Robert Dąbrowski,
SE Manager, Fortinet

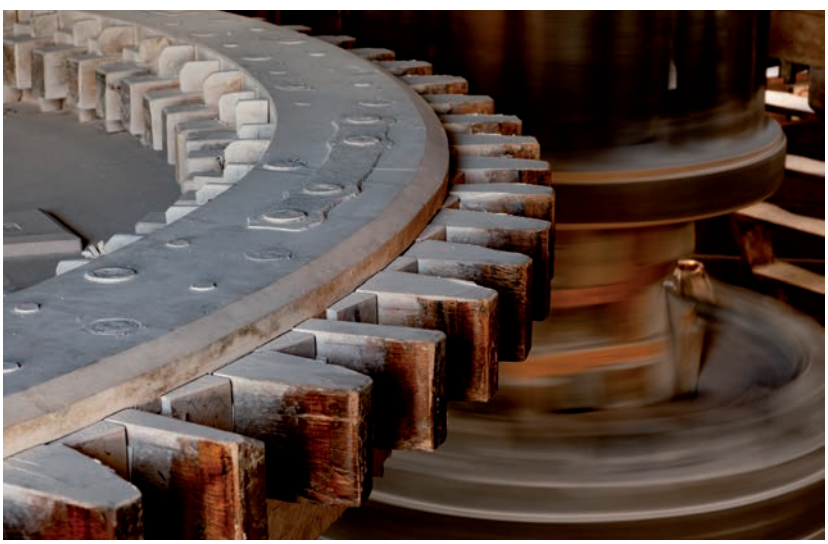
Przeciwdziałanie zagrożeniom bezpieczeństwa IoT i OT związanym z cyfrową transformacją za pomocą technik „Deception"/oszukiwania

Obecny powszechnie oczekiwany status dostępu do sieci to „podłączony". Oprócz tradycyjnych modeli obliczeniowych, łączność jest stanem domyślnym dla urządzeń mobilnych i pełnej gamy rozwiązań Smart-X, w tym samochodów i systemów transportowych, urządzeń, budynków, hal produkcyjnych, miast i infrastruktur krytycznych. W rzeczywistości, wiele osób żyje w otoczeniu czujników opartych na protokole IP, które zapewniają nam - i zdumiewającej liczbie urządzeń - łączność i komunikację.

Co się zmieniło w świecie OT?

Odpowiedzią jest ryzyko. Nawet w przypadku podłączenia do sieci, wiżkszołœ rozwiązań OT była chroniona, poniewa£ były one odizolowane od sieci korporacyjnej i publicznej. Piżtnałcie lat temu, mimo £e czujniki przemysłowe wykorzystywały do komunikacji sieci IP, atakujący byli bardziej skoncentrowani na infrastrukturze IT, gdzie mogli uzyskaœwiżkszy i szybszy zwrot z inwestycji w złołliwe oprogramowanie. Próba przejżcia kontroli nad prostym czujnikiem wdro£onym w sieci OT wiązała siż z dużą ilością dodatkowej pracy - i dawała niewielką szansż na zysk. A ransomware, które obecnie jest wykorzystywane przez napastników do przechwytywania krytycznych systemów OT i urządzeń IoT dla okupu, tak naprawdż zaczżło działaœdopiero w 2005 r., a nawet wtedy przez lata było ukierunkowane przede wszystkim na urządzenia dla u£ytkowników ko§cowych. W rzeczywistołci, do czasu uderzenia Stuxnetu w 2010 r., zainteresowanie atakowaniem systemów SCADA i ICS było wciąż niewielkie.

Czujniki OT i wczesne funkcje urządze§ IoT były tak proste, £e nie było wiele do wykorzystania. Ich ochrona polegała przede wszystkim na izo-

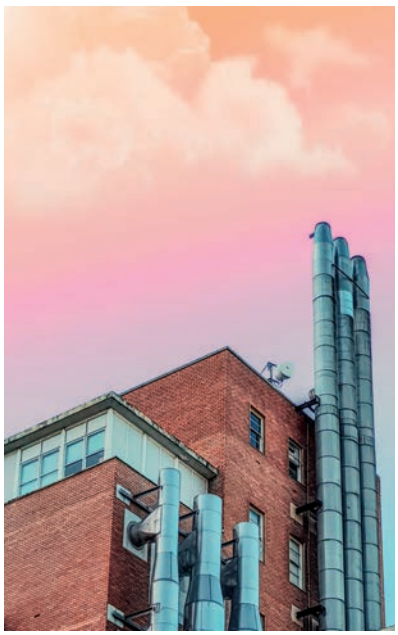


lowaniu od Internetu łr odowiska OT i umieszczeniu firewalla przed siecią OT w celu odseparowania od IT. Obecnie jednak to wszystko siż zmieniło. Te proste czujniki stały siż teraz „inteligentnymi czujnikami", oferującymi szerszy zakres mo£liwołci. Urządzenia IoT - lub przemysłowe IoT (IIoT) w niektórych łr odowiskach - równie£ stały siż bardziej zaawansowane. Jednoczełnie, aby generowacewiększą wydajnołce i zapewnicesprawne reagowanie na nowe potrzeby rynku, sieci i urządzenia IT oraz OT zaczżły siż zbiegace.Wszystko to sprawiło, £e powierzchnia ataku OT stała siż bardziej skomplikowana do ochrony.

Zrozumienie krajobrazu zagrożeń IoT/OT

Oto niektóre z zagro£e§ dla bezpiecze§stwa, które dotyczą systemów i rozwiązań IoT oraz OT:

- Czujniki IoT/OT są coraz czżłciej podłączane do sieci IP, umożliwiając zdalny dostżp, co oznacza, £e mogą bycerównie£ atakowane przez Internet z ka£dego miejsca na łwiecie.
- Czujniki IoT i OT albo korzystają ze starszego systemu operacyjnego (łr ednio 10-15 lat) wdro£onego w delikatnym łr odowisku, którego nie mo£na dezaktywowacew celu aktualizacji lub wprowadzenia poprawek, albo z zastrze£onego systemu operacyjnego, który nie pozwala na instalacjż oprogramowania zabezpieczającego. Utrudnia to ustanowienie tradycyjnej kontroli bezpiecze§stwa, jak w przypadku zwykłych zasobów informatycznych.
- Nowsze czujniki IoT i OT posiadają teraz znacznie szerszy zakres mo£liwołci, co czyni je bardziej atrakcyjnymi dla przestżpców. Ponadto, w ciągu ostatniej dekady pojawiła siż nowa rasa napastników. Hakktywiłci i cyberterroryłci są gotowi do wywołania naruszenia o du£ym zasiżgu, które nie przyniesie £adnych korzyłci finansowych, ale wyrządzi szkody gospodarcze lub infrastrukturalne w kraju lub regionie - w celu wsparcia programu politycznego.
- Wiele urządze§ IoT nie mo£e byceaktualizowane. Zamiast tego, aby zapewnicechronż, organizacje muszą polegacena kontrolach dostżpu, gdzie obowiązuje zasada „zero zaufania".



Od czasu Stuxnet w 2010 r., sieci OT są coraz czżłciej atakowane. Wszyscy pamiżtamy botnet Mirai zaprojektowany w celu kompromitacji milionów urządzeń IoT i OT na całym łwiecie, aby przeprowadzicudany atak DDoS na ameryka§ską infrastrukturż internetową. Ataki cybernetyczne oparte na technologii OT wymierzone zostały w krajowe sieci elektryczne, zaciemniając domy setek tysiżcy osób. Ataki ukierunkowane na urządzenia IoT/OT zainstalowane w stacjach pomp wody w łr odkowo-wschodnim pa§stwie przez podmiot z innego pa§stwa były próbą zatrucia dostaw wody poprzez zwiżkszenie poziomu chloru w wodzie płynącej do obszarów mieszkalnych.

Jak wykorzystać techniki „Deception" do ochrony infrastruktury OT?

Mo£na zadacepytanie, czy to jest nowa rzeczywistołce, w której £yjemy, jak mogż chronicemoją sieceprzed zagro£eniami związanymi z Internetem rzeczy i OT? Odłączyć je? Uaktualnicefirmware? Zastosowacekontrolż dostżpu do sieci? Zastosowacesegmentacjż sieci? Odpowied®mo£e byceTAK dla ka£dego lub wszystkich, w zale£nołci od okolicznołci. Istnieje jednak inna strategia, która pozwala organizacjom byceznacznie bardziej proaktywnymi. Mianowicie poprzez zintegrowanie technologii „Deception", czyli oszukiwania z obecnym stosem zabezpiecze§. Proaktywne podejłcie do bezpiecze§stwa, takie jak wykorzystanie technologii „Deception", nie atakuje

napastnika. Zamiast tego, proaktywnie wykorzystuje techniki i taktykż atakującego przeciwko niemu. Pomysł jest prosty. Technologia „Deception" pozwala zespołowi IT na „wdro£enie" wirtualnych, fałszywych elementów w infrastrukturze, które generują fałszywe dane na stacjach ko§cowych i na serwerach. Ta sfabrykowana sieœoszukuje napastników, zwabiając ich z dala od krytycznych zasobów i uniemożliwiając im wyrządzenie rzeczywistych szkód w sieci. Ale co wa£niejsze, poniewa£ wszystkie legalne urządzenia i procesy wiedzą, £e te elementy są fałszywe, tylko nieautoryzowani u£ytkownicy, urządzenia i aplikacje będą staraœsiż je wykorzystaœ.

Strategia ta jest szczególnie skuteczna w dojrzałych ł r odowiskach sieciowych. Dodanie strategii „Deception", czyli wprowadzania napastnika w błąd do rozwiązań SOC, na przykład, umo£liwia zespołom IT wykorzystanie „Deception"/ oszustwa jako „®ódła alertów o wysokiej wiarygodnołci". Poniewa£ alarmy związane z technologiami „Deception" są wyzwalane tylko przez nieautoryzowanych u£ytkowników, urządzenia i aplikacje, organizacje mogą je skuteczniej wykorzystywaœw celu stworzenia automatyzacji wokół mo£liwoł ci polowania na zagro£enia i reagowania na incydenty.

Co wiżcej, najlepsze technologie „Deception" nie tylko chronią przed znanymi zagro£eniami, ale tak£e potrafią wykrywaœ,analizowaœi broniœprzed atakami zero-day i innymi zaawansowanymi atakami, czżsto w czasie rzeczywistym. Technologie „Deception" pozwalają na bardziej proaktywną postawż w zakresie bezpiecze§stwa poprzez oszukiwanie napastników, wykrywanie ich, a nastżpnie pokonywanie, co pozwala przedsiżbiorstwu wróciœdo normalnej pracy.

Technologia „Deception" jako część strategii bezpieczeństwa dla OT

Oto kilka kluczowych powodów, dla których technologia „Deception" powinna byœwłączona do ka£dego stosu zabezpiecze§:

1. Zapewnia ona wczesne wykrywanie po dotarciu do celu, czżsto przed dokonaniem powa£nych uszkodze§ przez obecne w sieci złołliwe oprogramowanie.
2. Skraca czas przebywania w sieci - obecnie ponad 6 miesiżcy - dzižki wykrywaniu złołliwego oprogramowania zaprojektowanego do cichego poszukiwania luk w sieci i unikania ich wykrycia.
3. Poniewa£ jest to system odporny na awarie, co oznacza, £e działa tylko wtedy, gdy coł działa nieprawidłowo, skutecznie zmniejsza liczbż fałszywych trafie§.
4. Mo£na ją wdro£yœw wiżkszołci ł r odowisk OT w celu uzyskania widocznołci i kontroli nad IoT i innymi urządzeniami OT, które nie mogą byœchronione przy u£yciu bardziej tradycyjnych rozwiązań.
5. Dobra technologia wykrywania jest wysoce skalowalna i ma niewielki lub £aden wpływ na normalną wydajnołœ sieci.
6. Konfiguracja i zarządzanie rozwiązaniem „Deception" jest proste, a wykrywanie zagro£e§ jest w pełni zautomatyzowane.

Wdrażając technologiż „Deception" jako czżłœ stosu zabezpiecze§, mo£e ona działaœjako „®ódło alertu o wysokiej wiarygodnołci" w celu zautomatyzowania wykrywania, reagowania i usuwania zagro£e§.

Dowiedz siż, w jaki sposób Fortinet mo£e pomóc w zwiżkszeniu bezpiecze§stwa i utrzymaniu zgodnoł ci z przepisami w ka£dym ł r odowisku połączonym z ICS/SCADA: *www.fortinet.com/solutions/industries/scada-industrial-control-systems.html* □