenia podłączonego w danym momencie do swojej infrastruktury, ponieważ wymaga tego odpowiednie zabezpieczenie sieci OT. Ponadto musi korzystać zarówno z mechanizmów scentralizowanego zarządzania i alternatywnej kontroli (np. SIEM, NAC), jak i mechanizmów ochrony punktów końcowych i segmentacji sieci. Potrzebuje również zintegrowanej architektury zabezpieczeń, która połączy różne rozwiązania w spójny system zdolny do ochrony środowiska OT przed pełnym spektrum zagrożeń dotyczących sieci IT.

[1] „Independent Study Pinpoints Significant SCADA/ICS Cybersecurity Risks", Fortinet, 7 maja 2018 r.

[2] Ibid.

[3] „State of Operational Technology and Cybersecurity Report", Fortinet, marzec 2019 r.

[4] Jeff Goldman, „IoT Security Fail: 82 Percent of Companies Can't Identify All Network-Connected Devices", eSecurity Planet, 8 listopada 2017 r.

[5] „A Network Operations Guide for Intent-based Segmentation", Fortinet, 5 lutego 2019 r.

[6] „State of Operational Technology and Cybersecurity Report", Fortinet, marzec 2019 r.

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).

360444-0-0-PL

czerwca 26, 2019 8:16 PM

eb-network-operations-analyst_PL