RAPORT

Raport z niezależnego badania cyberbezpieczeństwa systemów SCADA/ICS

Spis treści

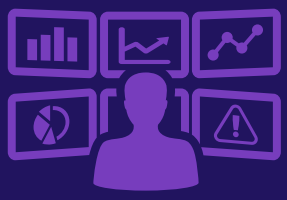
Streszczenie

Wiele przedsiębiorstw i agencji rządowych zaczęło w ostatnich latach korzystać z systemów nadzorowania procesów technologicznych (SCADA) lub przemysłowych systemów sterowania (ICS), systemy te stoją jednak w obliczu poważnych wyzwań w zakresie bezpieczeństwa **Niemal 60%** takich przedsiębiorstw i agencji przebadanych na zlecenie firmy Fortinet przez agencję Forrester Consulting stwierdziło, że w minionym roku **doświadczyło naruszenia bezpieczeństwa** posiadanego systemu SCADA/ICS. Ponadto wiele z tych przedsiębiorstw i agencji wystawia się na jeszcze większe ryzyko, zapewniając swoim partnerom technologicznym i innym podmiotom wysoki poziom dostępu do tych systemów. Organizacje te zgłaszają również, że ich tradycyjne systemy IT **są połączone z systemami SCADA/ICS**, co daje hakerom dodatkowe możliwości zaatakowania tych systemów.

Mimo występowania tych zagrożeń, wiele organizacji w ogóle nie korzysta z dostępnych zabezpieczeń służących do ochrony systemów SCADA/ICS. Mniej więcej **50%** objętych badaniem organizacji **nie wdrożyła w tych systemach funkcji szyfrowania ruchu opartych na protokołach SSH lub TLS**, a wiele tych organizacji nie stosuje wobec pracowników żadnych mechanizmów kontroli dostępu opartego na rolach.

Jednocześnie wiele zbadanych organizacji otwiera hakerom nowe ścieżki ataku, zezwalając na podłączenie swoich systemów SCADA/ICS do zewnętrznych technologii takich jak system nawigacji satelitarnej (GPS), system aktywnej identyfikacji radiowej RFID lub różnego rodzaju urządzenia Wi-Fi. W tym samym czasie 97% respondentów stwierdziło, że integracja tradycyjnych technologii informatycznych (IT) i technologii operacyjnych (OT) niesie ze sobą zagrożenia dla bezpieczeństwa.

O ile zła wiadomość jest taka, że systemy SCADA/ICS są narażone na różne ataki, o tyle dobra wiadomość jest taka, że ich operatorzy mogą podjąć dodatkowe działania, aby te systemy chronić za pomocą dodatkowych zabezpieczeń.



SCADA a ICS

Systemy ICS są często zarządzane za pośrednictwem systemów SCADA, które zapewniają operatorom graficzny interfejs użytkownika służący do monitorowania statusu systemu, otrzymywania alertów lub wprowadzania zmian w zarządzaniu procesami.

Według prognoz wartość rynku systemów ICS szybko wzrośnie i wyniesie

81 mld USD w 2021 r.

Co roku zwiększa się powierzchnia ataku.

Według prognoz wartość rynku systemów SCADA będzie rosnąć w tempie **6,6%** r/r i wyniesie

13,43 mld USD

w 2022 r.

Systemy SCADA/ICS — atrakcyjne cele dla cyberprzestępców

W ostatnich latach wiele przedsiębiorstw, nie tylko energetycznych i wodociągowych, wdrożyło systemy SCADA/ICS w celu automatyzacji działań związanych ze zbieraniem danych i obsługą sprzętu. Systemy te stały się jednak atrakcyjnymi celami dla hakerów mających na celu zakłócenie działalności biznesowej, wymuszenie okupu lub zaatakowanie krytycznej infrastruktury w obcym kraju[1]. Wyniki przeprowadzonych przez firmę Forrester badań wskazują, że w ciągu ostatniego roku **56%** organizacji korzystających z systemów SCADA/ICS **zgłosiło naruszenie bezpieczeństwa**, a tylko 11% z nich stwierdziło, że do takiego naruszenia nigdy u nich nie doszło.

Powstające wskutek ataków szkody mogą być bardzo poważne. W grudniu 2015 r. kilka regionów zachodniej Ukrainy doświadczyło przerw w dostawach prądu spowodowanych cyberatakiem na przemysłowe systemy sterowania stosowane przez dostawców energii elektrycznej[2]. Ataki takie mają miejsce również w Stanach Zjednoczonych. Na przykład w marcu 2016 r. hakerzy naruszyli zabezpieczenia sieciowe nienazwanego amerykańskiego przedsiębiorstwa wodociągowego i przez krótki czas przejęli kontrolę nad kilkoma sterownikami PLC odpowiedzialnymi za regulację przepływu toksycznych substancji chemicznych stosowanych do uzdatniania wody[3].

Za dużą część problemu odpowiada kwestia dostępu osób trzecich do systemów SCADA/ICS. Wiele organizacji ma duże zaufanie do zabezpieczeń stosowanych przez swoich dostawców technologii i innych partnerów zewnętrznych, zapewniając im szeroki dostęp do swoich systemów wewnętrznych. Mniej więcej **60%** respondentów wspomnianego badania udzieliło swoim partnerom lub instytucjom rządowym dostępu do tych systemów na **najwyższym lub wysokim poziomie**. Krótko mówiąc, operatorzy systemów SCADA/ICS stoją w obliczu poważnych zagrożeń i muszą pokonać kilka przeszkód na drodze do lepszego zabezpieczenia tych systemów.

Zakres i specjalizacja systemów SCADA/ICS szybko rośnie

Rynki systemów SCADA/ICS dynamicznie się rozwijają. Według firmy analitycznej Transparency Market Research wartość globalnego rynku samych systemów ICS wzrośnie z 58 mld USD w 2014 r. do 81 mld USD w 2021 r., przy rocznym tempie wzrostu na poziomie 4,9% w latach 2015–2021[4]. Systemy ICS są na szeroką skalę stosowane w zakładach produkcyjnych, portach morskich, zakładach uzdatniania wody, przedsiębiorstwach energetycznych. przy obsłudze rurociągów naftowych oraz w systemach sterowania warunkami środowiskowymi w budynkach[5]. Tempo wzrostu wartości rynku systemów SCADA, które służą jako graficzny interfejs użytkownika do systemów ICS, to natomiast 6,6% r/r[6].

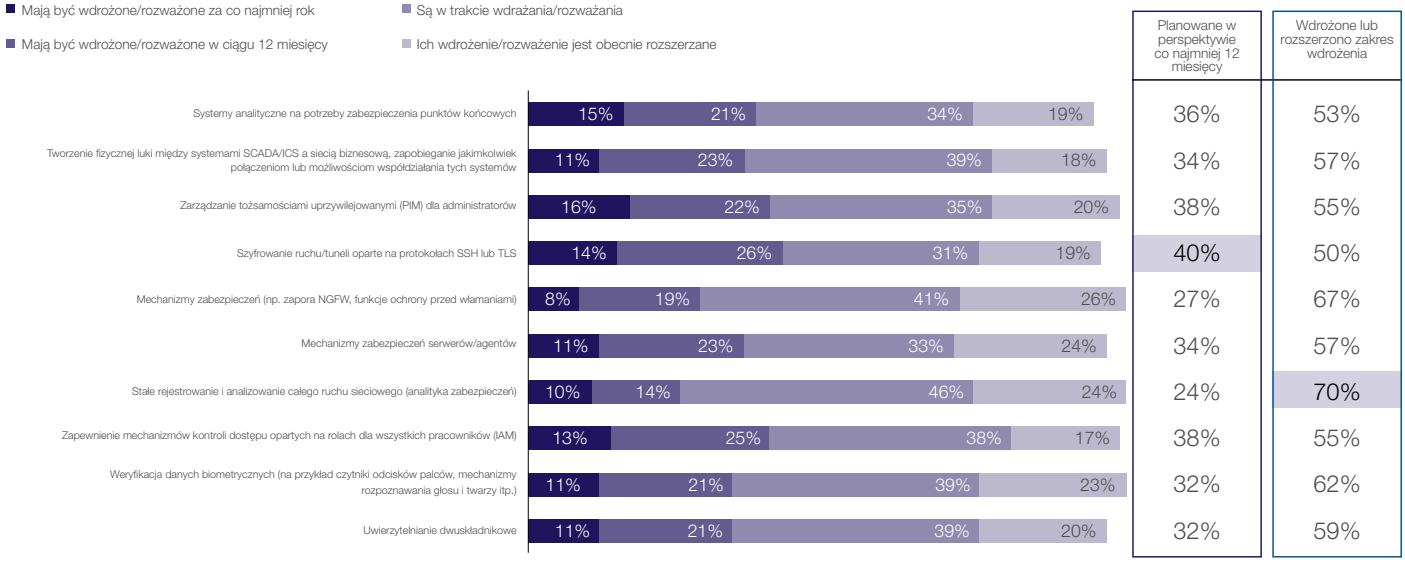
Dobra wiadomość jest taka, że operatorzy systemów SCADA/ICS zdają sobie raczej sprawę z istniejących zagrożeń i chronią swoje systemy za pomocą różnych rozwiązań i zabezpieczeń. Wyniki przeprowadzonych przez firmę Forrester badań wskazują na przykład, że **70%** badanych organizacji **stale rejestruje i analizuje cały swój ruch sieciowy**, z czego 24% rozbudowuje swoje systemy analityczne używane na potrzeby zabezpieczeń. Około **66%** tych organizacji korzysta również z **mechanizmów zabezpieczeń**, a **62%** stosuje **mechanizmy zabezpieczeń oparte na danych biometrycznych** (skanery odcisków palców, technologie rozpoznawania twarzy itp.).

Mimo tych liczb wiele organizacji nie wdrożyło innych technologii bezpieczeństwa, które mogłyby pomóc w ochronie systemów SCADA/ICS. Połowa respondentów nie wdrożyła funkcji szyfrowania ruchu opartych na protokołach SSH lub TLS, chociaż ponad połowa z nich planuje wdrożenie jednej z tych technologii w ciągu roku.

Ponadto **45%** respondentów nie korzysta z funkcji zarządzania tożsamościami uprzywilejowanymi (PIM) dla administratorów, która pozwala na monitorowanie w środowiskach IT kont o wysokim poziomie dostępu. **45%** respondentów nie stosuje natomiast mechanizmów kontroli dostępu opartego na rolach dla pracowników. Tylko niewielki odsetek respondentów twierdzi jednak, że nie planuje wdrożenia tych technologii.

Większość organizacji podejmuje obecnie liczne działania w celu zabezpieczenia posiadanych systemów SCADA/ICS

P1 — Jakie plany ma Państwa organizacja w kontekście wdrożenia lub rozważania następujących środków mających na celu zabezpieczenie posiadanego systemu SCADA/ICS?



Baza. 429 osób odpowiedzialnych za podejmowanie globalnych decyzji dotyczących zabezpieczeń infrastruktury krytycznej, ochrony na poziomie IP, połączeń z Internetem rzeczy lub systemów SCADA
Źródło. Zamówione badanie przeprowadzone przez firmę Forrester Consulting w imieniu firmy Fortinet, styczeń 2018 r.

Rys. 1. Większość operatorów systemów SCADA/ICS na bieżąco rejestruje i analizuje ruch sieciowy, a jedynie nieco ponad połowa z nich wdraża odpowiednie funkcje analityczne na potrzeby zabezpieczenia punktów końcowych.

Wielu operatorów systemów SCADA/ICS ignoruje potrzebę wdrożenia podstawowych zabezpieczeń.

45% nie korzysta z mechanizmów kontroli dostępu opartych na rolach.

W efekcie stwarza to pole do działania hakerom wewnętrznym.

Wyzwania dla bezpieczeństwa systemów SCADA/ICS

Organizacje korzystające z systemów SCADA/ICS wydają się być zaniepokojone nie tylko stosowaniem technologii chmurowych przez dostawców tychże systemów, ale również, i w szczególności, wykorzystywaniem przez pracowników technologii osobistych i chmurowych, które mogą łączyć się z systemami SCADA/ICS.

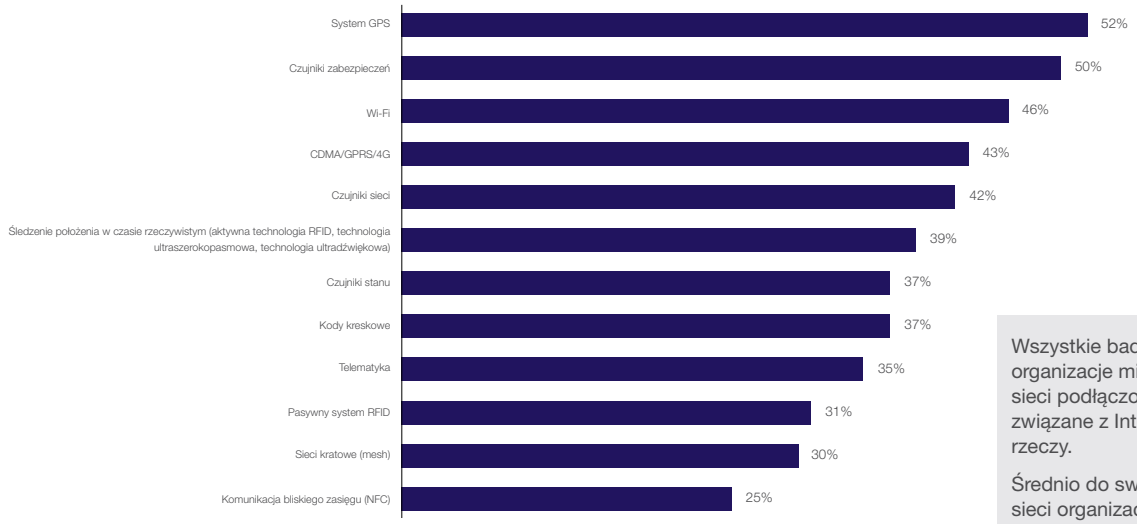
Nawet jeśli organizacje dostrzegają te potencjalne zagrożenia dla bezpieczeństwa, swoimi niektórymi działaniami jeszcze te zagrożenia zwiększają, na przykład zezwalając na **podłączenie do swoich sieci** znacznej liczby urządzeń bezprzewodowych i urządzeń związanych z Internetem rzeczy. Każde przedsiębiorstwo objęte badaniem firmy Forrester zgłosiło, że do jego sieci są podłączone wspomniane urządzenia i mogą one również być podłączone do systemów SCADA/ICS. Zważywszy na fakt, że średnio do takiej sieci podłączonych jest niemal pięć urządzeń związanych z Internetem rzeczy (4,7), zagrożenie jest bardzo poważne.

Równie dużym problemem są sieci Wi-Fi. Ponad **40%** badanych organizacji ma do swoich sieci podłączone urządzenia Wi-Fi, urządzenia przenośne i czujniki sieciowe. Prowadzi to często do powstawania problemów podczas podejmowanych prób integracji systemu IT z systemem OT, czyli sprzętem i oprogramowaniem obsługującym systemy SCADA i ICS. Ponadto prawie **75%** respondentów ma co najmniej podstawowe połączenia między systemami IT i OT, co powinno być powodem do wzmożonej ostrożności, jeśli chodzi o ochronę przed zagrożeniami.

Obawy dotyczące integracji systemów IT i OT mają charakter zróżnicowany. Około **40%** respondentów obawia się, że albo oni, albo ich partnerzy w dziedzinie bezpieczeństwa nie mają wiedzy specjalistycznej potrzebnej do ochrony tych systemów. **39%** respondentów obawia się wycieków danych wrażliwych, a **33%** niepokoi się możliwością złośliwego wykorzystania „tylnych wejść" do urządzeń podłączonych do wspomnianych systemów. Innym potencjalnym problemem dla operatorów systemów SCADA/ICS jest poziom dostępu udzielony partnerom, w tym partnerom technologicznym, który zapewnia hakerom dodatkową ścieżkę ataku.

Technologie Internetu rzeczy połączone z siecią

P13 — Które z następujących technologii Internetu rzeczy są obecnie podłączone do sieci w Państwa organizacji (wybierz wszystkie odpowiedzi mające zastosowanie)?



Baza. 429 osób odpowiedzialnych za podejmowanie globalnych decyzji dotyczących zabezpieczeń infrastruktury krytycznej, ochrony na poziomie IP, połączeń z Internetem rzeczy lub systemów SCADA
Źródło. Zamówione badanie przeprowadzone przez firmę Forrester Consulting w imieniu firmy Fortinet, styczeń 2018 r.

Wszystkie badane organizacje miały do swojej sieci podłączone urządzenia związane z Internetem rzeczy.

Średnio do swoich sieci organizacje mają podłączone po około pięć urządzeń (4,7).

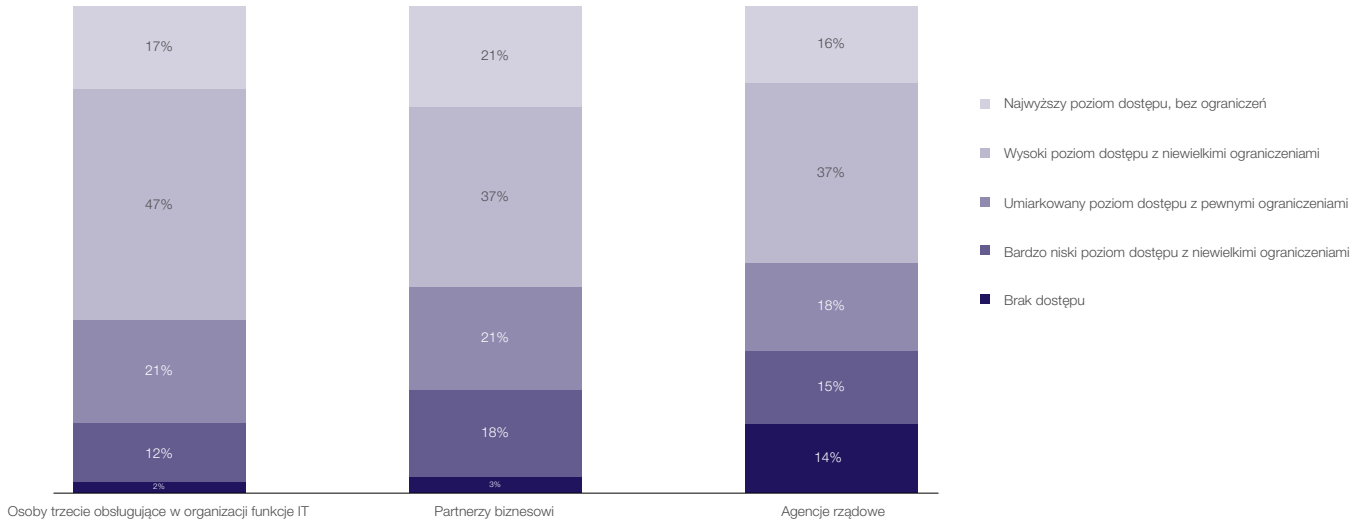
Rys. 2. Większość użytkowników systemów SCADA/ICS ma do swoich sieci podłączonych wiele innych technologii.

Na przykład **64%** respondentów zapewnia zewnętrznym partnerom ds. IT najwyższy lub wysoki poziom dostępu do swoich systemów SCADA/ICS. Problem nie dotyczy jednak tylko tego poziomu relacji: prawie 60% respondentów daje najwyższy lub wysoki poziom dostępu innym partnerom biznesowym, a ponad **50%** daje taki poziom dostępu agencjom rządowym. Jeśli chodzi o przemysł, producenci są najbardziej skłonni do udzielania podmiotom zewnętrznym najwyższych uprawnień dostępu do swoich systemów.

Dodatkowym czynnikiem zwiększającym potencjalne ryzyko jest fakt, że wielu operatorów zleca wykonanie części czynności niezbędnych do zabezpieczenia swoich systemów SCADA/ICS podmiotom zewnętrznym w ramach outsourcingu. Wśród takich najważniejszych czynności zlecanych dostawcom IT można wymienić zabezpieczenie sieci bezprzewodowych, zabezpieczenie połączeń z Internetem rzeczy oraz obsługę funkcji wykrywania włamań i mechanizmów kontroli dostępu do sieci. Sam outsourcing również jest daleki od doskonałości: **56%** respondentów zleca zabezpieczenie swoich systemów SCADA różnym podmiotom zewnętrznym, co czasami prowadzi do stosowania **niespójnych zabezpieczeń, które kiepsko ze sobą współdziałają.**

Większość organizacji przyznaje podmiotom zewnętrznym najwyższy lub wysoki poziom dostępu

P3 — Jaki poziom dostępu do systemów SCADA/ICS zapewnia Państwa organizacja następującym podmiotom?



Baza. 429 osób odpowiedzialnych za podejmowanie globalnych decyzji dotyczących zabezpieczeń infrastruktury krytycznej, ochrony na poziomie IP, połączeń z Internetem rzeczy lub systemów SCADA
Źródło. Zamówione badanie przeprowadzone przez firmę Forrester Consulting w imieniu firmy Fortinet, styczeń 2018 r.

Rys. 3: Wielu operatorów systemów SCADA/ICS daje partnerom technologicznym i innym partnerom biznesowym wysoki poziom dostępu do tych systemów.

Organizacje korzystające z systemów SCADA/ICS powierzają obsługę tych systemów swoim partnerom.

64% daje swoim zewnętrznym dostawcom IT najwyższy lub wysoki poziom dostępu.

Luka w zabezpieczeniach systemu dostawcy IT może być luką Twojej organizacji.

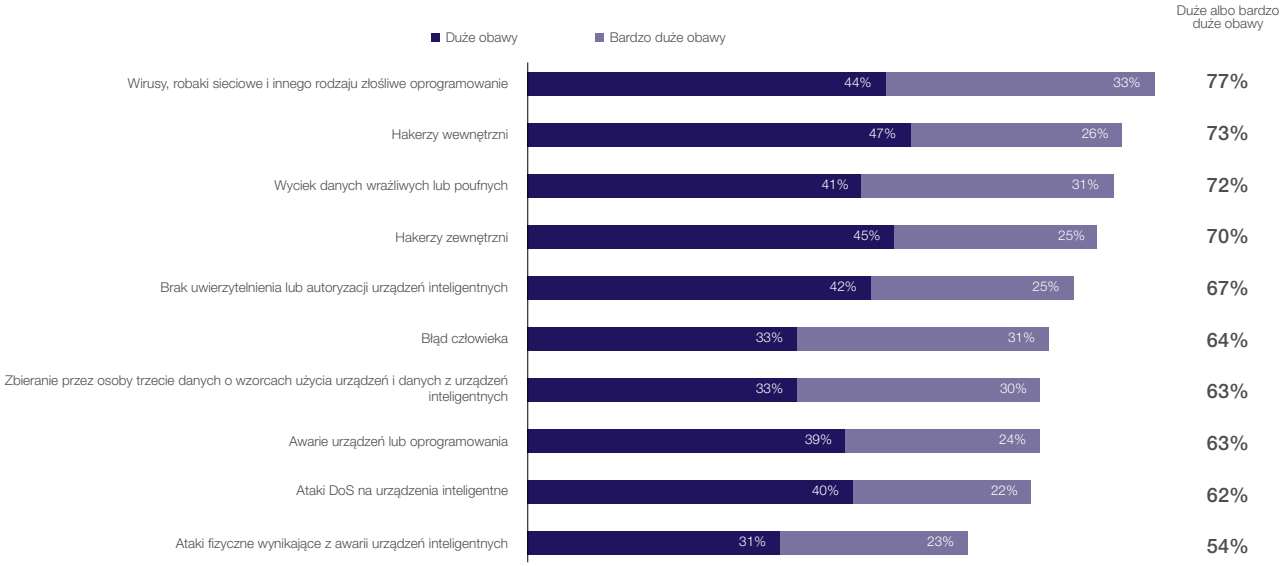
Zagrożenia dla systemów SCADA/ICS

Oprócz pytań dotyczących zasad wewnętrznych, firma Forrester zapytała operatorów systemów SCADA/ICS o najpoważniejsze zagrożenia, z jakimi mieli do czynienia. Operatorzy dostrzegają wiele zagrożeń pochodzących z kilku źródeł, przy czym największe z nich to złośliwe oprogramowanie i wewnętrzne wycieki danych. Ponad **75%** respondentów stwierdziło, że ma duże albo bardzo duże obawy w związku ze złośliwym oprogramowaniem. Ponad **70%** respondentów stwierdziło, że ma duże albo bardzo duże obawy w związku z wyciekiem poufnych danych oraz wewnętrznymi i zewnętrznymi hakerami. Ponad **66%** respondentów było zaniepokojonych brakiem uwierzytelnienia lub autoryzacji urządzeń inteligentnych, a prawie 66% obawia się błędów człowieka oraz zbierania przez osoby trzecie danych, w tym danych o wzorcach korzystania z urządzeń.

Obawy dotyczące złośliwego oprogramowania i wewnętrznych hakerów nasiliły się od czasu przeprowadzenia podobnego badania w 2016 r. Od tego czasu zagrożenia znacznie się zmieniły i w odniesieniu do systemów SCADA/ICS są znacznie poważniejsze, operatorzy tych systemów twierdzą jednak, że w rzeczywistości zagrożenia te są mniejsze. Na przykład błędy człowieka, zbieranie danych przez osoby trzecie i awaria urządzeń lub oprogramowania są dla nich teraz mniej istotne, ale być może dostrzegają zagrożenia dla bezpieczeństwa płynące z innych źródeł.

Obawy dotyczące bezpieczeństwa dotyczą wirusów, hakerów, wycieków danych i braku uwierzytelnienia

P7 — Jak oceniają Państwo swoje obawy dotyczące następujących kwestii w kontekście zabezpieczeń systemów SCADA/ICS.



Baza. 429 osób odpowiedzialnych za podejmowanie globalnych decyzji dotyczących zabezpieczeń infrastruktury krytycznej, ochrony na poziomie IP, połączeń z Internetem rzeczy lub systemów SCADA
Źródło. Zamówione badanie przeprowadzone przez firmę Forrester Consulting w imieniu firmy Fortinet, styczeń 2018 r.

Rys. 4: Operatorzy SCADA/ICS obawiają się złośliwego oprogramowania, hakerów wewnętrznych i kilku innych zagrożeń.

Ponad

70% operatorów systemów OT

w bardzo dużym stopniu obawia się hakerów wewnętrznych, wycieku danych wrażliwych i hakerów zewnętrznych.

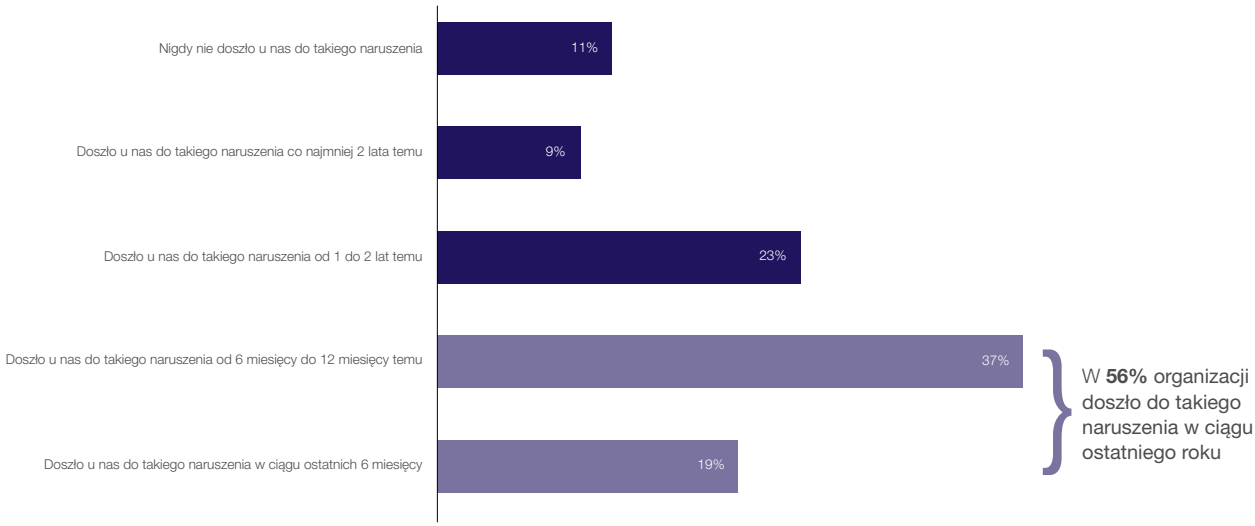
Skutki zagrożeń

Mimo wdrożenia różnych zabezpieczeń w wielu organizacjach, naruszenia bezpieczeństwa systemów SCADA/ICS są powszechne. Na przykład w ubiegłym roku przypadki takie zgłosiło **56%** respondentów, a kolejne **32%** miało z nimi do czynienia wcześniej. Tylko mały odsetek respondentów stwierdził, że bezpieczeństwo ich systemów nigdy nie zostało naruszone.

Naruszenia bezpieczeństwa systemów SCADA/ICS mają poważne skutki. **63%** respondentów twierdzi, że miały one bardzo duży lub krytyczny wpływ na bezpieczeństwo pracowników. **58%** respondentów zgłasza poważne konsekwencje dla stabilności finansowej przedsiębiorstwa, a **63%** widzi w nich poważne przeszkody utrudniające prowadzenie działalności na odpowiednim poziomie.

56% organizacji doświadczyło w ciągu ostatnich 12 miesięcy naruszenia bezpieczeństwa systemów SCADA/ICS

P8 — Czy według Państwa wiedzy doszło w Państwa organizacji do naruszenia bezpieczeństwa systemów SCADA/ICS?



Baza. 429 osób odpowiedzialnych za podejmowanie globalnych decyzji dotyczących zabezpieczeń infrastruktury krytycznej, ochrony na poziomie IP, połączeń z Internetem rzeczy lub systemów SCADA
Źródło. Zamówione badanie przeprowadzone przez firmę Forrester Consulting w imieniu firmy Fortinet, styczeń 2018 r.

Rys. 5. U większości użytkowników systemów SCADA/ICS doszło do naruszenia bezpieczeństwa tych systemów w ostatnim roku.

Naruszenia bezpieczeństwa systemów SCADA/ICS zdarzają się często.

56% operatorów systemów SCADA/ICS zgłosiło, że doszło u nich do takiego naruszenia w ciągu ostatniego roku.

Wspomniane naruszenia narażają na szwank bezpieczeństwo pracowników i finansową stabilność organizacji.

Zalecenia dotyczące sposobów ograniczenia ryzyka

Wiele organizacji dostrzega kilka sposobów zwiększenia bezpieczeństwa systemów SCADA/ICS. Prawie połowa z nich uznaje pełną ocenę ryzyka biznesowego lub operacyjnego za najlepszy sposób na poprawę bezpieczeństwa w kontekście integracji systemów OT i IT. Inne typowe podejścia do ograniczania ryzyka obejmują wprowadzenie wspólnych standardów, zwiększenie centralizacji procesu zarządzania urządzeniami oraz przeprowadzanie konsultacji z organami rządowymi takimi jak Zespół ds. Przeciwdziałania Cyberatakom na Przemysłowe Systemy Sterowania (ICS-CERT).

Na pytanie o wybór dostawcy zabezpieczeń do systemów SCADA/ICS tylko nieco ponad połowa respondentów odpowiedziało, że konsultanci technologiczni przekazują im rzetelne informacje. Jeśli chodzi o zdobyte zaufanie, dostawcy i partnerzy w zakresie systemów SCADA/ICS uzyskują tu wynik nieco wyższy niż **50%**.

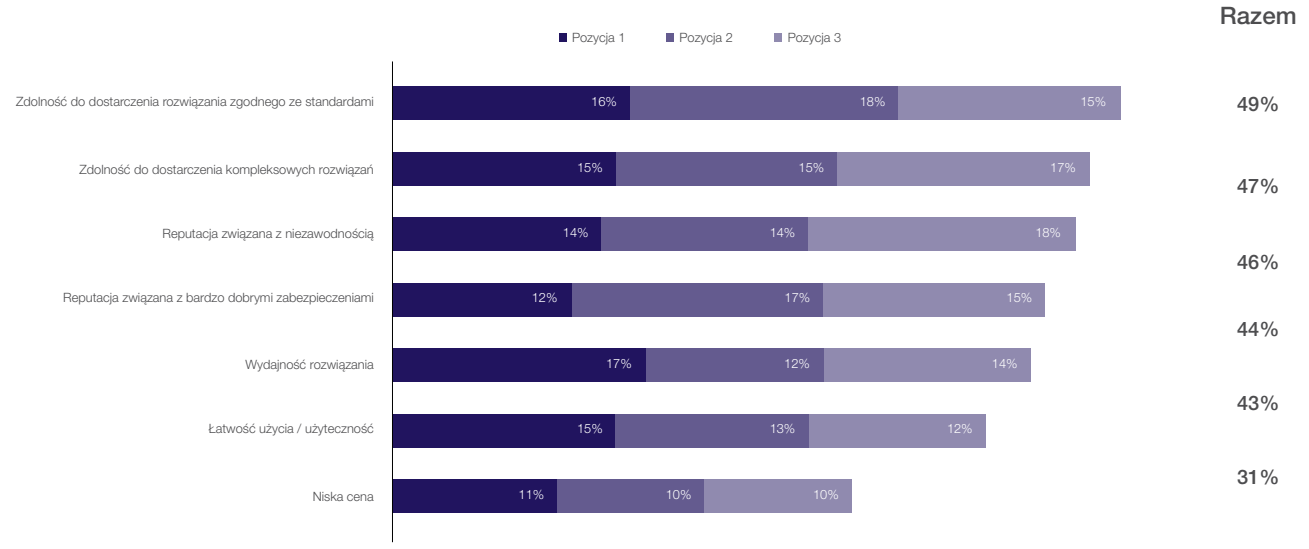
W celu oceny dostawców i technologii zabezpieczeń organizacje powinny rozważyć następujące elementy:

- Wydajność rozwiązania
- Zdolność rozwiązania do zapewnienia zgodności z obowiązującymi normami
- Kompleksowość rozwiązania

Posiadanie reputacji dostawcy niezawodnych i dobrych zabezpieczeń było wysoko oceniane przez respondentów. Kwestią podstawową była również zdolność do zapewnienia zgodności z normami branżowymi i standardami bezpieczeństwa, przy czym niemal połowa respondentów uznała ten element za czynnik decydujący o wyborze rozwiązań w zakresie bezpieczeństwa. Zdolność do dostarczenia kompleksowego rozwiązania zajęła drugie miejsce na liście czynników decydujących o wyborze danego rozwiązania. Co ciekawe, tylko **30%** respondentów za kwestię podstawową uznało cenę rozwiązania.

Zgodność ze standardami, oferta kompleksowych rozwiązań i niezawodność to najważniejsze czynniki brane pod uwagę podczas wyboru dostawcy

P20 — Które z wymienionych poniżej czynników są dla Państwa najważniejsze podczas wyboru dostawcy systemów SCADA/ICS (należy wskazać i zaklasyfikować trzy najważniejsze czynniki)?



Baza. 429 osób odpowiedzialnych za podejmowanie globalnych decyzji dotyczących zabezpieczeń infrastruktury krytycznej, ochrony na poziomie IP, połączeń z Internetem rzeczy lub systemów SCADA
Źródło. Zamówione badanie przeprowadzone przez firmę Forrester Consulting w imieniu firmy Fortinet, styczeń 2018 r.

Rys. 6: Przy wyborze dostawców zabezpieczeń operatorzy systemów SCADA/ICS kierują się kilkoma priorytetami takimi jak zdolność do zapewnienia zgodności ze standardami oraz zdolność do dostarczenia kompleksowych rozwiązań.

Prognozy na przyszłość

Wiele organizacji korzystających z systemów SCADA/ICS planuje w tym roku zwiększyć wydatki na zabezpieczenia tych systemów. Organizacje, które tego nie planują, ryzykują, że pozostaną w tyle. Prawie 75% organizacji planuje zwiększyć wydatki na zabezpieczenie połączeń z Internetem rzeczy, z czego 36% ma zamiar zwiększyć te wydatki o co najmniej 5%. Ponad 70% organizacji planuje wydać więcej na zabezpieczenie systemów OT, a prawie **40%** planuje zwiększyć te wydatki o co najmniej 5%. **70%** organizacji chce w tym roku wydać więcej na infrastrukturę OT, a 37% ma zamiar zwiększyć te wydatki o co najmniej 5%. Plany te wskazują na stałe i zwiększone zaangażowanie na rzecz zabezpieczenia systemów OT oraz przestrzegania norm bezpieczeństwa i wdrożenia mechanizmów kontroli niezbędnych do ochrony tych systemów.

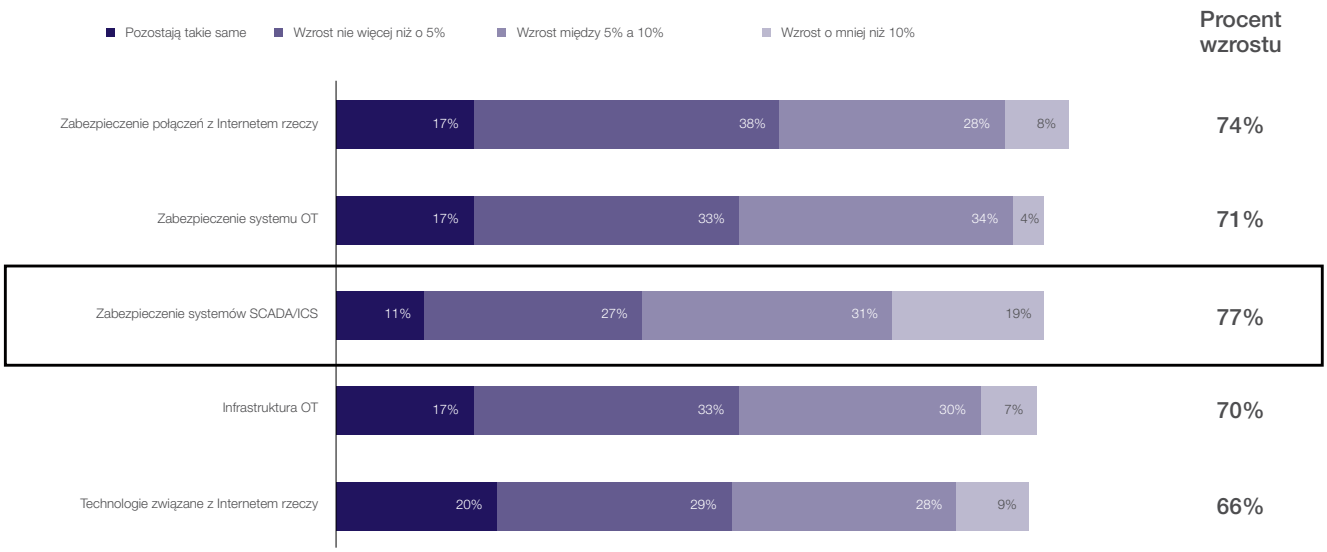
Rozważając potencjalne zakupy zabezpieczeń, operatorzy systemów SCADA/ICS mogą je chronić, podejmując kilka następujących działań:

- Segmentacja sieci w drodze odłączenia od systemów SCADA/ICS wszelkich podłączonych do nich urządzeń bezprzewodowych i urządzeń związanych z Internetem rzeczy
- Zabezpieczenie infrastruktury sieciowej, w tym przełączników, ruterów i sieci bezprzewodowych, za pomocą zapór i innych stosownych zabezpieczeń
- Wdrożenie zasad zarządzania tożsamością i dostępem w celu uniemożliwienia osobom z zewnątrz dostępu do sieci oraz uniemożliwienia pracownikom dostępu do tych części sieci, do których dostępu mieć nie muszą
- Korzystanie z zapory aplikacji WWW (WAF) w celu skanowania i zabezpieczania niechronionych aplikacji WWW
- Wdrożenie zabezpieczeń punktów końcowych w celu zapewnienia przydatnych informacji o zagrożeniach oraz widoczności tych zagrożeń w czasie rzeczywistym

Z uwagi na możliwość narażenia na szwank bezpieczeństwa fizycznego pracowników lub klientów, podejście do zabezpieczenia systemów SCADA/ICS musi się różnić od podejścia do zabezpieczenia systemów IT. Dobra wiadomość jest taka, że przyjmując wielowarstwowe podejście do zabezpieczenia systemów SCADA/ICS, organizacje mogą znacznie poprawić swoje bezpieczeństwo i tym samym zmniejszyć zagrażające im ryzyko.

Wydatki na zabezpieczenie systemów SCADA/ICS rosną szybciej niż wydatki w innych obszarach

P20 — Które z wymienionych poniżej czynników są dla Państwa najważniejsze podczas wyboru dostawcy systemów SCADA/ICS (należy wskazać i zaklasyfikować trzy najważniejsze czynniki)?



Baza. 429 osób odpowiedzialnych za podejmowanie globalnych decyzji dotyczących zabezpieczeń infrastruktury krytycznej, ochrony na poziomie IP, połączeń z Internetem rzeczy lub systemów SCADA
Źródło. Zamówione badanie przeprowadzone przez firmę Forrester Consulting w imieniu firmy Fortinet, styczeń 2018 r.

Rys. 7. Wielu operatorów systemów SCADA/ICS planuje zwiększenie w 2018 r. wydatków na zabezpieczenia w kilku obszarach.

Źródła

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

[2] Kim Zetter, „Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", WIRED, 3 marca 2016 r.

[3] John Leyden, „Water treatment plant hacked, chemical mix changed for tap supplies", The Register, 24 marca 2016 r.

[4] „Global Industrial Controls System Market to Grow at CAGR of 4.9% from 2015 to 2021", Transparency Market Research, wrzesień 2015 r.

[5] Mark Fabro, „Industrial Control Systems Cyber Security", Presentation to U.S. Department of Defense, 7 czerwca 2017 r.

[6] „SCADA Market Worth 13.43 Billion USD by 2022", MarketsandMarkets, dostęp z dnia 12 kwietnia 2019 r.

www.fortinet.com

373566-A-1-PL

sierpnia 2, 2019 2:50 PM

report-operational-technology-forrester_A4_PL