RAPORT

Raport o stanie technologii operacyjnej i cyberbezpieczeństwa za rok 2023

FORTINET

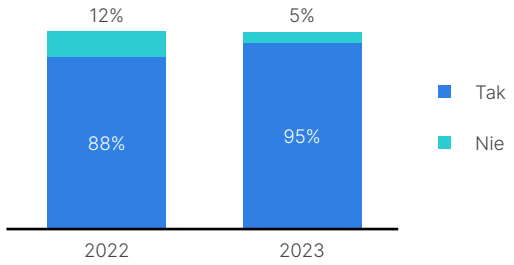
Spis treści

Najważniejsze wnioski

Kadra

W niemal wszystkich badanych przedsiębiorstwach cyberbezpieczeństwem systemów OT zajmuje się lub wkrótce będzie się zajmować dyrektor ds. bezpieczeństwa infrastruktury informatycznej (CISO). Warto również zauważyć, że coraz więcej specjalistów ds. cyberbezpieczeństwa systemów OT wywodzi się raczej ze struktur kierowniczych odpowiedzialnych za bezpieczeństwo infrastruktury IT, niż z działów operacyjnych.

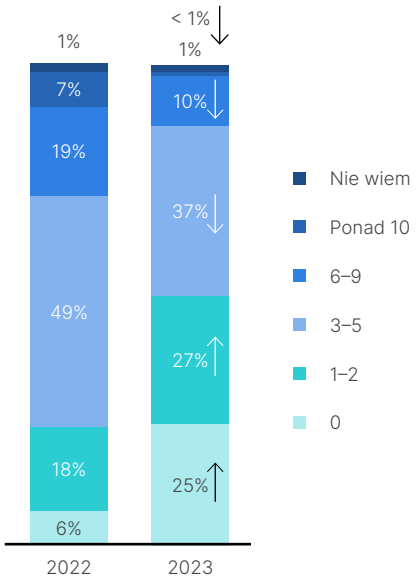
Cyberbezpieczeństwo ma w ciągu najbliższych 12 miesięcy przejść w zakres obowiązków CISO



Incydenty dotyczące cyber-bezpieczeństwa

Liczba przedsiębiorstw, które nie padły ofiarą cyberprzestępców, znacznie wzrosła r/r (z 6% w 2022 r. do **25% w 2023 r.**), wciąż jednak pozostaje wiele do zrobienia, ponieważ w ciągu ostatniego roku trzy czwarte przedsiębiorstw korzystających z systemów OT zgłosiło co najmniej jedno włamanie, a prawie jedna trzecia przedsiębiorstw przyznała, że padła ofiarą ataku za pomocą oprogramowania ransomware (**32%**, bez zmian w porównaniu z 2022 r). Liczba włamań za pomocą złośliwego oprogramowania i phishingu wzrosła odpowiednio o **12%** i **9%**.

Liczba włamań w poprzednim roku

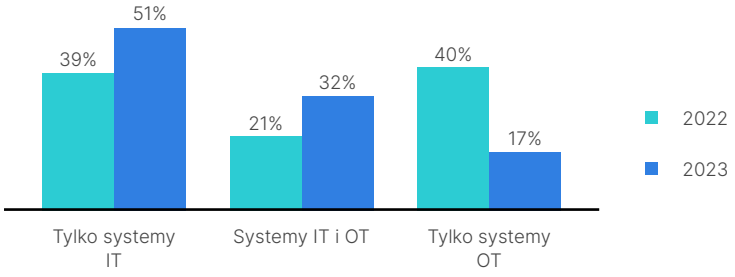


# Według dojrzałości cyberzabezpieczeń	Poziom 0 – 2	Poziom 3	Poziom 4
Nie wiem	1%	0%	0%
Ponad 10	1%	2%	0%
6–9	11%	11%	6%
3–5	38%	35%	40%
1–2	36%[B]	21%	25%
0	14%	31%[A]	29%[A]

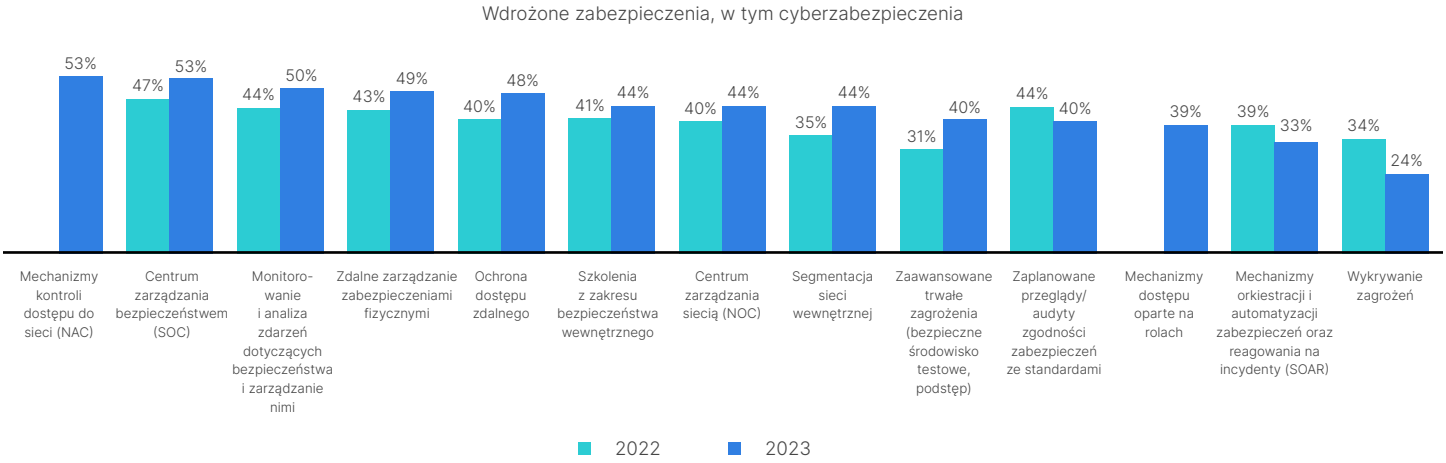
Zasięg włamań

Ilekroć na początku tego roku dochodziło do cyberataku, niemal jedna trzecia **(32%)** respondentów wskazywała, że dotyczył on zarówno systemów IT, jak i systemów OT (w ubiegłym roku odsetek ten wynosił zaledwie 21%). Aby przeciwdziałać włamaniom, specjaliści ds. systemów OT zwiększają w swoich sieciach przemysłowych liczbę cyberzabezpieczeń.

Systemy dotknięte atakiem

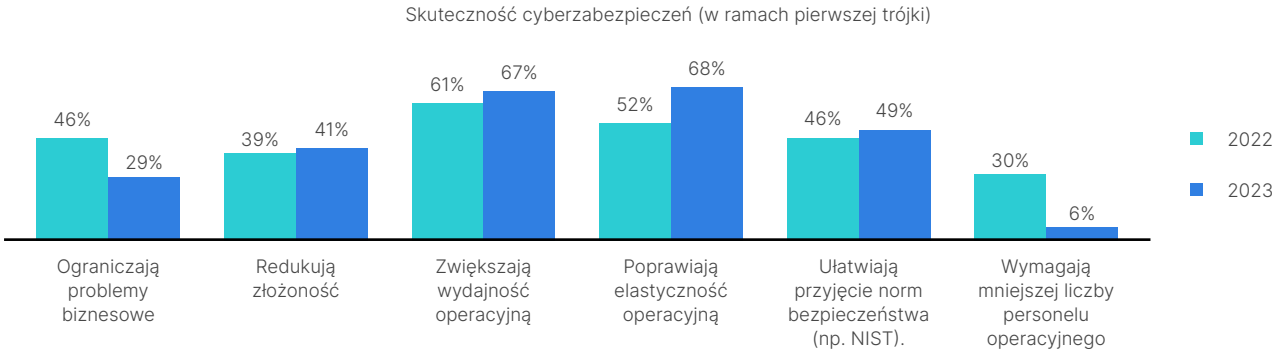


W największym stopniu wzrosła liczba wdrożonych zabezpieczeń chroniących przed zaawansowanymi, trwałymi zagrożeniami oraz rozwiązań służących do segmentacji sieci wewnętrznej i zapewnienia bezpiecznego dostępu zdalnego. Zmalała natomiast liczba stosowanych rozwiązań służących do zbierania i analizy informacji o zagrożeniach.



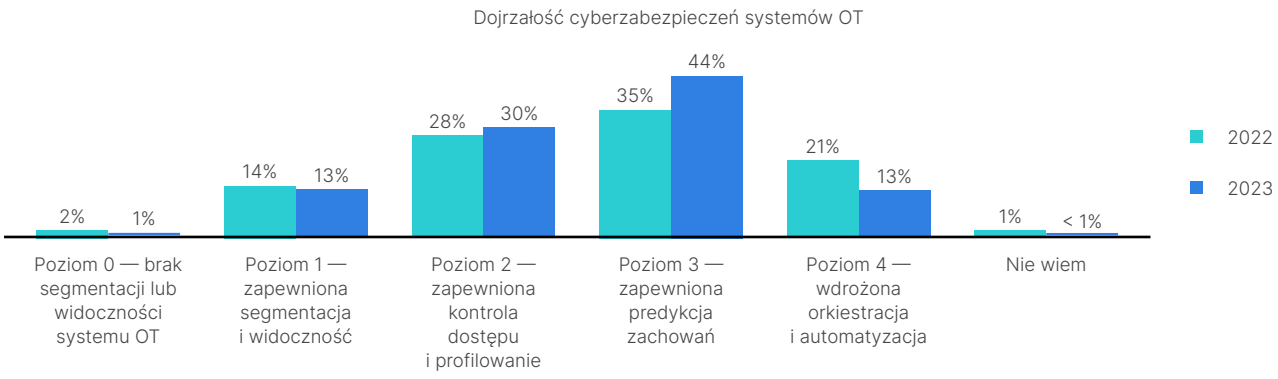
Skuteczność cyberzabezpieczeń

Wprawdzie z wyników ankiety wynika, że cyberzabezpieczenia nadal przyczyniają się do sukcesu działań podejmowanych przez większość **(76%)** specjalistów ds. systemów OT, a zwłaszcza do poprawy wydajności **(67%)** i elastyczności **(68%)**, daje się jednak zauważyć, że rozproszenie tych rozwiązań utrudnia spójną ochronę połączonych systemów IT i OT.

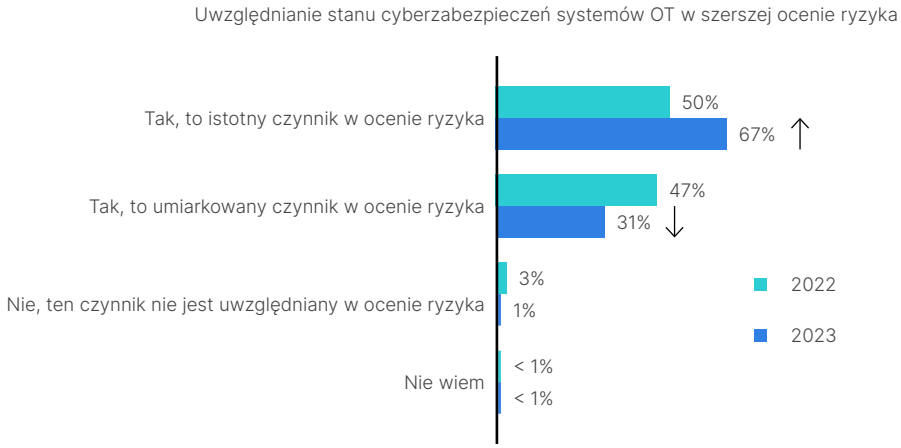


Stan cyberzabezpieczeń

O ile w tym roku mniej respondentów określiło stan cyberzabezpieczeń swoich systemów OT jako bardzo dojrzały (poziom 4), co w porównaniu z rokiem 2022 stanowi spadek **z 21% do 13%**, to **44%** wszystkich respondentów oceniło ten stan na poziomie 3, co stanowi wzrost z 35% w ubiegłym roku. Może to świadczyć o coraz bardziej dojrzałym podejściu do oceny własnego potencjału, co przekłada się na bardziej realistyczny obraz stanu cyberzabezpieczeń.



Niemal wszyscy respondenci (98%) uwzględniają stan cyberzabezpieczeń systemów OT w ramach szerszej oceny ryzyka przedstawianej członkom ścisłego kierownictwa i radom dyrektorów.

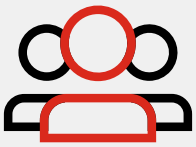


Streszczenie

Niniejszy „Raport o stanie technologii operacyjnej i cyberbezpieczeństwa za rok 2023" to nasze piąte coroczne badanie oparte na danych pochodzących ze szczegółowej, ogólnoświatowej ankiety przeprowadzonej wśród 570 specjalistów ds. systemów OT przez uznaną, zewnętrzną firmę badawczą.

Ochrona systemów OT jest obecnie ważniejsza niż kiedykolwiek, ponieważ coraz więcej przedsiębiorstw podłącza swoje systemy OT do Internetu. Wprawdzie połączenie systemów IT i OT niesie ze sobą wiele korzyści, wiąże się jednak z narażeniem na różne zaawansowane i destrukcyjne w skutkach cyberataki. Ofiarą tych ataków coraz częściej padają systemy OT. Z tych powodów wyniki tegorocznej ankiety wskazują, że cyberbezpieczeństwo systemów OT jest obecnie coraz bardziej centralnym i istotnym czynnikiem oceny ryzyka w badanych przedsiębiorstwach.

Analiza danych z 2023 r. ujawnia panujące obecnie na świecie cztery główne tendencje:



Z raportu za 2023 r. wynika, że w 95% przedsiębiorstw za cyberbezpieczeństwo systemów OT odpowiadają dyrektorzy ds. bezpieczeństwa infrastruktury informatycznej (CISO).

- Ogólny spadek liczby włamań ze względu na mniejszą liczbę wewnętrznych naruszeń bezpieczeństwa, przy czym ataki typu ransomware i phishing nadal stanowią poważne zagrożenie. Sytuacja ta może jednak wynikać z bardziej ukierunkowanego podejścia cyberprzestępców, a nie ze spadku ryzyka w tym obszarze.
- Powierzenie w niemal wszystkich badanych przedsiębiorstwach działań z zakresu cyberbezpieczeństwa systemów OT dyrektorowi ds. bezpieczeństwa infrastruktury informatycznej (CISO), a nie kierownictwu operacyjnemu.
- Zastosowanie przez respondentów szerokiej gamy cyberzabezpieczeń do przeciwdziałania włamaniom. Istnieją przesłanki wskazujące na to, że produkty punktowe i rozproszone rozwiązania mogą utrudniać wdrażanie i spójne egzekwowanie polityk bezpieczeństwa w połączonych systemach IT/OT.
- Liczba respondentów, którzy uważają, że dojrzałość stosowanych przez nich cyberzabezpieczeń jest na poziomie 4, spadła r/r z 21% do 13%. Liczba respondentów, którzy uważają, że dojrzałość stosowanych przez nich cyberzabezpieczeń jest na poziomie 3, wzrosła z 35% do 44%. Wydaje się to wskazywać na coraz bardziej realistyczną samoocenę posiadanego potencjału do przeciwdziałania cyberzagrożeniom dla systemów OT.

Z wyników pięciu edycji naszego rocznego badania wynika, że kwestie związane z cyberbezpieczeństwem systemów OT wydają się w końcu wychodzić z cienia, obszar ten znajduje się już bowiem w centrum uwagi członków ścisłego kierownictwa przedsiębiorstw. Większość respondentów ma tu jednak jeszcze wiele do zrobienia, a poza tym w kwestii cyberbezpieczeństwa nigdy nie można spocząć na laurach.

Aby pomóc odbiorcom naszego raportu w poprawie stanu bezpieczeństwa systemów OT, na jego końcu przedstawiamy listę najlepszych praktyk stosowanych przez przedsiębiorstwa najlepiej radzące sobie w tej dziedzinie.

Wstęp

Obecnie nie można już wątpić w znaczenie ochrony systemów OT. Technologie operacyjne (OT) kontrolują infrastrukturę o krytycznym znaczeniu, na której wszyscy polegamy, w tym sieci elektroenergetyczne, systemy wodno-kanalizacyjne, sieci transportowe, produkcję podstawowych towarów i globalne łańcuchy dostaw. Ponadto są również kluczowym elementem podejmowanych przez wiele przedsiębiorstw działań na rzecz przyspieszenia cyfrowego.

Aby w panujących warunkach rynkowych utrzymać konkurencyjność, przedsiębiorstwa z różnych sektorów muszą stosować metodyki i technologie z zakresu czwartej rewolucji przemysłowej (Przemysł 4.0), które są niezbędne do urzeczywistnienia „ery łączności, automatyzacji oraz zaawansowanych technologii analitycznych i produkcyjnych”[1].

Cyberzagrożenia dla systemów OT

Połączenie systemów IT i OT nie uszło uwadze cyberprzestępców i agresywnych państw narodowych. Z najnowszych raportów FortiGuard Labs „Global Threat Landscape” wynika, że w systemach OT coraz częściej wykrywane jest złośliwe oprogramowanie i dostrzegane są złośliwe działania[2].

Ten stan rzeczy potwierdza kilka głośnych cyberataków, które powinny być sygnałem ostrzegawczym dla wszystkich osób zajmujących się ochroną systemów OT. Jednym z najlepszych przykładów są nieustanne ataki Rosji na infrastrukturę krytyczną Ukrainy[3], które ponad rok temu przerodziły się w prawdziwą wojnę[4]. Wspomniane ataki nie występują jednak wyłącznie w ramach otwartej konfrontacji między państwami. Systemy OT na całym świecie są bowiem nadal celem cyberprzestępców, zwłaszcza w branży produkcji przemysłowej, w której nadal dochodzi do ukierunkowanych ataków typu ransomware na systemy OT[5].

Odsetek respondentów tegorocznego badania, którzy doświadczyli ataku typu ransomware (32%) jest niestety taki sam jak w roku ubiegłym (również 32%). Oznacza to, że w tej dziedzinie konieczne są dalsze postępy w zakresie cyberzabezpieczeń. Mając na uwadze ewolucję i rosnącą złożoność ataków typu ransomware, nie dziwi fakt, że 84% respondentów naszego badania jest bardzo lub bardzo poważnie zaniepokojonych tym zagrożeniem[6].

Wprawdzie liczba umyślnych i nieumyślnych wewnętrznych naruszeń bezpieczeństwa znacznie w tym roku spadła, ale z odpowiedzi ankietowych wynika, że liczba włamań z wykorzystaniem złośliwego oprogramowania i phishingu znacznie wzrosła (odpowiednio o 12% i 9%). Wyniki ankiety znajdują potwierdzenie w najnowszym raporcie FortiGuard Labs „Global Threat Report”, w którym barwnie stwierdzono, że „złośliwe oprogramowanie wie, jak trafiać na pierwsze strony gazet i utrzymywać przedsiębiorstwa w napięciu”[7].

Koniec izolacji

Po powszechnej integracji systemów IT i OT zniknęła izolacja, która do tej pory sprawiała, że systemy OT były niemal niewrażliwe na cyberataki. W rezultacie powierzchnie ataku przedsiębiorstw przemysłowych znacznie się rozszerzyły. Jeśli dodać do tego coraz częstsze wdrażanie urządzeń przemysłowego Internetu rzeczy (IIoT) (co oznacza nowe zagrożenia dla systemów OT związane z włamaniami do systemów IT) oraz dużą wartość atakowanych środowisk produkcyjnych, co zwiększa motywację ofiar cyberprzestępstw do zapłacenia okupu, staje się jasne, dlaczego ochrona systemów OT stała się tak istotna.

Cyberbezpieczeństwo systemów OT w centrum uwagi

W zeszłorocznym raporcie o stanie technologii operacyjnej i cyberbezpieczeństwa[8] stwierdzono, że zwiększone zainteresowanie i inwestycje związane z cyberbezpieczeństwem systemów OT stanowią bardzo dobry krok naprzód. Niemniej jednak z tegorocznej ankiety wynika, że wiele przedsiębiorstw ma jeszcze wiele do zrobienia, aby odpowiednio zabezpieczyć te systemy.

Przyjrzyjmy się zatem wynikom tegorocznej ankiety, aby poznać aktualny stan cyberbezpieczeństwa systemów OT. Miejmy również nadzieję, że w przyszłym roku w naszym raporcie zauważymy istotny postęp w tym zakresie.

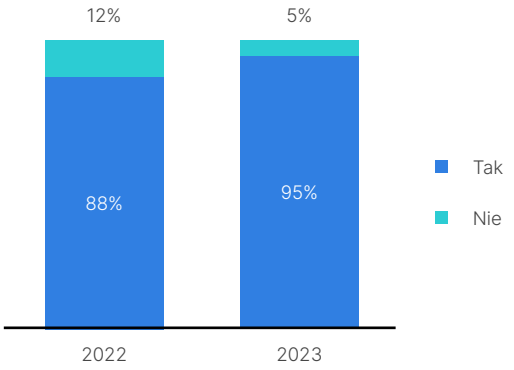
Najważniejsze spostrzeżenia

Spostrzeżenie 1. Odpowiedzialność za cyberbezpieczeństwo systemów OT przechodzi z personelu OT na specjalistów ds. cyberbezpieczeństwa

Specjalistów ds. systemów OT można znaleźć w niemal każdej dużej branży: produkcji przemysłowej, transporcie, logistyce, opiece zdrowotnej, przemyśle farmaceutycznym, przemyśle naftowym, przemyśle gazowym, energetyce, usługach użyteczności publicznej, chemii, gospodarce wodno-ściekowej itp. Specjaliści ci tradycyjnie mają również duży wpływ na decyzje dotyczące cyberbezpieczeństwa w podlegających im środowiskach OT.

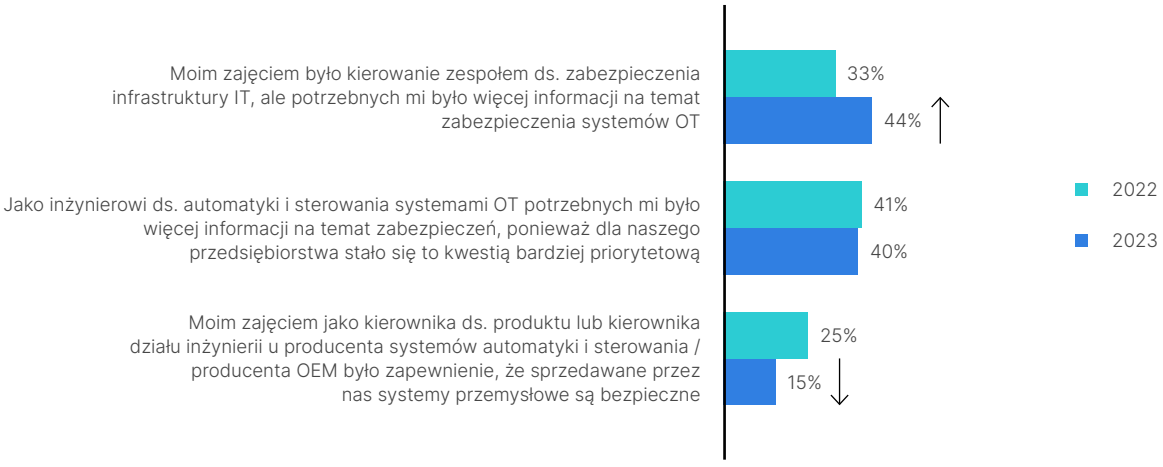
Wydaje się jednak, że ciągła podatność systemów OT na cyberataki doprowadziła do oddania decyzji związanych z cyberbezpieczeństwem tych systemów w gestię dyrektorów ds. bezpieczeństwa infrastruktury informatycznej (CISO). Z danych wynika również, że specjaliści ds. bezpieczeństwa systemów OT wywodzą się raczej z personelu IT niż z osób z doświadczeniem w zarządzaniu produktami. W rezultacie (co potwierdzają dane ankietowe) członkowie ścisłego kierownictwa i tradycyjni menedżerowie ds. bezpieczeństwa, a zwłaszcza CISO/CSO, uzyskują coraz większy wpływ na decyzje związane z cyberbezpieczeństwem.

P. Czy Państwa przedsiębiorstwo planuje w ciągu najbliższych 12 miesięcy włączyć zapewnienie cyberbezpieczeństwa systemów OT w zakres obowiązków CISO?



Cyberbezpieczeństwo ma w ciągu najbliższych 12 miesięcy przejść w zakres obowiązków CISO

P. Jakie doświadczenie zawodowe doprowadziło Państwa do funkcji obejmującej zabezpieczenie systemu OT?

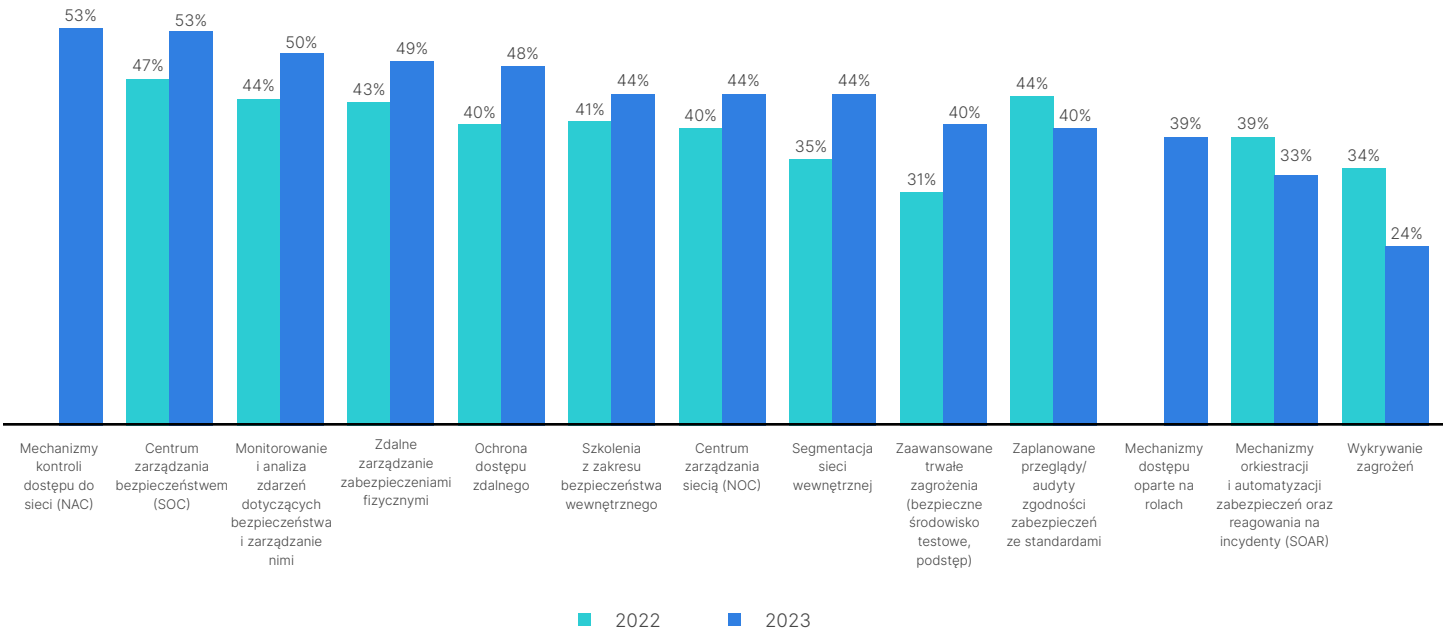


Ścieżka kariery, która doprowadziła do zajęcia się kwestiami z zakresu bezpieczeństwa systemów OT

Spostrzeżenie 2. Specjaliści ds. systemów OT korzystają z różnych rozwiązań

Ankietowani w tym roku specjaliści ds. systemów OT poszukują cyberzabezpieczeń, które przede wszystkim wykryją znane luki w zabezpieczeniach. Jednym z największych problemów dla takich specjalistów jest fakt, że przestój systemu OT ma często o wiele bardziej poważne skutki niż przestój systemu IT. W rezultacie sukces w kontekście systemów OT jest w mniejszym stopniu mierzony zachowaniem poufności i integralności danych, a w większym — dostępnością systemu. To z kolei sprawia, że priorytetem staje się czas reakcji na atak, co potwierdza powszechny wzrost liczby wdrożeń rozwiązań służących zażegnaniu tych problemów.

Podobnie jednak jak w przypadku sieci IT, samo wdrożenie odpowiednich rozwiązań nie wystarczy, aby zapobiec wszystkim atakom na systemy OT. W tym kontekście można zauważyć, że jeśli wdrożone rozwiązania będą pochodzić od różnych dostawców i nie zapewnią spójnego działania, wówczas wykrycie zagrożenia stanie się trudniejsze.



Wdrożone zabezpieczenia, w tym cyberzabezpieczenia

Spostrzeżenie 3. Liczba włamań wciąż jest niepokojąca

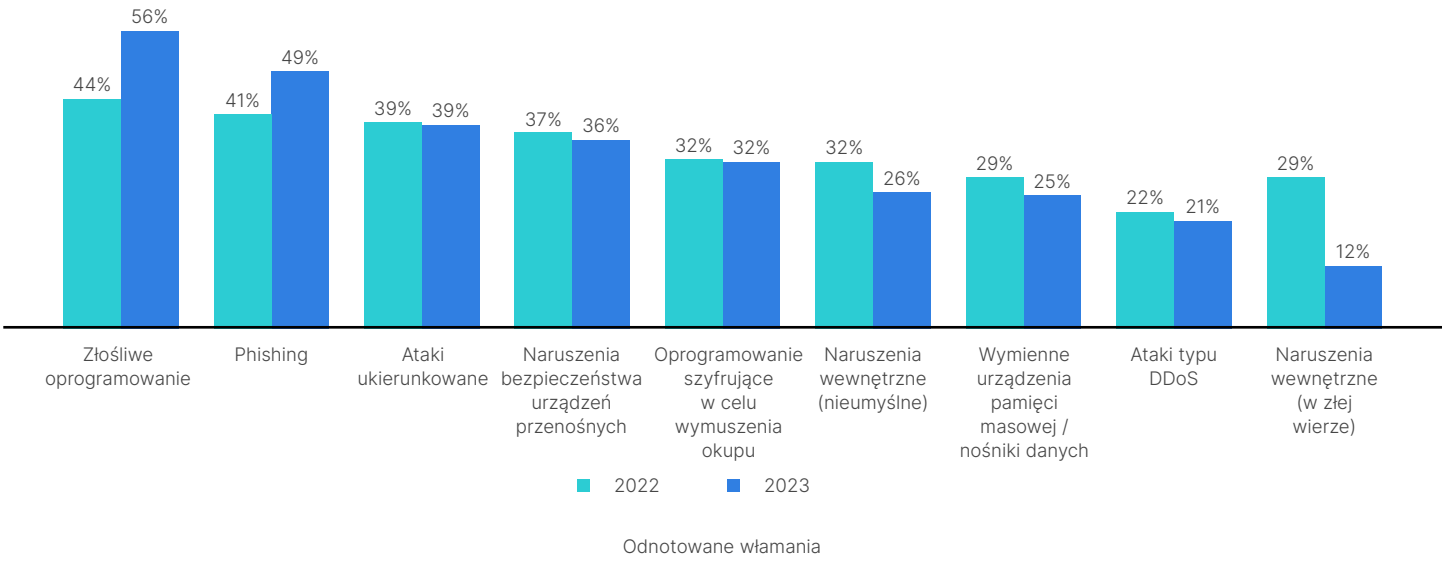
Liczba odnotowanych włamań spada, ale nadal 75% respondentów zgłasza, że doświadczyło co najmniej jednego włamania w ciągu ostatnich 12 miesięcy. Ogólny spadek w tej kategorii przypisuje się jednak mniejszej liczbie wewnętrznych naruszeń bezpieczeństwa, a nie mniejszej liczbie cyberataków.

Wprawdzie incydenty związane ze złośliwym oprogramowaniem i phishingiem pozostają najczęstszymi zagrożeniami, a ich liczba wzrosła w porównaniu z ubiegłym rokiem, ale to ataki typu ransomware (których liczba stale rośnie) nadal budzą największe obawy. Skutki wspomnianych incydentów były szerokie i w coraz większym stopniu wpływały na systemy IT i OT, ale zazwyczaj były eliminowane w ciągu kilku godzin (coraz częściej w ciągu kilku minut).

Niektóre spadki liczby włamań mogą wynikać ze zmiany taktyki cyberprzestępców. Metody działania atakujących są jednak nadal skuteczne, o czym świadczy wzrost liczby wykrytych przypadków złośliwego oprogramowania i phishingu. Mimo to, biorąc pod uwagę wysoką wartość systemów OT, przewidujemy stosowanie przez przestępców coraz bardziej ukierunkowanych ataków.

Należy zauważyć, że nadmierna pewność siebie co do gotowości na zagrożenia szkodzi w takim samym stopniu, jak stosowanie niewłaściwych zabezpieczeń, co według naszego najnowszego raportu o atakach typu ransomware[9], jest kolejnym problemem, z którym boryka się większość respondentów. O ile na przykład ochrona przed takim atakiem jest dla większości respondentów priorytetem, o tyle wiele rozwiązań uznawanych przez nich za kluczowe dla strategii cyberbezpieczeństwa zapewnia niewielką ochronę przed tymi atakami.

P. Z jakim typem włamań mieli Państwo do czynienia? (proszę zaznaczyć wszystkie opcje mające zastosowanie)



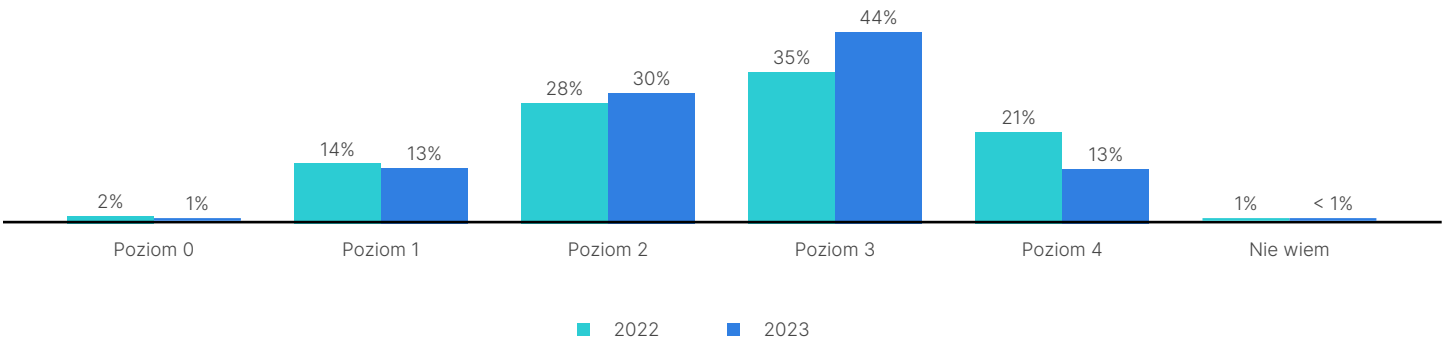
Odnotowane włamania

Spostrzeżenie 4. Wzrasta średni poziom dojrzałości cyberzabezpieczeń

Dokładna samoocena własnych zdolności w zakresie cyberbezpieczeństwa i dojrzałości stanu zabezpieczeń jest kluczowym pierwszym krokiem w kierunku właściwego zabezpieczenia systemów OT przed cyberzagrożeniami. W tym roku mniejsza liczba respondentów określiła stan bezpieczeństwa swoich systemów OT jako bardzo dojrzały (spadek z 21% w 2022 r. do 13% w tym roku). Jednocześnie 44% respondentów oceniło swoją dojrzałość cyberzabezpieczeń swoich systemów OT na poziomie 3 (w porównaniu z 35% rok temu). Z danych tych wynika, że tegoroczni respondenci mogą oceniać swoje zdolności w zakresie cyberbezpieczeństwa systemów OT w sposób bardziej realistyczny.

Skala dojrzałości	
Poziom 0	Brak segmentacji lub widoczności systemów OT
Poziom 1	Zapewniona segmentacja i widoczność
Poziom 2	Zapewniona kontrola dostępu i profilowanie
Poziom 3	Zapewniona predykcja zachowań
Poziom 4	Wdrożona orkiestracja i automatyzacja

P: Jak oceniliby Państwo stan bezpieczeństwa swojej infrastruktury OT pod kątem dojrzałości?

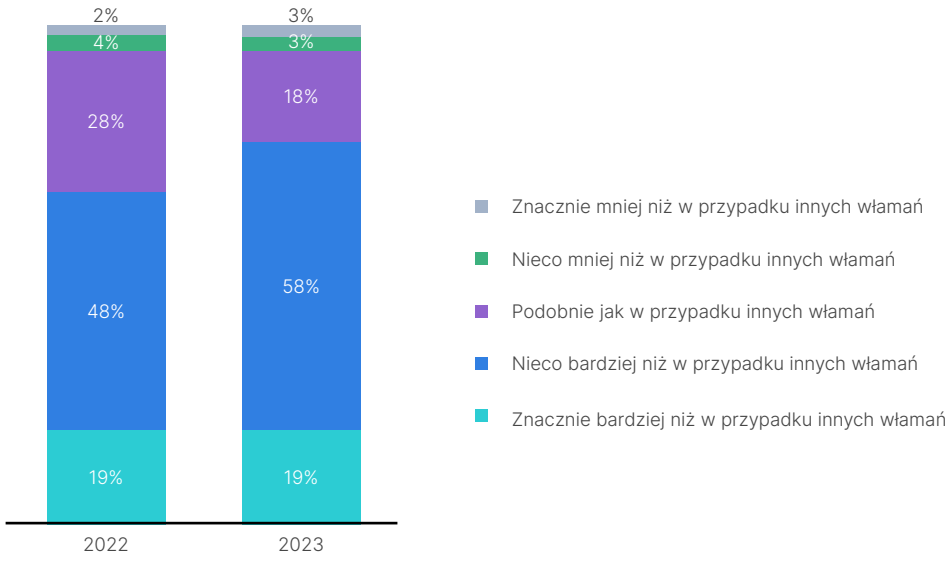


Dojrzałość cyberzabezpieczeń systemów OT

Szczegółowe informacje o ankiecie za 2023 r.

P. Jak bardzo, w porównaniu z innymi włamaniami, niepokoi Państwa wpływ ataków typu ransomware na Państwa środowisko OT?

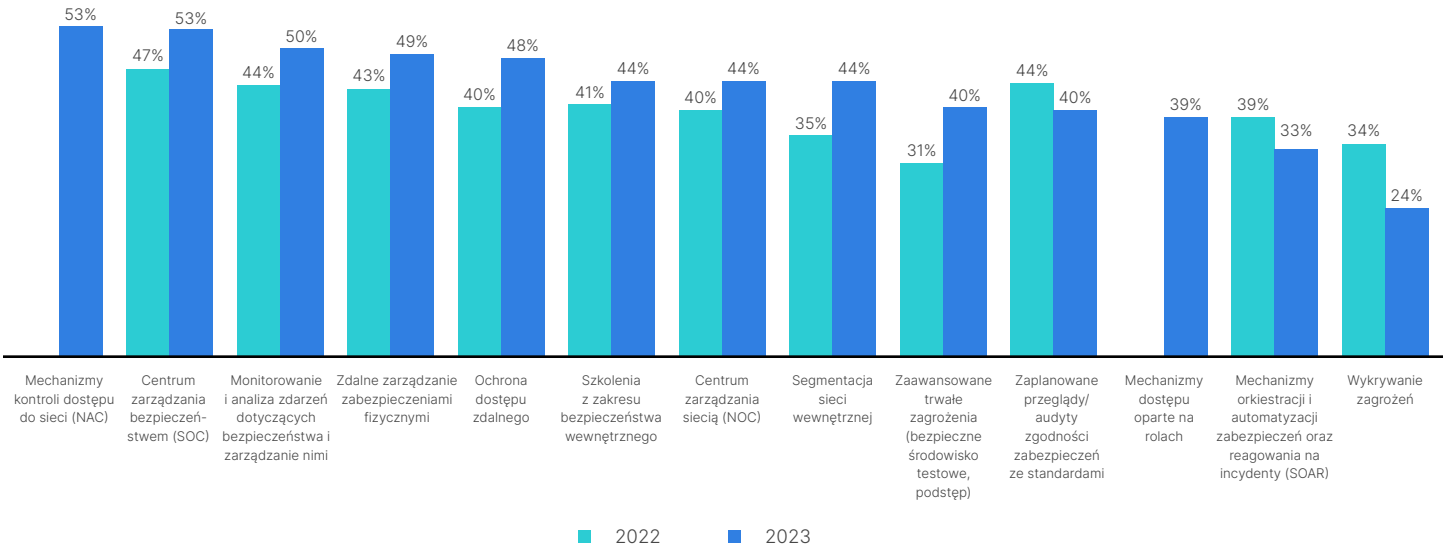
Występujące w przedsiębiorstwie lub sieci IT incydenty związane z atakami typu ransomware mogą bezpośrednio lub pośrednio wpływać na produkcję. Respondenci są coraz bardziej zaniepokojeni tym zagrożeniem niż innymi zagrożeniami (mimo że przypadki phishingu i użycia złośliwego oprogramowania są bardziej powszechne). Ataki typu ransomware pozostają zatem największą przyczyną niepokoju ze względu na ich skutki produkcyjne i finansowe.



Niepokój o wpływ ataków typu ransomware

P. Jakie zabezpieczenia, w tym cyberzabezpieczenia, są obecnie przez Państwa stosowane?

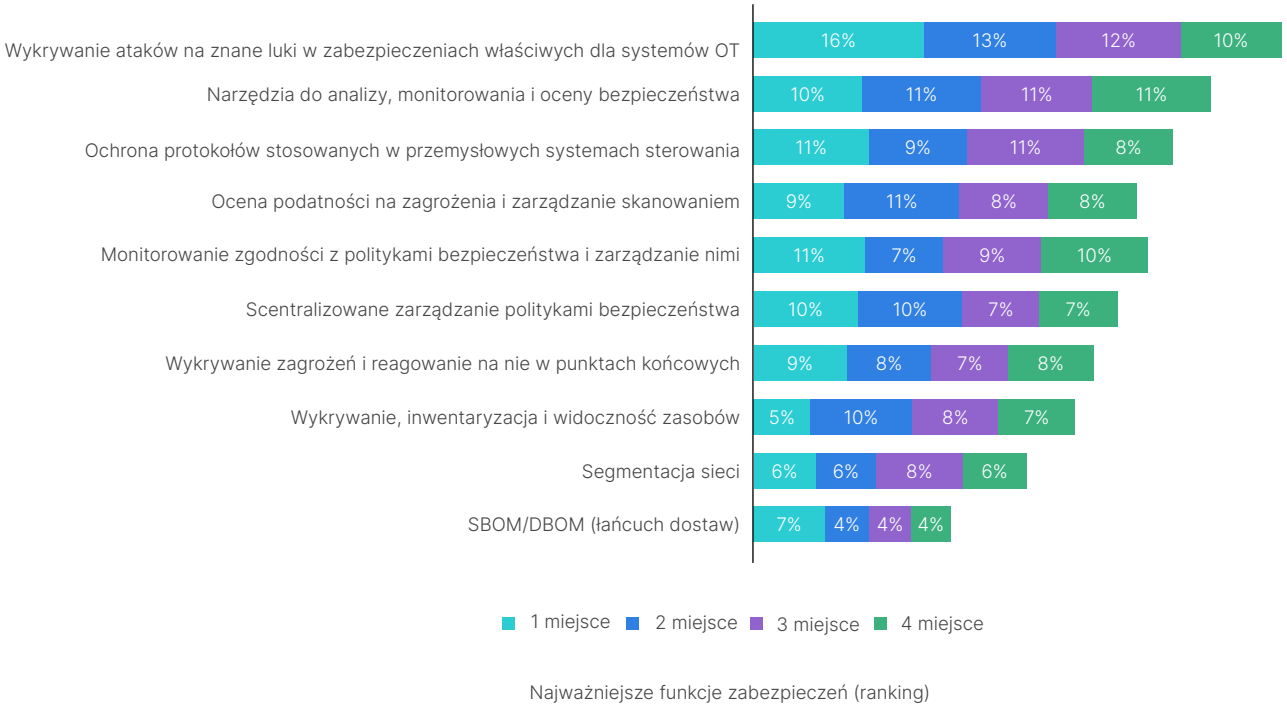
Aby przeciwdziałać włamaniom, specjaliści ds. systemów OT wzmacniają stosowane zabezpieczenia. Wraz z upowszechnianiem się i wzrostem liczby takich zabezpieczeń, w tym coraz większym ich zaawansowaniem (rozwiązania SOAR, analiza informacji o zagrożeniach), podejrzewamy, że liczba audytów bezpieczeństwa będzie spadać. Gdy te nowe funkcje będą już w pełni działać, liczba wspomnianych audytów prawdopodobnie wzrośnie do wcześniejszego poziomu.



Wdrożone zabezpieczenia, w tym cyberzabezpieczenia

P: Jakie funkcje cyberzabezpieczeń systemów OT są dla Państwa najważniejsze? (proszę uszeregować maksymalnie cztery z nich)

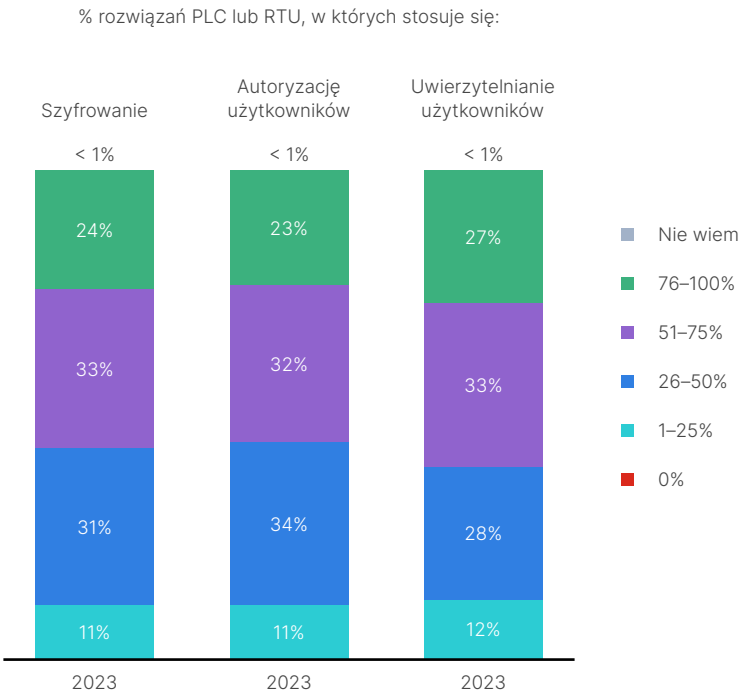
Wykrywanie ataków na znane luki w zabezpieczeniach jest obecnie najważniejszą funkcją cyberzabezpieczeń, której znaczenie wzrosło w ciągu ostatniego roku. Innym wskaźnikiem rosnącej dojrzałości w zakresie bezpieczeństwa systemów OT jest niższy priorytet nadawany wykrywaniu i segmentacji zasobów. Według naszych obserwacji branżowych oraz zgodnie z danymi CIS[10] większość klientów po podjęciu tych podstawowych działań decyduje się na bardziej zaawansowane rozwiązania infrastrukturalne i organizacyjne.



Najważniejsze funkcje zabezpieczeń (ranking)

P. Jaki procent Państwa programowalnych sterowników logicznych (PLC) lub zdalnych terminali (RTU) korzysta z poszczególnych funkcji bezpieczeństwa wymienionych poniżej?

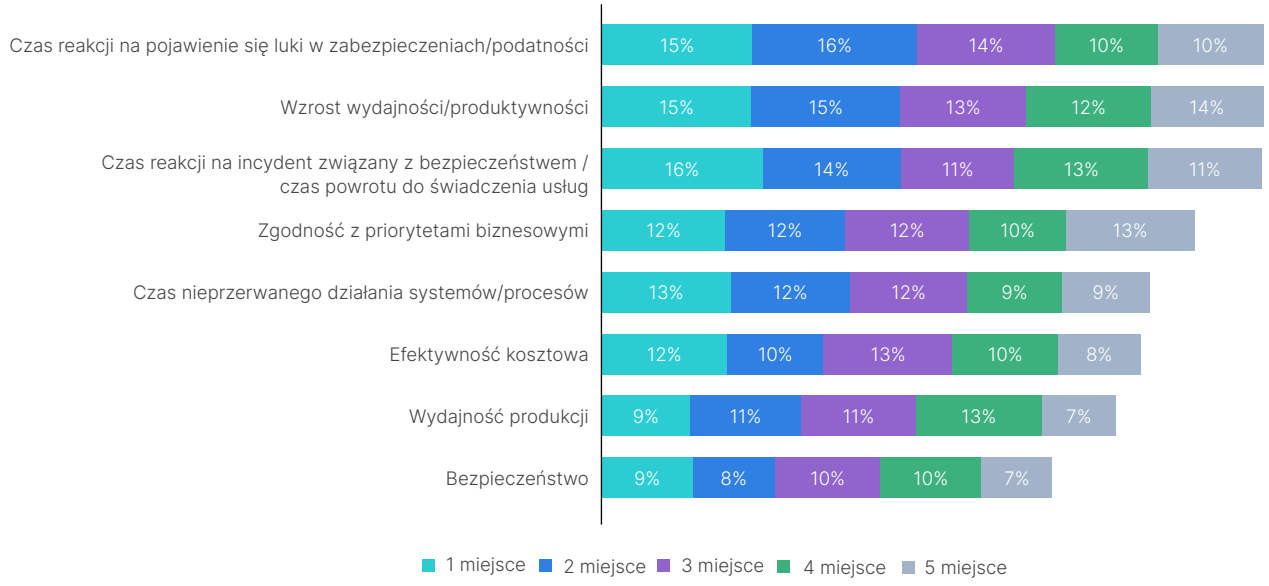
Szyfrowanie, autoryzacja użytkowników i uwierzytelnianie użytkowników to funkcje stosowane w przypadku ponad połowy rozwiązań PLC i RTU.



Wpływ globalny

P: Jak mierzą Państwo swój sukces? (proszę uszeregować maksymalnie pięć z tych elementów)

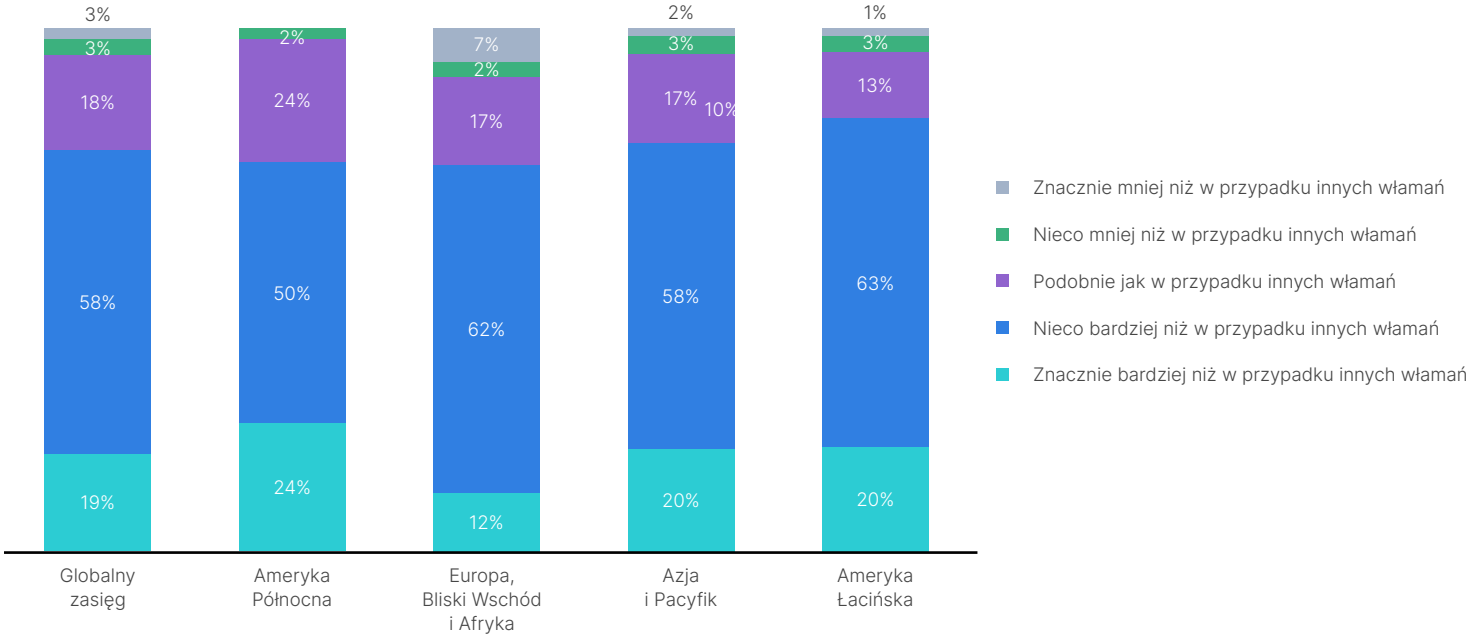
Nie ma jednej definicji sukcesu w kontekście zabezpieczenia systemów OT, co wskazuje na niedojrzałość tego obszaru. Niemniej jednak, zgodnie z oczekiwaniami osób zajmujących się tym obszarem, czas reakcji i wzrost produktywności znalazły się na szczycie listy.



Sposoby mierzenia sukcesu (ranking)

P. Jak bardzo, w porównaniu z innymi włamaniami, niepokoi Państwa wpływ ataków typu ransomware na Państwa środowisko OT?

Chociaż ataki typu ransomware nie są najczęstszymi zagrożeniami, są jednak głównym powodem do niepokoju większości respondentów na całym świecie (bardziej niż jakiekolwiek inne zagrożenia). Wynika to prawdopodobnie z nadawanego im rozgłosu oraz wysokich kosztów przywracania zainfekowanych systemów.



Niepokój o wpływ ataków typu ransomware

Najlepsze praktyki

75% respondentów tegorocznego badania zgłosiło co najmniej jedno włamanie w ciągu ostatnich 12 miesięcy. Jest to jednak poprawa w stosunku do 2022 r., kiedy to ponad 90% respondentów zgłosiło co najmniej jedno włamanie. W tym roku tylko 11% respondentów poinformowało o co najmniej sześciu włamaniach (w ubiegłym roku było to 27%).

Cyberzabezpieczenia nadal przyczyniają się do sukcesu większości (76%) specjalistów ds. systemów OT, w szczególności poprzez poprawę wydajności (67%) i elastyczności (68%). Wyniki raportu wskazują jednak na to, że rozproszenie rozwiązań nadal utrudnia spójne wdrażanie, stosowanie i egzekwowanie zasad w coraz bardziej połączonych systemach IT i OT. Problem ten jest pogłębiany wskutek starzenia się systemów, przy czym większość (74%) respondentów podaje, że średni wiek wdrożonych u nich systemów ICS wynosi od sześciu do dziesięciu lat. Bez wątpienia poczyniono pewne postępy w zakresie globalnego cyberbezpieczeństwa systemów OT, ale dalsze działania w tym zakresie muszą być kontynuowane.

Poniżej przedstawiono kilka najlepszych praktyk, które naszym zdaniem stoją za niewielką, ale istotną poprawą stwierdzoną w tegorocznych wynikach ankiety.

Przygotowanie strategii dotyczącej dostawcy i cech platformy zapewniającej cyberbezpieczeństwo systemu OT.

Efektem konsolidacji jest ograniczenie złożoności i szybsze osiąganie wyników. Należy zatem zacząć od zbudowania odpowiedniej platformy we współpracy z dostawcą, który tworzy swoje produkty z myślą o integracji i automatyzacji. Dostawca taki umożliwi spójne wdrożenie i egzekwowanie zasad w coraz bardziej połączonych systemach IT i OT. Warto pamiętać, aby dostawca taki dysponował również szeroką ofertą obejmującą zarówno rozwiązania podstawowe (inwentaryzacja i segmentacja zasobów), jak i rozwiązania bardziej zaawansowane (funkcje centrum SOC dla systemu OT lub funkcje wspólnego centrum SOC dla systemów IT/OT).

Wdrożenie mechanizmów kontroli dostępu do sieci (NAC).

Rozwiązywanie problemów związanych z zabezpieczaniem przemysłowych systemów sterowania (ICS), systemów nadzorowania procesów technologicznych (SCADA), Internetu rzeczy (IoT), urządzeń prywatnych używanych w celach służbowych (BYOD) i innych punktów końcowych wymaga, aby zaawansowane mechanizmy kontroli dostępu (NAC) wchodziły w skład kompleksowej architektury bezpieczeństwa. Skuteczne rozwiązanie NAC pomaga również utrzymać pełną kontrolę nad siecią przedsiębiorstwa, umożliwiając zarządzanie nowymi urządzeniami, które chcą się łączyć lub komunikować z innymi częściami infrastruktury przedsiębiorstwa.

Zastosowanie podejścia zerowego zaufania.

Po wdrożeniu podstawowych etapów inwentaryzacji i segmentacji zasobów należy zastosować podejście zerowego zaufania, które sprawia, że ilekroć użytkownik, aplikacja lub urządzenie chce uzyskać dostęp do krytycznych zasobów, niezależnie od tego, gdzie się znajdują, wykonywana jest wówczas odpowiednia weryfikacja uprawnień do takiego dostępu.

Uruchomienie szkoleń podnoszących świadomość w zakresie cyberbezpieczeństwa.

Szkolenia z zakresu cyberbezpieczeństwa są nadal niezwykle ważne, ponieważ walka z cyberprzestępcami wymaga wyposażenia każdego pracownika w wiedzę i świadomość niezbędną do współpracy w celu ochrony siebie i danych pracodawcy. Warto tutaj rozważyć szkolenia nietechniczne, skierowane do każdego użytkownika komputera lub urządzenia przenośnego, począwszy od telepracowników, a skończywszy na ich rodzinach.

Najważniejsze porady

1. Po wdrożeniu podstawowych etapów inwentaryzacji i segmentacji zasobów należy przejść do bardziej zaawansowanych rozwiązań w zakresie mikrosegmentacji i wirtualnego patchowania w celu ochrony posiadanych urządzeń przed znanymi lukami w zabezpieczeniach (przez zapewnienie wystarczającej ilości czasu na eliminację tych luk).
2. Dzięki współpracy zespołów zajmujących się systemami IT, systemami OT i produkcją można odpowiednio oceniać zagrożenia, zwłaszcza związane z atakami typu ransomware, oraz informować o nich CISO w celu zapewnienia odpowiedniej świadomości niebezpieczeństwa, nadania działaniom odpowiednich priorytetów, określenia budżetu i przydzielenia personelu.
3. Warto przygotować strategię dotyczącą dostawcy i cech platformy zapewniającej cyberbezpieczeństwo systemu OT. Ostatnio oferowanych jest wiele nowych rozwiązań w zakresie bezpieczeństwa, ale luka kadrowa w przedsiębiorstwach wciąż się powiększa. Ponadto w miarę dojrzewania stanu bezpieczeństwa należy dążyć do nawiązania współpracy z dostawcami mającymi szeroką ofertę rozwiązań podstawowych służących do inwentaryzacji i segmentacji zasobów oraz rozwiązań bardziej zaawansowanych (funkcje centrum SOC dla systemu OT lub funkcje wspólnego centrum SOC dla systemów IT/OT).

Metodyka badania

Większość respondentów tego badania zajmuje stanowiska związane z działalnością operacyjną lub działalnością produkcyjną, przy czym prawie jedna trzecia z nich to wiceprezesi lub dyrektorzy ds. operacyjnych. Bez względu na zajmowane stanowisko większość ankietowanych jest mocno zaangażowana w podejmowanie decyzji dotyczących cyberbezpieczeństwa i to właśnie takie osoby mają coraz więcej do powiedzenia przy podejmowaniu decyzji o zakupach dotyczących systemów OT. Z tegorocznego badania wynika, że 91% respondentów regularnie uczestniczy w podejmowaniu decyzji dotyczących zakupu cyberzabezpieczeń dla swojego pracodawcy.

Wszyscy respondenci tegorocznego badania pracowali w jednej z następujących branż:

- Produkcja przemysłowa
- Transport i logistyka
- Opieka zdrowotna, przemysł farmaceutyczny
- Branża naftowo-gazowa i rafineryjna
- Energetyka i usługi użyteczności publicznej
- Przemysł chemiczny i petrochemiczny
- Gospodarka wodno-ściekowa

Cele badania

Na potrzeby przygotowania profilu specjalisty ds. systemów OT firma Fortinet zatrudniła zewnętrzną firmę badawczą InMoment.

W opracowanej wspólnie ankiecie zawarliśmy pytania, które mają nam pomóc w lepszym zrozumieniu poniższych kwestii:

- Jak dany respondent wpisuje się w strukturę przedsiębiorstwa
- Jak korzysta się z zabezpieczeń
- Jak się śledzi i raportuje informacje
- Jakie są wpływy i czynniki sukcesu

Podejście

Na bazie próby panelowej uzyskano 570 wypełnionych ankiet od respondentów reprezentujących przedsiębiorstwa z następujących branż:

- Produkcja przemysłowa
- Transport i logistyka
- Opieka zdrowotna, przemysł farmaceutyczny
- Branża naftowo-gazowa i rafineryjna
- Energetyka i usługi użyteczności publicznej
- Przemysł chemiczny i petrochemiczny
- Gospodarka wodno-ściekowa
  - zatrudniających ponad 1000 pracowników (z wybranymi wyjątkami)
- Ponadto w gestii respondenta leży zajmowanie się systemami OT
- Respondent odpowiada również za operacje produkcyjne lub działalność operacyjną zakładu.

- Co więcej respondent uczestniczy w podejmowaniu decyzji o zakupach cyberzabezpieczeń
- Globalny zasięg w latach 2022 i 2023:
  - Respondenci badania pochodzili z różnych krajów świata, w tym z Australii, Nowej Zelandii, Brazylii, Kanady, Egiptu, Francji, Niemiec, Indii, Japonii, Meksyku, RPA, Zjednoczonego Królestwa i Stanów Zjednoczonych.

Podsumowanie

Z niniejszego raportu za rok 2023 wynika, że przedsiębiorstwa traktują cyberbezpieczeństwo systemów OT priorytetowo. Jest to ważna i niezbędna tendencja, ponieważ 75% badanych przedsiębiorstw musiało zmierzyć się z co najmniej jednym cyberatakiem w ciągu ostatnich 12 miesięcy. Ponadto z badania wynika, że cyberbezpieczeństwo systemów OT wzrasta lub staje się coraz bardziej dojrzałe, a liczba incydentów wydaje się spadać. Ryzyko związane z incydentami dotyczącymi systemów OT staje się również coraz bardziej zauważalne za sprawą nagłaśnianych w tym zakresie wydarzeń na świecie. Co więcej przedsiębiorstwa podchodzą do kwestii bezpieczeństwa systemów OT coraz agresywniej, a w zabezpieczanie tych systemów coraz bardziej angażują się zespoły IT.

Z danych ankietowych przebija coraz powszechniejsze stosowanie w przedsiębiorstwach różnych rozwiązań z zakresu cyberbezpieczeństwa systemów OT. Wspomniane cyberbezpieczeństwo, jak również własność, ryzyko i wdrażanie cyberzabezpieczeń tych systemów stają się coraz bardziej dojrzałe i mają coraz większy wpływ na prowadzenie działalności. Przed większością przedsiębiorstw jest jednak jeszcze długa droga do zapewnienia odpowiedniej ochrony przed najpopularniejszym obecnie złośliwym oprogramowaniem jakim jest ransomware.

1 „What are Industry 4.0, the Fourth Industrial Revolution, and 4IR?", McKinsey and Company, 17 sierpnia 2022 r.

2 „2022 Global Threat Landscape Report", FortiGuard Labs, 22 luty 2023 r.

3 „Cyber-Attack Against Ukrainian Critical Infrastructure", CISA, 20 lipca 2021 r.

4 „Ukraine: Russian attacks on critical energy infrastructure amount to war crimes", Amnesty International, 22 października 2022 r.

5 Jonathan Reed, „Pipedream Malware Can Disrupt or Destroy Industrial Systems", Security Intelligence, 19 kwietnia 2023 r.

6 „The 2023 Global Ransomware Report", Fortinet, 24 kwietnia 2023 r.

7 „2022 Global Threat Landscape Report", FortiGuard Labs, 22 luty 2023 r.

8 „2022 State of Operational Technology and Cybersecurity Report", Fortinet, 21 czerwca 2022 r.

9 „The 2023 Global Ransomware Report", Fortinet, 24 kwietnia 2023 r.

10 „CIS Critical Security Controls ICS Companion Guide", Center for Internet Security, wersja 7.

28 czerwca 2023

2101968-0-0-PL