RAPORT

Raport o stanie technologii operacyjnej i cyberbezpieczeństwa

Spis treści

Streszczenie

Technologia operacyjna (OT) ma kluczowe znaczenie dla bezpieczeństwa publicznego i dobrobytu gospodarczego, ponieważ kontroluje urządzenia stosowane przez zakłady przemysłowe, przedsiębiorstwa energetyczne, przedsiębiorstwa wodociągowe, linie żeglugowe itp.

Rozwój systemów OT rozpoczął się na początku XX wieku, kiedy to maszyny i urządzenia sterujące zasilane parą i siłą mięśni zostały zastąpione przez maszyny i urządzenia sterujące zasilane energią elektryczną. Technologie operacyjne pojawiły się na wiele dziesięcioleci przed technologiami informatycznymi (IT), a potem przez długi czas były od nich oddzielone. Ostatnio jednak niektóre technologie IT, takie jak czujniki, funkcje uczenia maszynowego (ML) i funkcje Big Data, są integrowane z sieciami OT w celu uzyskania nowych korzyści i zdobycia przewagi konkurencyjnej. Integracja taka zwiększa jednak cyfrową powierzchnię ataku i ryzyko włamań.

W celu zbadania stanu cyberbezpieczeństwa w środowiskach OT firma Fortinet przeprowadziła badania ankietowe wśród dyrektorów operacyjnych i kierowników produkcji w dużych przedsiębiorstwach produkcyjnych i energetycznych, przedsiębiorstwach użyteczności publicznej, placówkach opieki zdrowotnej i firmach transportowych. Wyniki tych ankiet wskazują na to, że:

1. **Skutki cyberataków na środowisko OT są szeroko zakrojone i sięgają głęboko.** Około 74% operatorów systemów OT doświadczyło w ciągu ostatnich 12 miesięcy włamań za pomocą złośliwego oprogramowania, które negatywnie odbiły się na produktywności, przychodach, zaufaniu do marki, własności intelektualnej i bezpieczeństwie fizycznym.

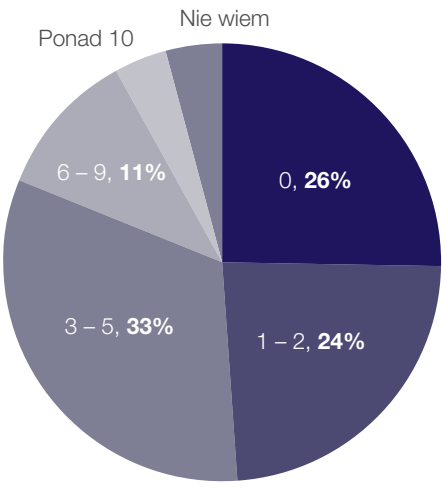
2. **Brak cyberzabezpieczeń przyczynia się do zwiększenia ryzyka.** 78% operatorów ma tylko częściowo scentralizowaną widoczność cyberzabezpieczeń swojego środowiska OT. W 65% organizacji brakuje mechanizmów kontroli dostępu opartych na rolach, a ponad połowa organizacji nie korzysta z uwierzytelniania wieloskładnikowego ani nie segmentuje sieci wewnętrznej.

3. **Potrzeba poprawy zabezpieczeń systemu OT jest ograniczona koniecznością nadążania za szybkimi zmianami i brakiem odpowiednio wykwalifikowanych pracowników.** 64% osób odpowiedzialnych za technologie operacyjne twierdzi, że poznawanie takich zmian jest ich największym wyzwaniem, a prawie połowa (45%) uznała, że jest ograniczona brakiem wykwalifikowanej siły roboczej.

4. **Obecnie w organizacjach korzystających z systemów OT rośnie nacisk na cyberbezpieczeństwo.** 70% takich organizacji planuje powierzenie w przyszłym roku nadzoru nad kwestiami cyberbezpieczeństwa menedżerom ds. zabezpieczeń infrastruktury informatycznej (CISO) (obecnie jedynie 9% takich menedżerów nadzoruje te kwestie), a 62% organizacji zwiększyło nakłady na cyberbezpieczeństwo.

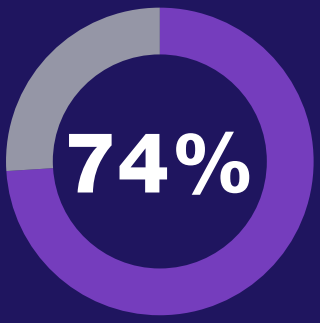
W raporcie tym dokonano przeglądu wyników wspomnianego badania, w tym:

- Określono wyzwania, które dyrektorzy operacyjni dostrzegają w kontekście zabezpieczenia posiadanych środowisk OT
- Przedstawiono typy i skutki włamań
- Przedstawiono sposoby zarządzania cyberbezpieczeństwem
- Zaprezentowano typy luk w zabezpieczeniach
- Przedstawiono kryteria sukcesu

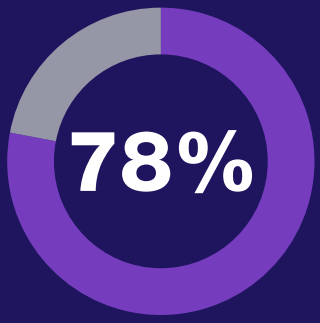


Rys. 1. Liczba włamań w ciągu ostatnich 12 miesięcy

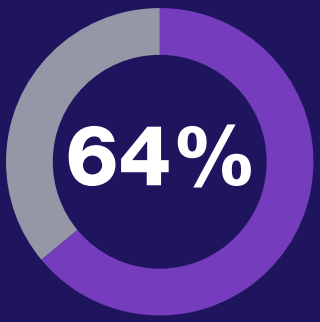
Infografika — najważniejsze wnioski dotyczące cyberbezpieczeństwa systemów OT



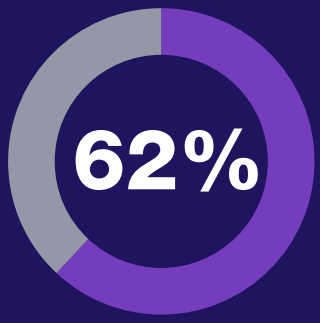
badanych operatorów systemów OT w ciągu ostatnich 12 miesięcy odnotowało do nich włamania skutkujące utratą danych, zakłóceniami lub przerwami w działalności operacyjnej lub narażeniem na szwank reputacji marki.



ma ograniczoną scentralizowaną widoczność cyberzabezpieczeń.



ma problemy z nadążeniem za zmianami.



zwiększa swoje nakłady na cyberbezpieczeństwo.

Naruszenia bezpieczeństwa negatywnie wpłynęły na:

- Produktywność (43%)
- Przychody (36%)
- Reputację marki (30%)
- Dane krytyczne dla działalności (28%)
- Bezpieczeństwo fizyczne (23%)

70% planuje **powierzenie nadzoru nad kwestiami cyberbezpieczeństwa menedżerom ds. zabezpieczeń infrastruktury informatycznej** w przyszłym roku.

Obecnie jednak jedynie 9% takich menedżerów nadzoruje te kwestie.

W porównaniu z najsłabiej zabezpieczonymi organizacjami korzystającymi z systemów OT (ponad sześć włamań w ciągu 12 miesięcy) najlepiej zabezpieczone organizacje (0 włamań w ciągu 12 miesięcy) cechują się następującymi elementami:

100% z nich potencjalnie stosuje uwierzytelnianie wieloskładnikowe

94% z nich potencjalnie stosuje mechanizmy kontroli dostępu oparte na rolach

68% z nich potencjalnie monitoruje i analizuje zdarzenia dotyczące bezpieczeństwa i zarządza nimi

51% z nich potencjalnie stosuje segmentację sieci

46% z nich potencjalnie planuje przeglądy zgodności zabezpieczeń ze standardami

Metodyka badania

Raport o stanie technologii operacyjnej i cyberbezpieczeństwa jest oparty na przeprowadzonej w styczniu 2019 r. ankiecie wśród osób, które:

- Są zatrudnione w przedsiębiorstwach mających ponad 2500 pracowników w sektorach produkcji przemysłowej, energetyki i użyteczności publicznej, opieki zdrowotnej i transportu
- Odpowiadają przede wszystkim za systemy OT
- Odpowiadają za działalność operacyjną
- Uczestniczą w podejmowaniu decyzji o zakupach cyberzabezpieczeń

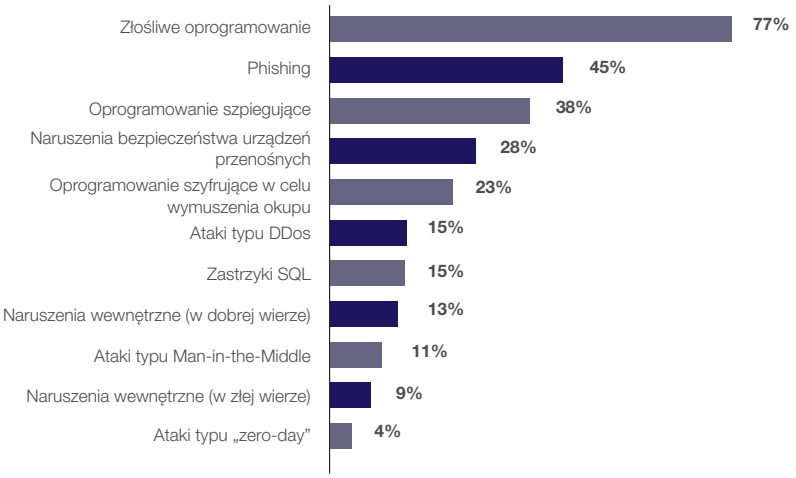
Obserwacje dotyczące cyberbezpieczeństwa systemów OT

Obserwacja — skutki cyberataków na systemy OT są szeroko zakrojone i sięgają głęboko

74% organizacji korzystających z systemów OT doświadczyło w ciągu ostatniego roku co najmniej jednego włamania za pomocą złośliwego oprogramowania, a 50% z nich odnotowała w tym okresie od 3 do ponad 10 włamań.

Jak to pokazano na rys. 2, złośliwe oprogramowanie to główna metoda stosowana we włamaniach. W dalszej kolejności wykorzystuje się w tym celu phishing (45%), oprogramowanie szpiegujące (38%) i naruszenia bezpieczeństwa urządzeń przenośnych (28%).

Skutki takich naruszeń są dla organizacji korzystających z systemów OT bardzo poważne (zob. rys. 3).

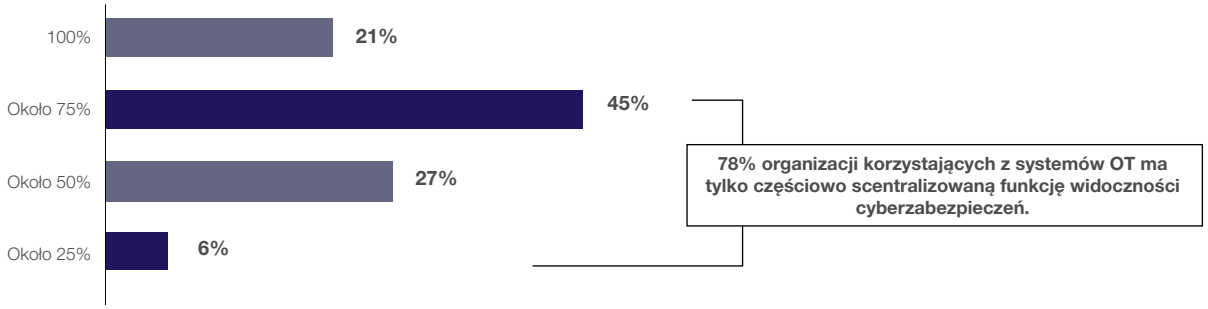


Rys. 2. Rodzaj odnotowanego włamania do systemu OT

Rys. 3. Skutki naruszeń bezpieczeństwa w organizacjach korzystających z systemów OT

Obserwacja — brak widoczności cyberzabezpieczeń zwiększa zagrożenie

78% organizacji ma tylko częściowo scentralizowaną funkcję widoczności cyberzabezpieczeń w kontekście systemów OT (zob. rys. 4).



Rys. 4. Odsetek działań z zakresu cyberbezpieczeństwa systemów OT widocznych centralnie

Obserwacja — niedobór wykwalifikowanych pracowników to główny czynnik hamujący wdrażanie cyberzabezpieczeń

64% dyrektorów operacyjnych uważa, że nadążanie za zmianami jest ich największym problemem tuż przed innymi problemami takimi jak:

- Stosunki ze związkami zawodowymi (45%)
- Niedobór wykwalifikowanych pracowników (45%)
- Zmiany przepisów (44%)
- Dostępność i dostęp do szkoleń (42%)
- Ograniczenia budżetowe (42%)

Brak wykwalifikowanych pracowników jest również przyczyną największych obaw dyrektorów operacyjnych w kontekście wdrażania nowych cyberzabezpieczeń:

- Zwiększenie złożoności (53%)
- Problemy z wdrożeniem standardów bezpieczeństwa (45%)
- Problemy ze znalezieniem dodatkowych pracowników operacyjnych (45%)
- Pogorszenie elastyczności operacyjnej (44%)

Według dodatkowych danych organizacje korzystające z systemów OT, mimo braku zasobów kadrowych, starają się poprawić swoje bezpieczeństwo. Na rys. 5 przedstawiono główne czynniki wymieniane przez dyrektorów operacyjnych zapytanych o motywacje do zwiększenia cyberbezpieczeństwa.

Rys. 5. Podstawowe motywacje do zwiększenia cyberbezpieczeństwa

Pytanie związane z rys. 5 brzmiało: „Jakie są trzy najważniejsze motywacje, dla których chcą Państwo rozszerzyć lub zmienić swoje cyberzabezpieczenia"? Im częściej dana motywacja pojawiała się w odpowiedziach, tym większą czcionką została zapisana powyżej.

Najczęstszymi motywacjami wymienianymi przez dyrektorów operacyjnych (pokazanymi na rys. 5) było uzyskanie zdolności do krzyżowania planów hakerom, zabezpieczenie rosnącej powierzchni ataku wynikającej z transformacji cyfrowej, utrzymanie bezpieczeństwa danych oraz zapewnienie bezpiecznego, wydajnego, efektywnego kosztowo i kompletnego środowiska w obliczu istniejących problemów związanych z niedoborem wykwalifikowanych pracowników.

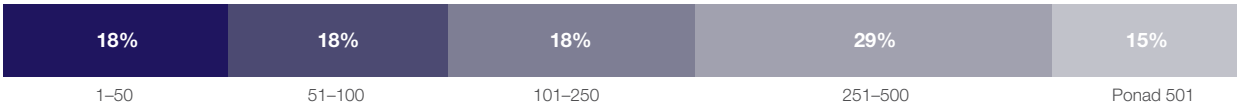
Obserwacja — w organizacjach korzystających z systemów OT kwestia cyberbezpieczeństwa jest coraz ważniejsza

70% badanych organizacji planuje powierzenie w przyszłym roku nadzoru nad kwestiami cyberbezpieczeństwa menedżerom ds. zabezpieczeń infrastruktury informatycznej. Obecnie jednak jedynie 9% takich menedżerów nadzoruje te kwestie. Za cyberbezpieczeństwo w 50% badanych organizacji odpowiada teraz dyrektor ds. OT lub kierownik ds. cyberbezpieczeństwa, a w 24% organizacji rolę taką przypisuje się dyrektorowi ds. inżynierii sieciowej i działalności operacyjnej.

Podniesienie priorytetu dla kwestii cyberbezpieczeństwa jest widoczne nie tylko w zmianie przypisania obowiązków. **62% organizacji twierdzi, że ponoszone przez nie nakłady na cyberbezpieczeństwo** w tym roku istotnie wzrosną, a 38% organizacji planuje utrzymać te nakłady na dotychczasowym poziomie. Organizacje korzystające z systemów OT przywiązują bardzo dużą wagę do pojawiających się zagrożeń: 94% organizacji wskazało, że ich menedżerowie ds. zabezpieczeń infrastruktury informatycznej wymieniają stan zabezpieczeń systemów OT jako istotny lub umiarkowanie istotny element szerszej oceny ryzyka prezentowanej na spotkaniach ścisłego kierownictwa lub rady dyrektorów.

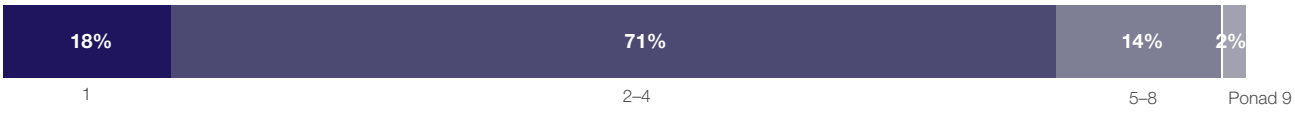
Obserwacja — wymagające ochrony środowiska OT są złożone

Zabezpieczane przez respondentów środowiska OT mają złożony charakter, składają się bowiem z dużej liczby urządzeń OT (od jednego do nawet powyżej pięciuset) (zob. rys. 6).



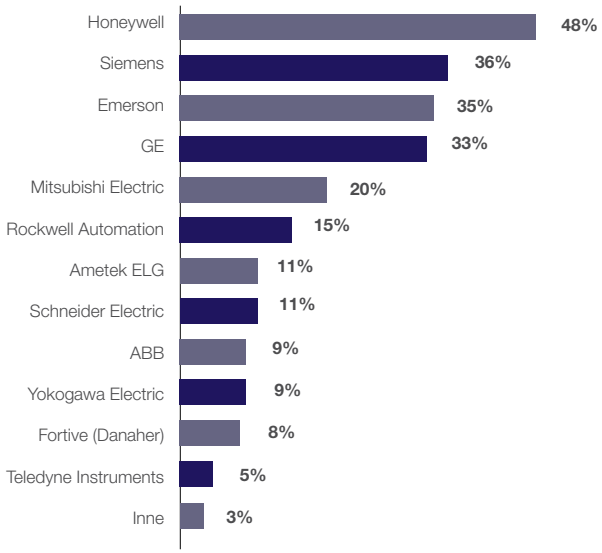
Rys. 6. Liczba działających urządzeń OT

Większość organizacji nabywa swoje urządzenia od 2–4 dostawców (zob. rys. 7).



Rys. 7. Liczba dostawców urządzeń OT dla danej organizacji

Najpopularniejszymi dostawcami urządzeń OT wymienionymi w ramach tego badania były firmy Honeywell, Siemens i Emerson (zob. rys. 8).



Rys. 8. Najpopularniejsi dostawcy urządzeń OT

Obserwacja — dyrektorzy operacyjni mają wpływ na poprawę cyberbezpieczeństwa

Dyrektorzy operacyjni aktywnie uczestniczą w wyborze rozwiązań mających na celu poprawę bezpieczeństwa systemów OT. 76% dyrektorów operacyjnych twierdzi, że ich opinie są regularnie uwzględniane w decyzjach dotyczących cyberbezpieczeństwa, a 45% z nich ma ostateczne zdanie w tych kwestiach. Prawie wszyscy są regularnie (56%) lub sporadycznie (39%) angażowani w rozwój strategii cyberbezpieczeństwa systemów IT swoich organizacji.

Warto zauważyć, że zapewnienie bezpiecznego i stabilnego środowiska jest niezbędne do spełnienia trzech najważniejszych kryteriów sukcesu, na podstawie których dyrektorzy operacyjni są oceniani: maksymalizacja produktywności (55%), minimalizacja kosztów (53%) i skrócenie czasu reakcji na pojawienie się luki w zabezpieczeniach (44%).

Zaskakujące może być to, że kryterium „skrócenia czasu reakcji na pojawienie się luki w zabezpieczeniach" jest trzecim najważniejszym kryterium sukcesu, ale warto też pamiętać, że skuteczny cyberatak może bardzo szybko zakłócić funkcjonowanie zakładu produkcyjnego, przedsiębiorstwa użyteczności publicznej lub kolei i tym samym bardzo negatywnie odbić się na produktywności, przychodach i bezpieczeństwie. Zapewnienie stabilnego i odpornego środowiska ma również kluczowe znaczenie dla wykonywania trzech najważniejszych bezpośrednich obowiązków dyrektorów operacyjnych: zarządzania wydajnością produkcji (77%), nadzorem nad działem operacyjnym (77%) oraz zarządzaniem procesami produkcji i zapewnienia jakości (76%).

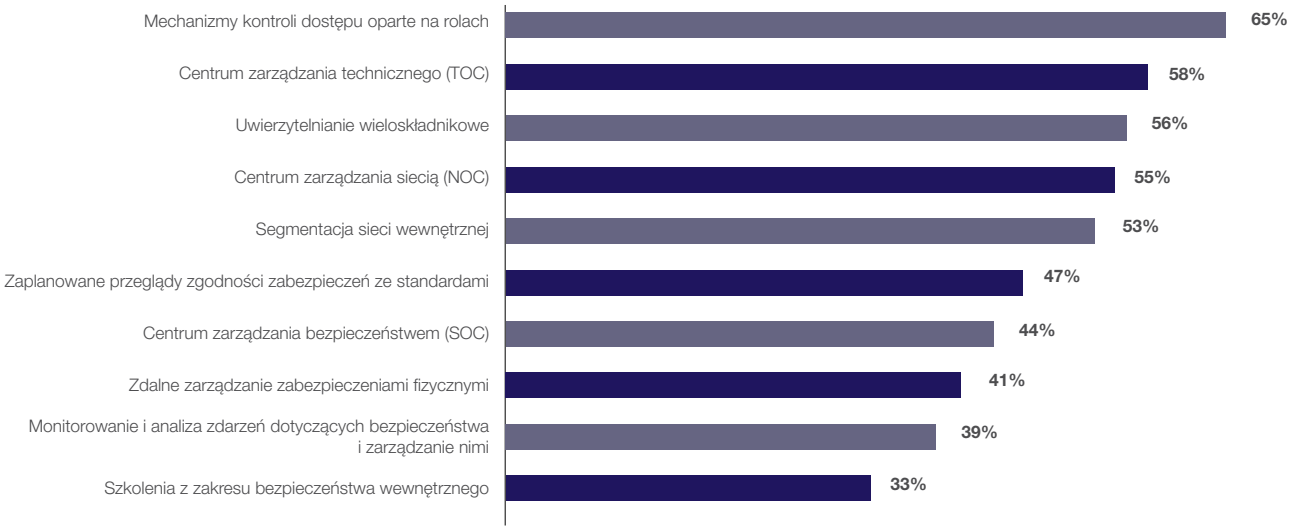
> ***„Zagrożenie cyberatakami nas przytłacza, dlatego inwestujemy w środki zapobiegawcze".***
>
> – dyrektor operacyjny w zakładzie produkcyjnym

Zważywszy na znaczenie zapewnienia wspomnianej stabilności i odporności, nie dziwi fakt, że 76% dyrektorów operacyjnych aktywnie uczestniczy w podejmowaniu decyzji dotyczących cyberbezpieczeństwa systemów OT. Działanie to będzie zajmować coraz więcej czasu, ponieważ przewiduje się, że wydatki na cyberbezpieczeństwo wzrosną z 12,22 mld USD w 2017 r. do 18,05 mld USD w 2023 r.[1].

Istnieje szereg niedoskonałości w zakresie cyberbezpieczeństwa, którymi zespoły OT muszą się zająć, co zaprezentowano w następnej sekcji.

Obserwacja — luki w zabezpieczeniach systemów OT dotyczą mechanizmów kontroli dostępu, uwierzytelniania, segmentacji itp.

Na rys. 9 przedstawiono odsetek respondentów, którzy nie mają wdrożonych podstawowych funkcji z zakresu cyberbezpieczeństwa.



Rys. 9. Odsetek organizacji korzystających z systemów OT, które nie mają wdrożonych podstawowych zabezpieczeń i cyberzabezpieczeń

Brak funkcji określonych na rys. 9 jest przyczyną powstawania luk w zabezpieczeniach:

- **65%** zbadanych organizacji korzystających z systemów OT nie ma mechanizmów kontroli dostępu opartej na rolach, co daje atakującym większą swobodę poruszania się w środowiskach OT.
- **56%** organizacji korzystających z systemów OT nie stosuje uwierzytelniania wieloskładnikowego. Z ostatniego raportu firmy Verizon wynika, że 81% naruszeń miało swój początek w zagubieniu lub kradzieży danych uwierzytelniających[2]. Wiele naruszeń bezpieczeństwa środowisk OT jest poprzedzonych ukierunkowanymi działaniami phishingowymi mającymi na celu uzyskanie danych uwierzytelniających. (*The Wall Street Journal* szacuje, że w ciągu ostatnich dwóch lat naruszono bezpieczeństwo w ponad dwudziestu amerykańskich przedsiębiorstwach z branży energetycznej. Dokonano tego za pomocą danych uwierzytelniających skradzionych dzięki ukierunkowanemu phishingowi, a atakujący pozostawili w tamtejszych systemach OT złośliwe oprogramowanie do wykorzystania na potrzeby ewentualnego sabotażu w przyszłości[3]). Uwierzytelnienie wieloskładnikowe utrudnia skuteczne wykorzystanie skradzionych danych uwierzytelniających.
- **53%** organizacji nie korzysta z segmentacji sieci wewnętrznej. Według wytycznych Narodowego Instytutu Standaryzacji i Technologii (NIST) w zakresie cyberbezpieczeństwa segmentacja taka jest „jednym z najbardziej skutecznych rozwiązań w zakresie architektury systemowej, które organizacja może wdrożyć" w celu ochrony swojego środowiska OT[4]. Eksperci branżowi wskazują, że wiele niedawnych ataków na systemy OT przeprowadzonych za pomocą złośliwego oprogramowania mogło zostać udaremnionych, gdyby taką segmentację wdrożono, ponieważ ogranicza ona swobodę przemieszczania się zagrożeń między sieciami produkcyjnymi OT, a nawet w ramach tych sieci[5].
- **44%** organizacji nie ma centrum zarządzania bezpieczeństwem (SOC), a 55% nie ma centrum zarządzania siecią (NOC), co prowadzi do ograniczenia widoczności zagrożeń i zwiększenia ryzyka skutecznego ataku. Centrum SOC może szybciej wykryć i udaremnić naruszenie i zminimalizować jego skutki. Centrum NOC maksymalizuje natomiast przepustowość i dostępność sieci. Oba te centra mogą być również ze sobą zintegrowane w celu zwiększenia ich wydajności[6].
- **39%** organizacji nie monitoruje i nie analizuje zdarzeń dotyczących bezpieczeństwa ani nimi nie zarządza, co utrudnia wykrycie potencjalnych naruszeń. W sytuacji, gdy większość organizacji zdaje sobie sprawę z nieuchronności skutecznego ataku, uzyskanie cyberodporności, czyli zdolności do reagowania na incydenty i zarządzania zdarzeniami, ma kluczowe znaczenie dla zminimalizowania skutków naruszenia bezpieczeństwa[7].
- Wdrożenie podstawowych funkcji z zakresu bezpieczeństwa jest nadal wyzwaniem dla znacznej liczby organizacji, z których **33%** przyznaje, że nie prowadzi żadnych szkoleń z zakresu bezpieczeństwa wewnętrznego. Mając na uwadze fakt, że 30% wszystkich naruszeń miało charakter wewnętrzny, przeprowadzanie takich szkoleń jest koniecznością zarówno dla działu IT, jak i OT.[8]

Najlepsze praktyki w zakresie zabezpieczenia systemów OT stosowane przez najlepiej zabezpieczone organizacje

26% respondentów („najlepiej zabezpieczone organizacje") zgłosiło **zero włamań** w ciągu ostatnich 12 miesięcy. Z drugiej strony 17% respondentów („najsłabiej zabezpieczone organizacje") odnotowało **co najmniej sześć włamań** w ciągu ostatnich 12 miesięcy, a niektóre nie potrafiły nawet określić liczby takich włamań. Warto przyjrzeć się różnicom między tymi dwiema grupami. Przedstawiono je poniżej:

1. **Najlepiej zabezpieczone organizacje są ze 100% prawdopodobieństwem bardziej skłonne niż najsłabiej zabezpieczone organizacje do stosowania uwierzytelnienia wieloskładnikowego,** co utrudnia dostęp za pomocą skradzionych danych uwierzytelniających.

2. **Najlepiej zabezpieczone organizacje są z 94% prawdopodobieństwem bardziej skłonne niż najsłabiej zabezpieczone organizacje do stosowania mechanizmów kontroli dostępu opartej na rolach,** co ogranicza swobodę poruszania się atakującego.

3. **Najlepiej zabezpieczone organizacje są z 68% prawdopodobieństwem bardziej skłonne niż najsłabiej zabezpieczone organizacje do monitorowania i analizy zdarzeń dotyczących bezpieczeństwa i zarządzania nimi,** co zmniejsza ryzyko płynące z naruszeń bezpieczeństwa dzięki ich szybkiemu wykryciu.

4. **Najlepiej zabezpieczone organizacje są z 51% prawdopodobieństwem bardziej skłonne niż najsłabiej zabezpieczone organizacje do stosowania segmentacji sieci** w celu ograniczenia swobody poruszania się atakującego.

5. **Najlepiej zabezpieczone organizacje są z 46% prawdopodobieństwem bardziej skłonne niż najsłabiej zabezpieczone organizacje do planowania przeglądów zgodności zabezpieczeń ze standardami** w celu poprawy bezpieczeństwa.

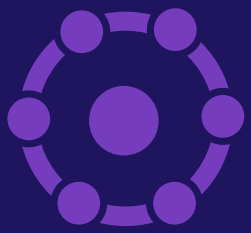
Podsumowanie — cyberbezpieczeństwo jest coraz istotniejszym czynnikiem dobrego działania systemu OT

W środowiskach OT ryzyko naruszenia bezpieczeństwa jest wysokie. Niemal 80% zbadanych organizacji doświadczyło takich naruszeń w ciągu ostatniego roku, a połowa z nich odnotowała w tym okresie co najmniej trzy takie zdarzenia. Skutki tych naruszeń negatywnie wpłynęły na produktywność, przychody, zaufanie do marki, własność intelektualną i bezpieczeństwo fizyczne. W ramach tego badania określono mechanizmy, które należy wdrożyć w celu ograniczenia ryzyka, takie jak scentralizowana funkcja widoczności cyberzabezpieczeń (nie ma jej 78% organizacji), uwierzytelnianie wieloskładnikowe (nie wdrożyło go 56% organizacji) i segmentacja sieci wewnętrznej (nie stosuje jej 53% organizacji), która jest bardzo zalecaną praktyką służącą zabezpieczeniu systemów OT[9].

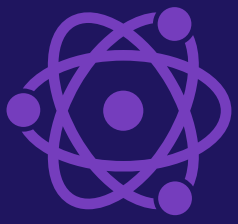
Dyrektorzy operacyjni nadzorujący systemy OT twierdzą, że aktywnie oceniają rozwiązania w zakresie cyberbezpieczeństwa i mają wpływ na decyzje o ich ewentualnym zakupie. Poszukują zatem rozwiązań, które umożliwią im realizację podstawowych obowiązków na tym stanowisku, czyli maksymalizację produktywności przy jednoczesnej minimalizacji kosztów.

Aby wyeliminować problemy związane z brakiem scentralizowanej widoczności i niedoborem wykwalifikowanego personelu, organizacje korzystające z systemów OT powinny uwzględnić następujące zalecenia:

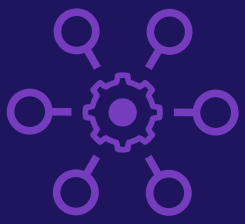
> ***„Rozwiązania w zakresie bezpieczeństwa muszą być inteligentniejsze i skuteczniejsze, nawet w obliczu zmniejszonych budżetów”.***
>
> – dyrektor działu produkcji w dużym przedsiębiorstwie produkcyjnym



Należy szukać rozwiązań w zakresie bezpieczeństwa, które ze sobą współdziałają w celu zapewnienia szerokiej widoczności całej cyfrowej powierzchni ataku obejmującej środowiska OT i IT.



Należy szukać strukturalnego podejścia do zabezpieczeń (ang. security fabric-based), które zapewnia zintegrowaną ochronę wszystkich urządzeń, sieci i aplikacji.



Należy szukać zautomatyzowanych funkcji bezpieczeństwa i rozwiązań, które skoordynują reakcję na zagrożenie i korzystają m.in. z technologii uczenia maszynowego.

Należy minimalizować ryzyko w drodze stosowania najlepszych praktyk w zakresie cyberbezpieczeństwa systemów OT takich jak segmentacja sieci, uwierzytelnianie wieloskładnikowe i mechanizmy kontroli dostępu oparte na rolach.

Takie podejście do cyberbezpieczeństwa poprawi bezpieczeństwo organizacji i jednocześnie pomoże zrekompensować niedobór wykwalifikowanych pracowników.

Źródła

[1] „Industrial Control Systems (ICS) Security Market worth $18.05 billion by 2023", MarketsandMarkets, dostęp z dnia 25 lutego 2018 r.

[2] „2017 Data Breach Investigations Report", Verizon, dostęp z dnia 30 listopada 2018 r.

[3] Rebecca Smith and Rob Barry, „America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It", The Wall Street Journal, 10 stycznia 2019 r.

[4] Keith Stouffer, et al., „Guide to Industrial Control Systems (ICS) Security", NIST, maj 2015 r.

[5] Peter Newton, „Securing IIoT requires extra care. NAC and segmentation can help", TechTarget, 28 września 2018 r.

[6] „Bridging the NOC-SOC Divide", Fortinet, dostęp z dnia 5 marca 2019 r.

[7] Patrick Spencer, „Cyber Resilience Rises to the Forefront in 2019, According to New Scalar Security Study", Scalar Security Blog, 20 lutego 2019 r.

[8] „2018 Data Breach Investigations Report", Verizon, marzec 2018 r.

[9] Keith Stouffer, et al., „Guide to Industrial Control Systems (ICS) Security", NIST, maj 2015 r.

www.fortinet.com

330327-0-1-PL

czerwca 26, 2019 2:49 PM

D:\ARGOS\2019\06_2019\Assignment A-344888-940697\Work\PAKIET\OT\General\Manufacturing-Plant Operations\Report-state-of-operational-technology-A4_PL\report-state-of-operational-technology-A4_PL