RAPORT

Dyrektorzy operacyjni a cyberbezpieczeństwo infrastruktury OT

Raport na temat bieżących priorytetów i wyzwań

Spis treści

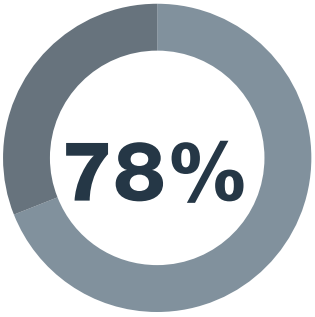
Streszczenie

Niniejszy raport zatytułowany „Dyrektorzy operacyjni a cyberbezpieczeństwo infrastruktury OT — raport na temat bieżących priorytetów i wyzwań" został przygotowany przez Fortinet w celu zbadania stojących przed dyrektorami operacyjnymi problemów oraz przedstawienia podejmowanych przez nich działań w kontekście odpowiedniego zabezpieczenia infrastruktury technologii operacyjnej (OT). Odpowiedzialność za bezpieczeństwo infrastruktury OT spoczywa zazwyczaj na menedżerze ds. zabezpieczeń infrastruktury informatycznej (Chief Information Security Officer, CISO) lub innym dyrektorze wykonawczym, dyrektor operacyjny (Chief Operating Officer, COO) odgrywa jednak w tych działaniach istotną rolę, ponieważ w gestii podlegających mu zespołów leży często zakup sprzętu używanego w procesach produkcyjnych, w tym narzędzi bezpieczeństwa, oraz zarządzanie tym sprzętem.

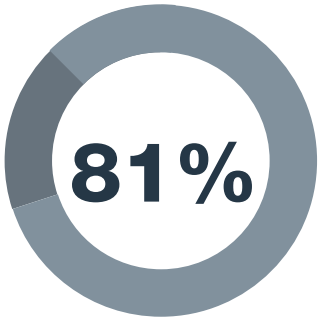
Ostatnie badanie przeprowadzone przez Fortinet ujawniło przede wszystkim następujące fakty dotyczące roli dyrektora operacyjnego w systemie bezpieczeństwa infrastruktury OT:

1. Dyrektorzy operacyjni stoją w obliczu **bezprecedensowych zmian**, których źródłem są takie zjawiska, jak proces łączenia ze sobą sieci OT i IT, wyższe oczekiwania pionów biznesowych oraz rosnący udział menedżera ds. zabezpieczeń infrastruktury informatycznej w procesach poprawy cyberbezpieczeństwa systemów OT.
2. Dyrektorzy operacyjni stoją w głównej mierze **przed wyzwaniami związanymi z zarządzaniem ryzykiem**.
3. Ścisłe kierownictwo jest skłonne zatwierdzać **większe budżety na cyberbezpieczeństwo systemów OT,** ale oczekuje, że dyrektor operacyjny spożytkuje je w sposób gwarantujący wymierne rezultaty.
4. Dyrektorzy operacyjni mają również trudności **z dotrzymaniem tempa zmian** ze względu na coraz bardziej zaawansowane metody włamań.

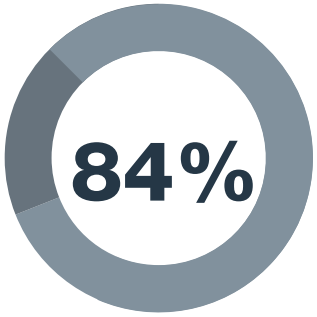
Uwzględniwszy wspomniane tendencje i wyzwania, dokonaliśmy bardziej szczegółowej analizy danych i zidentyfikowaliśmy dwa podzbiory respondentów na podstawie liczby włamań w poprzednim roku. Następnie poddaliśmy analizie cechy reprezentatywne dla dyrektorów operacyjnych najwyższego szczebla na tle cech reprezentatywnych dla dyrektorów operacyjnych najniższego szczebla w celu identyfikacji czynników, od których zależy powodzenie stosowanej strategii bezpieczeństwa. Z takich najlepszych praktyk wynika, że skuteczniejsi dyrektorzy operacyjni zręcznie równoważą kwestie cyberbezpieczeństwa z obowiązkami operacyjnymi w drodze śledzenia i raportowania kluczowych wskaźników cyberbezpieczeństwa, regularnego testowania zabezpieczeń i zgodności z przepisami oraz wdrażania sprawdzonych mechanizmów bezpieczeństwa takich jak uwierzytelnianie wieloskładnikowe.



dyrektorów operacyjnych bezpośrednio odpowiada za uwzględnienie kwestii bezpieczeństwa w procesach operacyjnych

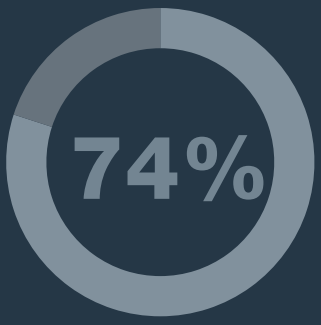


dyrektorów operacyjnych regularnie uczestniczy w kształtowaniu realizowanej przez dane przedsiębiorstwo strategii cyberbezpieczeństwa

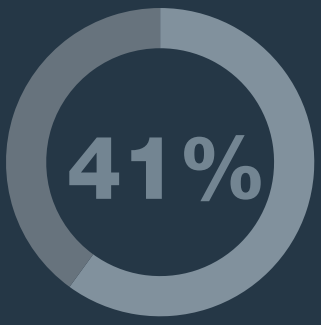


dyrektorów operacyjnych regularnie uczestniczy w procesie podejmowania decyzji o zakupach związanych z zapewnieniem cyberbezpieczeństwa

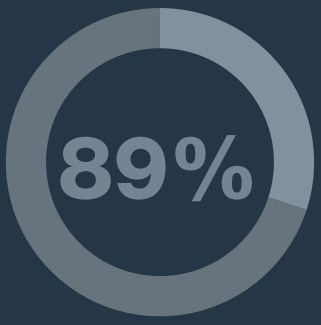
Infografika — najważniejsze wnioski



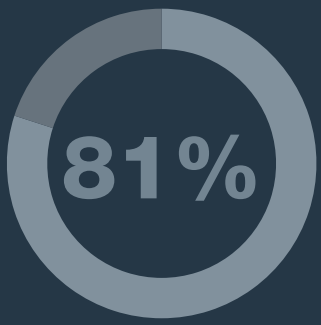
respondentów zarządza co najmniej setką urządzeń



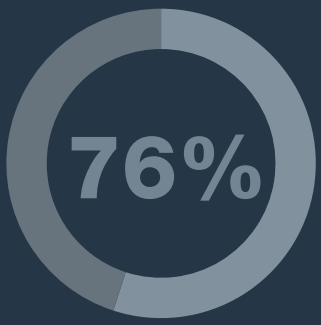
respondentów ma zainstalowanych ponad 250 urządzeń



respondentów miało do czynienia z włamaniami w ciągu ostatnich 12 miesięcy



respondentów miało do czynienia z przerwami w pracy podczas tych włamań



respondentów oczekuje zwiększenia budżetu na bezpieczeństwo w 2019 r., przy czym 10% z nich spodziewa się ***bardzo dużego*** wzrostu

Dyrektorzy operacyjni najwyższego szczebla są o:

168% bardziej skłonni do uznawania zmiany przepisów za główne wyzwanie do pokonania na drodze do odniesienia sukcesu

124% bardziej skłonni do pracy w przedsiębiorstwach, w których kadra kierownicza najwyższego szczebla nadzoruje kwestie dotyczące cyberbezpieczeństwa

79% bardziej skłonni do uznania wydajności produkcji za swój najważniejszy wskaźnik sukcesu

45% bardziej skłonni do planowania przeglądów zgodności z przepisami.

Wstęp

Termin „technologia operacyjna" (ang. operational technology) oznacza infrastrukturę służącą do monitorowania i kontroli procesów i działań produkcyjnych w zakładach przemysłowych, sieciach energetycznych, przedsiębiorstwach wodociągowych, przedsiębiorstwach zajmujących się wydobyciem ropy naftowej i gazu ziemnego, przedsiębiorstwach transportowych itp. Infrastruktura OT tradycyjnie bazuje na sprzęcie i oprogramowaniu opracowanym specjalnie na potrzeby przemysłu. W związku z powyższym infrastruktura OT i infrastruktura IT od zawsze stanowiły odrębne byty z punktu widzenia zarówno budowy, jak i zarządzania.

Wiele sieci OT nie jest podzielonych na segmenty i używane są w nich różne protokoły produkcyjne, niezidentyfikowane zasoby i starsze urządzenia. Niektóre sieci OT mają niezabezpieczone kanały komunikacji z sieciami przedsiębiorstw lub sieciami IT, podczas gdy inne sieci OT nie mają w ogóle połączenia z Internetem i innymi sieciami zewnętrznymi. Ogólnie rzecz biorąc, sieci OT otwierają się jednak na świat zewnętrzny. Na przykład wyniki niedawno przeprowadzonego badania pokazały, że 34,5% sieci OT jest podłączonych do Internetu, a 66,4% tych sieci jest podłączonych do zewnętrznej infrastruktury prywatnej lub do sieci macierzystego przedsiębiorstwa[1].

Panująca w branży tendencja sprowadza się do łączenia ze sobą infrastruktur OT i IT w celu zapewnienia przedsiębiorstwu korzyści na kilka sposobów. Jeśli infrastruktury OT i IT są od siebie oddzielone (stanowią odrębne silosy), wymiana danych między nimi jest powolnym procesem odbywającym się raz na miesiąc lub raz na kwartał. Dzięki zbudowaniu wspólnej platformy dla danych z infrastruktur OT i IT przedsiębiorstwo może natomiast śledzić wartości kluczowych wskaźników wydajności (KPI) w czasie rzeczywistym na podstawie aktualnych informacji pochodzących z obu tych środowisk. Na bazie takich aktualnych wartości można szybciej reagować na zmiany sytuacji rynkowej, na przykład ostrzegając menedżerów produktów o gwałtownie rosnącym koszcie surowców, który istotnie wpływa na marże zysku. Korzyści ze wspomnianej integracji odnoszą zresztą menedżerowie z obu stron, ponieważ uzyskują dostęp do danych w kontekście całego przedsiębiorstwa oraz możliwości współpracy w ramach obu infrastruktur OT i IT.

Połączenie ze sobą infrastruktur OT i IT ma również istotny wpływ na bezpieczeństwo.

- **Zwiększona powierzchnia ataku.** Połączenie ze sobą infrastruktur OT i IT naraża każdą z nich na ataki prowadzone za pośrednictwem punktów końcowych drugiej infrastruktury. Stosunkowo słabo zabezpieczone urządzenia OT, takie jak zawory, pompy, czujniki, zamki elektroniczne, termostaty i roboty, stają się potencjalnymi punktami dostępu do infrastruktury IT. Alternatywnie, cyberprzestępcy mogą atakować krytyczne obiekty użyteczności publicznej, takie jak sieci elektryczne lub systemy transportowe, za pośrednictwem sieci komórkowej jako punktu dostępu.
- **Zwiększona złożoność.** Środowiska sieci OT są złożone i zazwyczaj wymagają monitorowania i zabezpieczania od 50 do 500 urządzeń różnych producentów. Złożoność ta utrudnia zapewnienie odpowiedniej widoczności i wiąże się z wyzwaniami kadrowymi, ponieważ każde urządzenie przechowuje własne dane i ma szczególne potrzeby i wymagania w zakresie konfiguracji zabezpieczeń.
- **Zaawansowane metody włamań.** Podłączenie infrastruktury OT do Internetu naraża ją na działanie wielu starszych rodzajów złośliwego oprogramowania, które jest łatwo neutralizowane przez stosowane w środowisku IT mechanizmy bezpieczeństwa oparte na rozpoznawaniu sygnatur, ale może być skuteczne w przypadku słabo zabezpieczonych urządzeń przemysłowych. Cyberprzestępcy często atakują niewielką liczbę komputerów za pomocą starego złośliwego oprogramowania, a gdy takie działanie zakończy się powodzeniem, wykorzystują je do przeprowadzania ataków na dużą skalę. Taki „recykling złośliwego oprogramowania" pozwala atakującym zmaksymalizować wartość posiadanego złośliwego oprogramowania przed zainwestowaniem w bardziej zaawansowane środki służące do włamań do sieci OT[2].

„Zwiększająca się powierzchnia ataku sprawia, że podejmujemy więcej środków ostrożności, aby chronić nasze systemy baz danych".

– respondent w badaniu dla sektora energetycznego

„Wskutek zwiększonej złożoności środowiska sieciowego poświęcamy więcej czasu na kwestie związane z cyberbezpieczeństwem kosztem operacji produkcyjnych".

– respondent w badaniu dla sektora produkcji przemysłowej

„Zaawansowane metody włamań sprawiają, że spędzamy o wiele więcej godzin tygodniowo na działaniach z zakresu poprawy bezpieczeństwa".

– respondent w badaniu dla sektora opieki zdrowotnej

Metodyka badania

Niniejszy raport zatytułowany „Dyrektorzy operacyjni a cyberbezpieczeństwo infrastruktury OT" opiera się na badaniu przeprowadzonym wśród dyrektorów operacyjnych. Nasi respondenci reprezentują przedsiębiorstwa zatrudniające ponad 2500 pracowników w różnych sektorach, z czego ponad połowa (59%) w sektorze produkcji przemysłowej, a ponad jedna czwarta (27%) — w sektorze energetycznym i użyteczności publicznej.

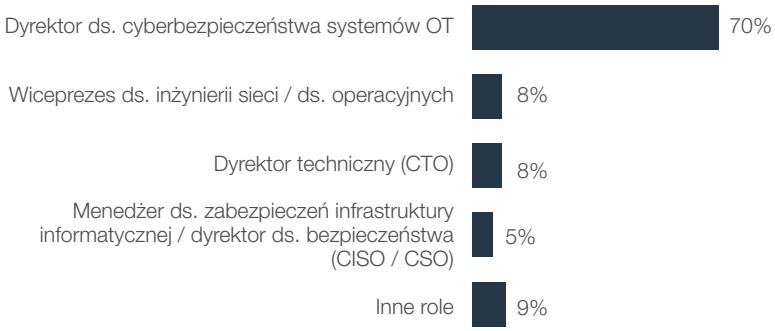
Nasze działania analityczne zasadzały się na następujących kwestiach. Po pierwsze w badaniu użyto danych ankietowych w celu zidentyfikowania kilku bieżących tendencji trendów dotyczących roli dyrektora operacyjnego w zabezpieczaniu posiadanej przez przedsiębiorstwo infrastruktury OT. Następnie poddano analizie swobodne odpowiedzi, których respondenci udzielali na kilka otwartych pytań dotyczących kluczowych wyzwań, i na tej podstawie stworzono obraz tego, co wpływa na ich codzienną pracę. Na koniec bardziej szczegółowo przeanalizowano dostępne dane, aby zidentyfikować podgrupę przedsiębiorstw, które w ciągu ostatnich 12 miesięcy doświadczyły maksymalnie trzech włamań, oraz drugą podgrupę przedsiębiorstw, które w ciągu ostatnich 12 miesięcy doświadczyły co najmniej czterech włamań. Po porównaniu ze sobą obu tych grup wskazano najlepsze praktyki, które najprawdopodobniej będą stosowane przez dyrektorów operacyjnych najwyższego szczebla w kontekście cyberbezpieczeństwa infrastruktury OT.

Tendencje w zakresie cyberbezpieczeństwa systemów OT dotyczące dyrektorów operacyjnych

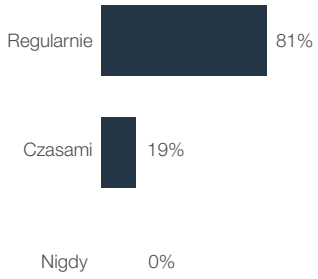
Tendencja: dyrektor operacyjny jest odpowiedzialny za cyberbezpieczeństwo systemów OT i wpływa na strategię bezpieczeństwa przedsiębiorstwa.

Ponad 75% respondentów uważa, że zapewnienie cyberbezpieczeństwa systemów OT leży w gestii dyrektora operacyjnego, z czego 70% wskazuje, że taki dyrektor operacyjny podlega dyrektorowi ds. cyberbezpieczeństwa systemów OT, a kolejne 8% — wiceprezesowi ds. inżynierii sieci / ds. operacyjnych (Rys. 1). Zdecydowana większość (81%) dyrektorów operacyjnych regularnie uczestniczy w procesie formułowania strategii cyberbezpieczeństwa, podczas gdy pozostała część dyrektorów operacyjnych uczestniczy w takim procesie rzadko (Rys. 2).

Zważywszy, że infrastruktury OT i IT są w wielu przedsiębiorstwach nadal od siebie oddzielone, ma sens fakt, że dyrektor operacyjny jest odpowiedzialny za całą infrastrukturę OT, w tym za wspomniane bezpieczeństwo. Jak pokazuje niniejszy raport, rola dyrektora operacyjnego w zapewnieniu cyberbezpieczeństwa ewoluuje i chociaż można podejrzewać, że jego obowiązki w kontekście zapewnienia cyberbezpieczeństwa są coraz mniejsze, w rzeczywistości jest dokładnie odwrotnie.



Rys. 1: Odpowiedzialność za cyberbezpieczeństwo systemów OT w przedsiębiorstwie.



Rys. 2: Udział dyrektorów operacyjnych w podejmowaniu decyzji dotyczących strategii cyberbezpieczeństwa.

Tendencja: Posiadana przez dyrektora operacyjnego kompetencja w zakresie bezpieczeństwa jest wyraźnie widoczna w przedsiębiorstwie.

Nie jest zaskoczeniem, że przedsiębiorstwa zwracają coraz większą uwagę na bezpieczeństwo infrastruktury OT. Ponad połowa (54%) dyrektorów operacyjnych uważa, że stan bezpieczeństwa infrastruktury OT odgrywa istotną rolę w ogólnej ocenie zagrożeń dla przedsiębiorstwa, podczas gdy ponad jedna trzecia (35%) z nich uważa, że rola ta jest umiarkowana (Rys. 3). Tymczasem zarządzanie ryzykiem stanowi największe wyzwanie stojące przed dyrektorami operacyjnymi, co omówiono poniżej w części „Największe wyzwania dla dyrektorów operacyjnych".

O rosnącym nacisku na bezpieczeństwo świadczy również fakt, że dyrektorzy operacyjni przywołują szeroką gamę wskaźników związanych z bezpieczeństwem i zgodnością z przepisami, takich jak wyniki testów włamaniowych (70%), liczba przypadków naruszenia bezpieczeństwa (65%), zaplanowane oceny stanu bezpieczeństwa (62%) oraz mierniki zgodności z normami bezpieczeństwa i przepisami branżowymi (odpowiednio 59% i 57%) (Rys. 4).

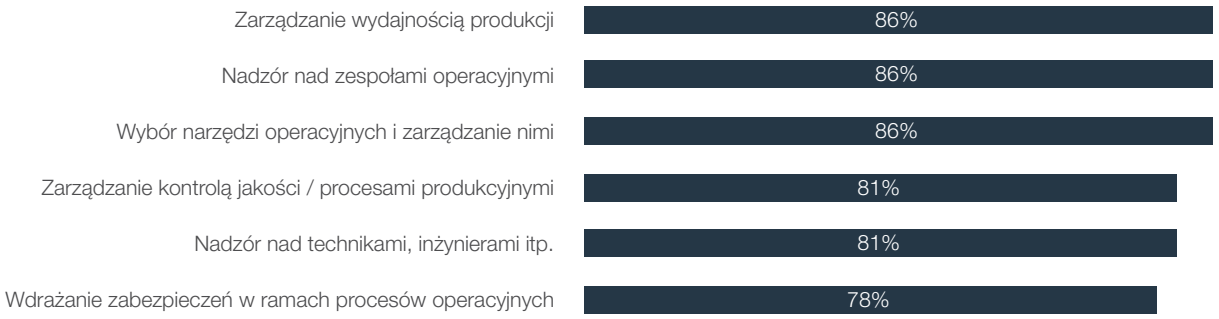
Rys. 3. Wpływ stanu bezpieczeństwa infrastruktury OT na ogólną ocenę ryzyka.

Rys. 4: Przywołane mierniki cyberbezpieczeństwa systemów OT.

Tendencja: Na dyrektorach operacyjnych spoczywa nie tylko typowa odpowiedzialność za działania operacyjne, ale również znaczna odpowiedzialność za zapewnienie bezpieczeństwa.

Głównym zadaniem dyrektorów operacyjnych jest zapewnienie sprawnego działania przedsiębiorstwa i kontrola kosztów operacyjnych. 86% dyrektorów operacyjnych bezpośrednio odpowiada za zarządzanie wydajnością produkcji, nadzorowanie zespołów operacyjnych (86%), wybór narzędzi operacyjnych i zarządzanie nimi (86%), zarządzanie kontrolą jakości (81%) oraz nadzorowanie techników i inżynierów (81%). Wszystkie te obszary mieszczą się w ramach tradycyjnej roli dyrektora operacyjnego polegającej na wspomnianym już zapewnieniu sprawnego działania przedsiębiorstwa i kontroli kosztów operacyjnych.

Ponadto przedsiębiorstwa oczekują, że na potrzeby zabezpieczenia infrastruktury produkcyjnej dyrektor operacyjny będzie współpracować z menedżerem ds. zabezpieczeń infrastruktury informatycznej i innymi dyrektorami ds. bezpieczeństwa. Ponad trzy czwarte (78%) respondentów stwierdziło, że odpowiada za zabezpieczenie procesów operacyjnych, mimo że często ma w tym zakresie niewielkie przeszkolenie i doświadczenie (Rys. 5). Tematem powracającym w niniejszym opracowaniu jest potrzeba zrównoważenia rosnącej odpowiedzialności dyrektorów operacyjnych za bezpieczeństwo z ich tradycyjnymi obowiązkami w zakresie działań operacyjnych.



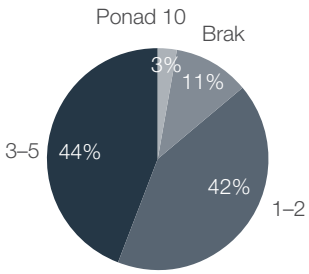
Rys. 5: Bezpośrednia odpowiedzialność dyrektorów operacyjnych.

Tendencja: Większość dyrektorów operacyjnych doświadczyła w minionym roku wielu włamań, w wyniku których przedsiębiorstwa odniosły poważne szkody.

Dla uczestniczących w tym badaniu dyrektorów operacyjnych wielokrotne włamania są regułą, a nie wyjątkiem. Tylko 11% dyrektorów operacyjnych nie zgłosiło żadnych włamań w ciągu ostatnich 12 miesięcy. Spośród dyrektorów operacyjnych, którzy mieli do czynienia z włamaniami, 42% doświadczyło maksymalnie dwóch włamań, a 47% — co najmniej trzech włamań (Rys. 6). Rodzaje ataków były bardzo zróżnicowane: w 69% przypadków miało miejsce użycie złośliwego oprogramowania, a w ponad 41% przypadków doszło do ataków przy użyciu oprogramowania szpiegującego lub ataków phishingowych (Rys. 7).

Spośród respondentów, którzy mieli do czynienia z włamaniami, w 81% przypadków doszło do przestojów w funkcjonowaniu infrastruktury OT, które negatywnie wpłynęły na prowadzoną działalność (53%), zagroziły bezpieczeństwu fizycznemu (31%) lub spowodowały spadek przychodów (28%). Częstość występowania tego rodzaju szkód związanych z naruszeniami bezpieczeństwa infrastruktury IT jest natomiast dość niska: jedynie nieco ponad jedna czwarta respondentów (28%) utraciła dane krytyczne dla działalności przedsiębiorstwa i tylko 22% respondentów ucierpiało z powodu narażenia na szwank reputacji marki (Rys. 8).

Warto porównać te wyniki z wynikami przeprowadzonego niedawno przez Fortinet badania, w którym 40% menedżerów ds. zabezpieczeń infrastruktury informatycznej zgłosiło awarie, które miały negatywny wpływ na produktywność, wartość marki i przychody[3]. To niekorzystne dla infrastruktury OT porównanie mogłoby pomóc w interpretacji innych ustaleń zawartych w tym raporcie, na przykład większej widoczności kwestii bezpieczeństwa infrastruktury OT oraz uwzględnienia stanu bezpieczeństwa infrastruktury OT w ogólnej ocenie ryzyka.



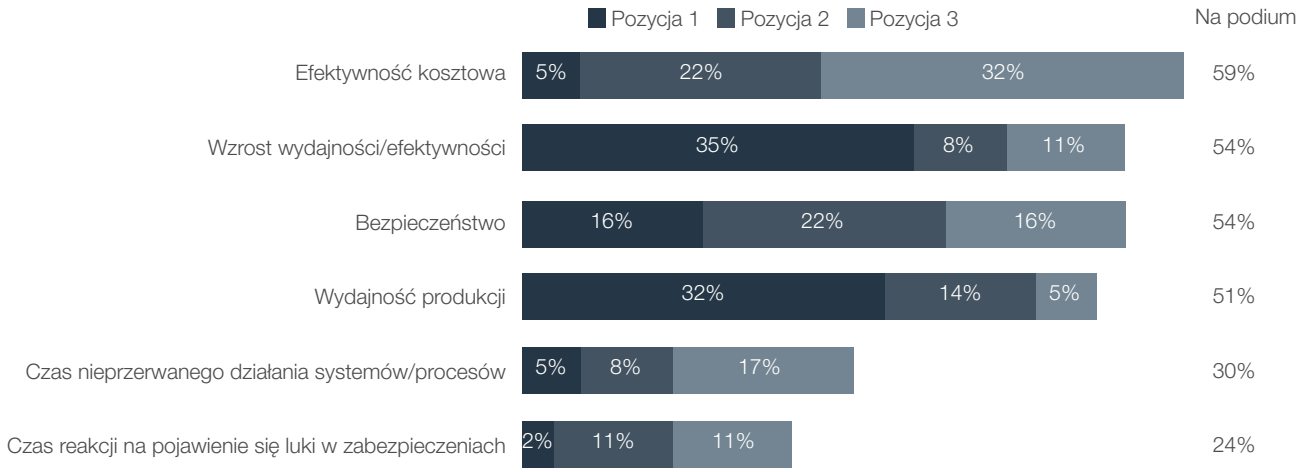
Rys. 6: Liczba włamań w ciągu ostatniego roku.

Rys. 7. Rodzaje odnotowanego włamania do systemu.

Rys. 8: Skutki włamań dla prowadzonej działalności.

Tendencja: Przestoje mogą mieć negatywny wpływ na wartości wskaźników mierzących sukces dyrektora operacyjnego.

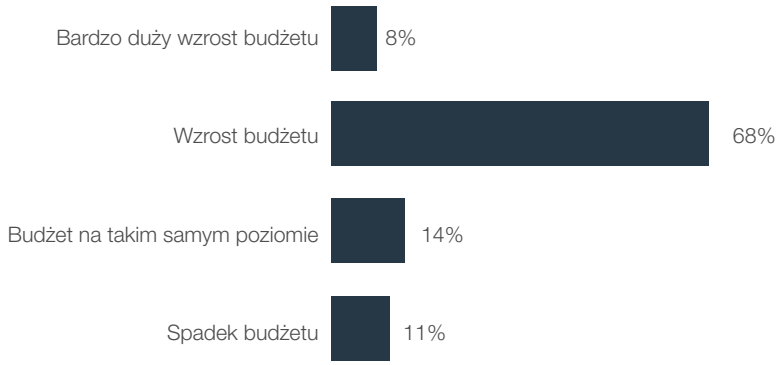
Przestoje nie tylko negatywnie wpływają na działalność przedsiębiorstwa, ale również mogą mieć bezpośredni wpływ na karierę dyrektorów operacyjnych, utrudniając im uzyskanie dobrych wartości wskaźników sukcesu. Pięć najważniejszych mierników sukcesu w przypadku dyrektorów operacyjnych to efektywność kosztowa (59%), wzrost wydajności (54%), bezpieczeństwo (54%), wydajność produkcji (51%) oraz czas nieprzerwanego działania systemów/procesów (30%), a nieplanowany przestój może mieć negatywny wpływ na wszystkie te czynniki (Rys. 9).



Rys. 9. Czynniki sukcesu dla dyrektorów operacyjnych.

Tendencja: Dyrektorzy operacyjni spodziewają się wzrostu (czasami bardzo dużego) swoich budżetów na bezpieczeństwo w następnym roku.

Kolejną oznaką rosnącej świadomości przedsiębiorstw w kontekście ryzyka pojawienia się przypadków naruszenia bezpieczeństwa infrastruktury OT jest gotowość ścisłej kadry zarządzającej do zwiększenia nakładów na bezpieczeństwo infrastruktury OT. W 2019 r. 76% dyrektorów operacyjnych odnotowało wzrost swoich budżetów na bezpieczeństwo, przy czym co dziesiąty z nich uznał taki wzrost za *bardzo duży* (Rys. 10). Wyniki innego badania pokazały, że w 2019 r. budżety na bezpieczeństwo infrastruktury OT wzrosły średnio o 17,9%[4].



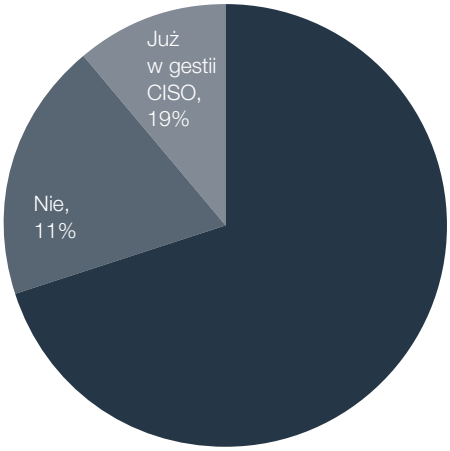
Rys. 10. Tendencje dotyczące budżetów dyrektorów operacyjnych na bezpieczeństwo za 2019 r.

Kadra kierownicza najwyższego szczebla, która zatwierdza wspomniane budżety, oczekuje, że dyrektor operacyjny zmniejszy liczbę włamań, zwiększy produktywność i zapewni większą zgodność z przepisami. W odpowiedzi na te oczekiwania większość dyrektorów operacyjnych stosuje mierniki włamań (68%), skutków finansowych (68%), wykrytych i zablokowanych luk w zabezpieczeniach (62%) i zredukowanych/unikniętych kosztów (57%) oraz mierzy wymierne efekty zarządzania ryzykiem (51%) (Rys. 11). Więcej informacji na temat sposobów, w jakie dyrektorzy zarządzający reagują na ryzyko, można znaleźć poniżej w części „Największe wyzwania dla dyrektorów operacyjnych".

Rys. 11. Stosowane i zgłoszone mierniki dotyczące cyberbezpieczeństwa.

Tendencja: Rola dyrektora operacyjnego ciągle się zmienia w miarę jak główna odpowiedzialność za bezpieczeństwo infrastruktury OT jest przenoszona na menedżera ds. zabezpieczeń infrastruktury informatycznej.

Zdecydowana większość (89%) respondentów oczekuje, że w następnym roku menedżer ds. zabezpieczeń infrastruktury informatycznej przejmie główną odpowiedzialność za bezpieczeństwo infrastruktury OT (Rys. 12). Wynika to najprawdopodobniej z połączenia ze sobą sieci OT i IT, ponieważ przedsiębiorstwa konsolidują działania dotyczące bezpieczeństwa infrastruktury, aby lepiej zarządzać ogólnym ryzykiem. Zmiana ta nie powinna być zatem postrzegana jako zmniejszenie odpowiedzialności COO za cyberbezpieczeństwo, która może i tak wzrosnąć w miarę wdrażania coraz większej liczby zabezpieczeń w sieci OT. Oczekiwany wzrost liczby inteligentnych urządzeń przemysłowych również zwiększy presję na dyrektora operacyjnego w kontekście zapewnienia bezpieczeństwa.



Rys. 12. Przeniesienie w ciągu jednego roku obowiązków w zakresie cyberbezpieczeństwa systemów OT w gestię menedżera ds. zabezpieczeń infrastruktury informatycznej.

Tendencja: Dyrektor operacyjny jest bardziej niż menedżer ds. zabezpieczeń infrastruktury informatycznej skłonny do śledzenia i zgłaszania kluczowych wskaźników cyberbezpieczeństwa.

Jak już wspomniano, w większości przedsiębiorstw menedżer ds. zabezpieczeń infrastruktury informatycznej wkrótce przejmie główną odpowiedzialność za bezpieczeństwo infrastruktury OT. Tendencja ta oznacza, że obie te osoby będą musieć współpracować w celu zapewnienia cyberbezpieczeństwa infrastruktury OT i dla obu będzie to nowość. Porównanie ich zachowań w kontekście śledzenia i zgłaszania wskaźników cyberbezpieczeństwa ujawnia jednak pewne interesujące podobieństwa i różnice.

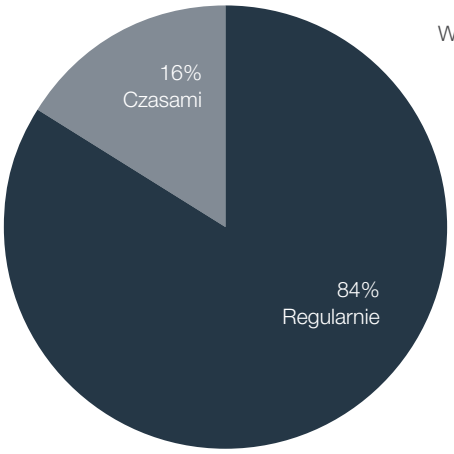
Przede wszystkim dyrektorzy operacyjni są znacznie bardziej niż menedżerowie ds. zabezpieczeń infrastruktury informatycznej skłonni do śledzenia wartości czterech najważniejszych wskaźników cyberbezpieczeństwa: włamania wykryte i zneutralizowane (68% do 59%), skutki finansowe (68% do 46%), wykryte i zablokowane luki w zabezpieczeniach (62% do 44%) oraz zredukowane/uniknięte koszty (57% do 51%) (Rys. 13). Wydaje się to może sprzeczne z intuicją, nabiera jednak większego sensu wówczas, gdy uwzględni się fakt, że podstawowa odpowiedzialność dyrektora operacyjnego obejmuje zarządzanie procesami produkcyjnymi, które z natury rzeczy są funkcją opartą na danych. Menedżer ds. zabezpieczeń infrastruktury informatycznej zajmujący się infrastrukturą OT powinien zatem zacząć posługiwać się językiem biznesowym, przy pomocy którego dyrektorzy operacyjni oceniają ogólną skuteczność inicjatyw w zakresie bezpieczeństwa. Podejście takie również pozwoli menedżerom ds. zabezpieczeń infrastruktury informatycznej na bardziej efektywną komunikację z innymi członkami najwyższego szczebla kierownictwa takimi jak dyrektor operacyjny, dyrektor finansowy i cała rada dyrektorów[5].

Największa różnica jest widoczna w kontekście wskaźnika skutków finansowych, który jest śledzony przez ponad dwie trzecie (68%) dyrektorów operacyjnych, ale mniej niż połowę (46%) menedżerów ds. zabezpieczeń infrastruktury informatycznej. Wynika to najprawdopodobniej ze znaczenia, jakie przedsiębiorstwa przywiązują do marży zysku, na którą silny wpływ mają czynniki będące pod kontrolą dyrektora operacyjnego. Zważywszy, że dyrektorzy operacyjni często mają większe doświadczenie w śledzeniu skutków finansowych, menedżerowie ds. zabezpieczeń infrastruktury informatycznej powinni skorzystać z ich doświadczeń i położyć większy nacisk na kwestie finansowe.

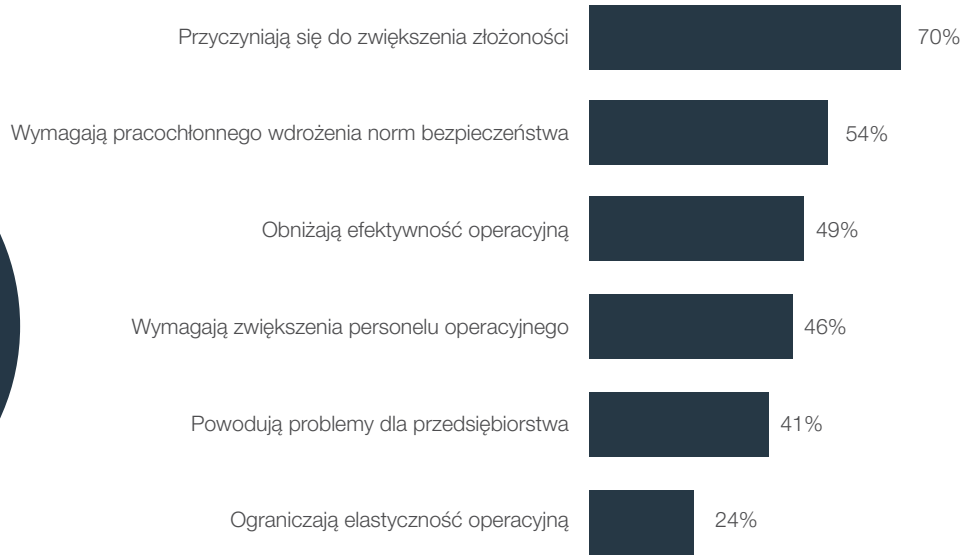
Rys. 13. Porównanie śledzonych i zgłoszonych w badaniu wskaźników (COO a CISO)

Tendencja: Dyrektorzy operacyjni muszą zarządzać złożonością, ponieważ podejmują decyzje dotyczące cyberbezpieczeństwa.

Zdecydowana większość (84%) dyrektorów operacyjnych regularnie uczestniczy w podejmowaniu decyzji zakupowych z zakresu cyberbezpieczeństwa infrastruktury OT, podczas gdy pozostali (16%) uczestniczą w podejmowaniu takich decyzji jedynie czasami (Rys. 14). Dyrektorzy operacyjni zgłaszają, że decyzje te mogą mieć negatywne skutki w kontekście złożoności (70%), norm bezpieczeństwa (54%) i efektywności operacyjnej (49%) (Rys. 14). Podobnie jak w wielu innych obszarach, dyrektorzy operacyjni podejmujący decyzje zakupowe muszą zachować równowagę między zapewnieniem bezpieczeństwa a zagwarantowaniem efektywności operacyjnej. Omówienie wpływu złożoności na ryzyko dla przedsiębiorstwa można znaleźć poniżej w części „Największe wyzwania dla dyrektorów operacyjnych”.



Rys. 14. Udział dyrektora operacyjnego w podejmowaniu decyzji zakupowych dotyczących infrastruktury OT.



Rys. 15. Negatywny wpływ rozwiązań w zakresie cyberbezpieczeństwa na sukces zawodowy dyrektora operacyjnego.

Najważniejsze wyzwania dla dyrektora operacyjnego

Na potrzeby naszego badania poprosiliśmy respondentów o udzielenie odpowiedzi na kilka otwartych pytań dotyczących najważniejszych wyzwań zawodowych. Udzielone odpowiedzi były bardzo zróżnicowane, ale skategoryzowaliśmy je tak, aby poznać najważniejsze dla dyrektorów operacyjnych kwestie dotyczące infrastruktury OT. Wspomniane pytania wiązały się z trzeba ogólnymi tendencjami w zakresie bezpieczeństwa: zaawansowanymi metodami włamań, zwiększającą się powierzchnią ataku i rosnącą złożonością.

Wyzwanie: Dla dyrektorów operacyjnych największym wyzwaniem w kontekście zaawansowanych metod włamań jest „nadążanie za tempem zmian”.

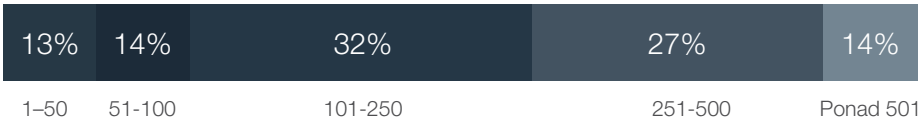
Oprócz zarządzania ryzykiem, 61% dyrektorów operacyjnych zgłasza, że zaawansowane metody włamań utrudniają nadążanie za tempem zachodzących zmian (Rys. 17). Może to wynikać z faktu, że wiele przedsiębiorstw łączy odizolowaną do tej pory infrastrukturę OT ze światem zewnętrznym. W rezultacie staje się ona celem zmasowanego ataku prowadzonego za pomocą starszych pakietów złośliwego oprogramowania. Pakiety te nie stanowią większego zagrożenia dla infrastruktury IT, mogą jednak siać spustoszenie w niektórych obszarach infrastruktury OT, które nie są chronione mechanizmami opartymi na rozpoznawaniu sygnatur. Nie dziwi zatem fakt, że dyrektorzy operacyjni mają problemy z radzeniem sobie z tymi nowymi wyzwaniami.

Wyzwanie: Zwiększająca się powierzchnia ataku utrudnia dyrektorom operacyjnym zarządzanie ryzykiem, nadążanie za tempem zmian i zapobieganie włamaniom.

Uczestniczący w badaniu dyrektorzy operacyjni stwierdzili, że zwiększająca się powierzchnia ataku utrudnia im zarządzanie ryzykiem (65%), nadążanie za tempem zmian (48%) i wdrażanie zabezpieczeń przed włamaniami (26%) (Rys. 18). Nadążanie za tempem zmian to w tej części badania powracający motyw, który zajmuje drugie miejsce we wszystkich tych trzech obszarach.

Wyzwanie: Rosnąca złożoność zarządzania cyberbezpieczeństwem w istotny sposób zwiększa stres i obciążenia związane z pracą dyrektora operacyjnego.

Środowiska sieciowe OT stają się coraz bardziej złożone już ze względu na samą liczbę znajdujących się w nich urządzeń. W przypadku tego badania 87% respondentów zarządza co najmniej setką urządzeń, podczas gdy 41% ma pod opieką ponad 250 urządzeń (Rys. 16). Taki wzrost liczby urządzeń przyczynia się do wzrostu złożoności, zwłaszcza w zakresie aktualizacji i obsługi.



Rysunek 16: Liczba eksploatowanych urządzeń.

Prawie jedna trzecia (32%) respondentów twierdzi, że złożoność zarządzania systemami cyberbezpieczeństwa zwiększyła ich obciążenie pracą i w rezultacie podniosła poziom stresu. Prawie tyle samo respondentów (29%) twierdzi, że złożoność ta utrudnia również znalezienie wykwalifikowanej kadry, co wywiera większą presję na dyrektorach operacyjnych i niewątpliwie przyczynia się do zwiększenia ich obciążenia pracą i stresu zawodowego (32%) (Rys. 19).

„Stale zwiększająca się powierzchnia ataku nie daje spać po nocach kierownictwu najwyższego szczebla zajmującemu się sprawami z zakresu cyberbezpieczeństwa i działalności biznesowej”.

– panelista na konferencji National Cyber Security Alliance Summit[6]

Dyrektorzy operacyjni stoją zatem w obliczu poważnych wyzwań, próbując optymalnie łączyć swoje obowiązki w zakresie cyberbezpieczeństwa systemów OT z obowiązkami w zakresie zapewnienia odpowiedniej dostępności, wydajności i produktywności. Tendencja ta prawdopodobnie będzie się nasilać wraz z rosnącą liczbą urządzeń OT i coraz bardziej złożonym zarządzaniem infrastrukturą OT.

Rys. 17. Wyzwania dla dyrektorów operacyjnych wynikające z zaawansowanych metod włamań.

Rys. 18. Wyzwania dla dyrektorów operacyjnych wynikające ze zwiększenia się powierzchni ataku.

Rys. 19: Wyzwania dla dyrektorów operacyjnych wynikające ze zwiększonej złożoności.

Wyzwanie: Ogólnie rzecz biorąc, zarządzanie ryzykiem jest dla dzisiejszych dyrektorów operacyjnych największym wyzwaniem w zakresie cyberbezpieczeństwa.

Ryzyko związane z cyberbezpieczeństwem jest obecnie największym problemem dla przedsiębiorstw każdej wielkości. Spośród 1200 uczestniczących w niedawnym badaniu dyrektorów przedsiębiorstw 55% stwierdziło, że ryzyko to stanowi dla nich powód do pewnych lub bardzo dużych obaw[7].

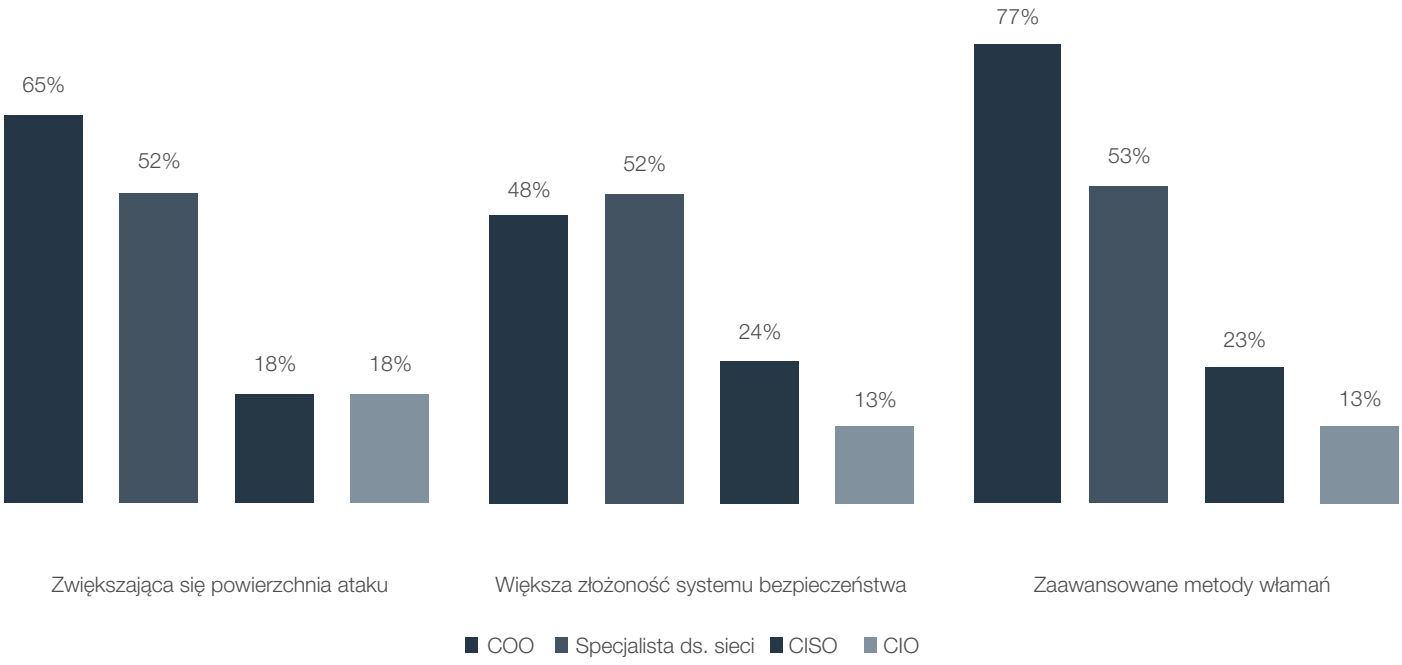
Analizując tę część badania całościowo, można zauważyć, że zarządzanie ryzykiem było wymieniane przez dyrektorów operacyjnych częściej niż jakiekolwiek inne wyzwanie: 77% dyrektorów wymieniało je w kontekście zaawansowanych metod włamań (Rys. 17), 65% — w kontekście zwiększonej powierzchni ataku (Rys. 18), a 48% — w kontekście wzrostu złożoności (Rys. 19). Obserwacja ta jest zgodna ze wcześniejszym stwierdzeniem, że stan bezpieczeństwa infrastruktury OT wpływa na ogólną ocenę ryzyka dla przedsiębiorstwa.

Aby zapewnić dodatkowy kontekst, w badaniu porównano wyniki badań dyrektorów operacyjnych z wynikami badań dyrektorów ds. informatycznych (CIO)[8], menedżerów ds. zabezpieczeń infrastruktury informatycznej (CISO)[9] oraz specjalistów ds. operacyjnych i inżynierii sieci[10] (Rys. 20). Na tej podstawie dokonano ciekawych obserwacji:

„Nasza instytucja radzi sobie ze zwiększoną złożonością, ucząc naszych pracowników proaktywnego zarządzania nowymi technologiami”.

– respondent w badaniu dla sektora energetycznego

- Więcej osób na stanowisku dyrektora operacyjnego uważa, że zaawansowane metody włamań stanowią wyzwanie dla zarządzania ryzykiem, niż ma to miejsce w przypadku osób na pozostałych stanowiskach. Wynika z tego, że dyrektorzy operacyjni są świadomi problemów stwarzanych przez stosunkowo słabo zabezpieczoną infrastrukturę OT i prawidłowo identyfikują tę sytuację jako stwarzającą ryzyko dla przedsiębiorstwa.
- Znacznie więcej dyrektorów operacyjnych i dyrektorów ds. inżynierii i operacji w sieci uznaje zarządzanie ryzykiem za największe wyzwanie w kontekście cyberbezpieczeństwa niż ma to miejsce w przypadku menedżerów ds. zabezpieczeń infrastruktury informatycznej i dyrektorów ds. informatycznych. Nie oznacza to jednak, że menedżerowie ds. zabezpieczeń infrastruktury informatycznej i dyrektorzy ds. informatycznych nie przejmują się zarządzaniem ryzykiem, ale raczej pokazuje ich priorytety (dla obu tych funkcji większe wyzwanie niż zarządzanie ryzykiem stanowi na przykład potrzeba szkoleń i rozwoju).
- Dyrektorzy ds. informatycznych najrzadziej wymieniają zarządzanie ryzykiem jako największe wyzwanie w zakresie cyberbezpieczeństwa. Może to wynikać z faktu, że dyrektorzy ci zazwyczaj skupiają się bardziej na dostępności i niezawodności niż na bezpieczeństwie. Innym możliwym wytłumaczeniem może być to, że dyrektorzy ci mają po prostu większe doświadczenie w zarządzaniu ryzykiem, jest zatem mniej prawdopodobne, aby uznawali takie czynniki, jak zwiększająca się powierzchnia ataku, za istotną przeszkodę we właściwym zarządzaniu ryzykiem.



Rys. 20: Odsetek respondentów wskazujących na wyzwania związane z zarządzaniem ryzykiem: dyrektor operacyjny (COO) / specjalista ds. sieci / menedżer ds. zabezpieczeń infrastruktury informatycznej (CISO).

Najlepsze praktyki dyrektorów operacyjnych najwyższego szczebla

W badaniu porównano odpowiedzi respondentów z dwóch podgrup na podstawie liczby zaistniałych włamań. Takie porównanie między respondentami z „najwyższego szczebla" a respondentami „najniższego szczebla" pozwoliło na identyfikację kilku najlepszych praktyk, które dyrektorzy operacyjni najwyższego szczebla są bardziej skłonni zastosować:

1. Dyrektorzy operacyjni najwyższego szczebla są o 168% bardziej skłonni do uznawania zmiany przepisów za główne wyzwanie do pokonania na drodze do odniesienia sukcesu oraz są o 45% bardziej skłonni do planowania przeglądów zgodności z przepisami.

Respondenci wymieniają szereg kwestii, które mają wpływ na ich pracę, dyrektorzy operacyjni najwyższego szczebla są jednak o 168% bardziej skłonni do uznawania zmiany przepisów za jedno z trzech głównych wyzwań mających wpływ na odniesienie sukcesu zawodowego. Z powiązanej obserwacji również wynika, że dyrektorzy operacyjni najwyższego szczebla są o 45% bardziej skłonni do przeprowadzania przeglądów zgodności z przepisami bezpieczeństwa, co prawdopodobnie wskazuje, że dyrektorzy ci reagują na wspomniane wyzwanie w sposób proaktywny.

2. Dyrektorzy operacyjni najwyższego szczebla są o 124% bardziej skłonni do pracy w przedsiębiorstwach, w których kadra kierownicza najwyższego szczebla ponosi ostateczną odpowiedzialność za cyberbezpieczeństwo.

Zważywszy na wzrost w przedsiębiorstwie świadomości omawianego wcześniej znaczenia bezpieczeństwa infrastruktury OT, nie dziwi fakt, że na im wyższym szczeblu jest przypisana odpowiedzialność za cyberbezpieczeństwo, tym mniej włamań odnotowuje się w danym przedsiębiorstwie. Jak już wcześniej wspomniano, wiele przedsiębiorstw powierza odpowiedzialność za cyberbezpieczeństwo systemów OT menedżerowi ds. zabezpieczeń infrastruktury informatycznej, który powinien odwdzięczyć się zmniejszeniem liczby włamań.

3. Dyrektorzy operacyjni najwyższego szczebla są o 79% bardziej skłonni do uznania wydajności produkcji za swój najważniejszy wskaźnik sukcesu.

Dyrektorzy operacyjni starają się dostosować swoje tradycyjne ukierunkowanie na działalność operacyjną do rosnących oczekiwań dotyczących ochrony infrastruktury OT. Dyrektorzy operacyjni najwyższego szczebla potrafią dotrzymać swoich zobowiązań w zakresie bezpieczeństwa bez zaniedbywania kwestii efektywności operacyjnej.

4. Dyrektorzy operacyjni najwyższego szczebla są o 49% bardziej skłonni do stosowania uwierzytelniania wieloskładnikowego.

Uwierzytelnianie wieloskładnikowe to sprawdzony sposób na poprawę stanu bezpieczeństwa przedsiębiorstwa. Z najnowszego badania wynika, że w celu zapewnienia sobie bezpieczeństwa osobistego specjaliści ds. bezpieczeństwa stosują w uzupełnieniu hasła przede wszystkim uwierzytelnianie wieloskładnikowe[11]. Najskuteczniejsi w kwestiach cyberbezpieczeństwa dyrektorzy operacyjni stosują wspomnianą praktykę i w rezultacie zapewniają coraz lepszą ochronę przed włamaniami.

5. Dyrektorzy operacyjni najwyższego szczebla są o 34% bardziej skłonni do śledzenia wzrostu produktywności jako miernika cyberbezpieczeństwa.

Dyrektorzy operacyjni są oceniani na podstawie produktywności, ich działania z zakresu bezpieczeństwa uwzględniają zatem zapewnienie odpowiedniej wydajności operacyjnej, szybciej wykonując zadania lub je automatyzując. Dyrektorzy operacyjni najwyższego szczebla są o 49% bardziej skłonni do śledzenia skutków finansowych jako miernika cyberbezpieczeństwa.

Przedsiębiorstwa rutynowo oceniają swoich dyrektorów operacyjnych na podstawie ogólnych wyników finansowych. Nie dziwi zatem fakt, że dyrektorzy operacyjni najwyższego szczebla uwzględniają w swoich działaniach z zakresu cyberbezpieczeństwa śledzenie budżetu.

6. Dyrektorzy operacyjni najwyższego szczebla są o 34% bardziej skłonni do zgłaszania wyników testów penetracyjnych i włamaniowych osobie odpowiedzialnej za cyberbezpieczeństwo.

Obserwacja ta podkreśla znaczenie, jakie osoby odpowiedzialne za cyberbezpieczeństwo przywiązują do testów służących do odpowiedniego oszacowania ryzyka. Testy w sposób proaktywny identyfikują luki w zabezpieczeniach i wskazują obszary wymagające podjęcia działań naprawczych. Fakt, że dyrektorzy operacyjni najwyższego szczebla mają czas na takie testowanie, sugeruje, że dysponują oni dodatkowym personelem, który może zająć się bieżącą obsługą zadań związanych z bezpieczeństwem.

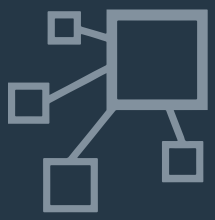
Podsumowanie

Z niniejszego badania wynika, że w kontekście cyberbezpieczeństwa systemów OT dyrektorzy operacyjni są zarówno bardzo widoczni w przedsiębiorstwie, jak i postawieni przed trudnym wyzwaniem związanym z zarządzaniem ryzykiem i zapewnieniem cyberbezpieczeństwa w uzupełnieniu swoich tradycyjnych obowiązków służbowych. Dyrektorzy operacyjni, którzy chcą poprawić swoje działania w zakresie zapewnienia bezpieczeństwa, mogą stosować następujące najlepsze praktyki wypracowane na przestrzeni lat:

Raportowanie i śledzenie kluczowych wskaźników w zakresie bezpieczeństwa i działalności operacyjnej

Przeprowadzanie regularnych testów bezpieczeństwa i przeglądów zgodności z przepisami

Skupienie się na skutkach finansowych podjętych środków cyberbezpieczeństwa



Inwestowanie w sprawdzone środki poprawy bezpieczeństwa takie jak uwierzytelnianie wieloskładnikowe

Źródła

[1] Barbara Filkins, Doug Wylie, „SANS 2019 State of OT/ICS Cybersecurity Survey", SANS Institute, 11 czerwca 2019 r.

[2] „Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems", Fortinet, 8 maja 2019 r.

[3] „The CISO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 26 kwietnia 2019 r.

[4] Barbara Filkins, Doug Wylie, „SANS 2019 State of OT/ICS Cybersecurity Survey", SANS Institute, 11 czerwca 2019 r.

[5] „The CFO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 11 września 2019 r.

[6] Doug Olenick, „Expanding Attack Surfaces and Difficulties Obtaining The Right People Worry NCSA panelists", SC Magazine, 16 października 2018 r.

[7] „Cyber Risk Is Top Concern for All, SMB Risks CISOs Need to Heed", The CISO Collective, 25 października 2019 r.

[8] „The CIO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 23 maja 2019 r.

[9] „The CISO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 26 kwietnia 2019 r.

[10] „Cybersecurity and the Network Engineering and Operations Leader: A Report on Current Priorities and Challenges", Fortinet, 4 września 2019 r.

[11] „The 2019 State of Password and Authentication Security Behaviors Report", Ponemon Institute, styczeń 2019 r.

FORTINET

www.fortinet.com

23 kwietnia, 2020 3:22 PM

report-FA-COO-and-cybersecurity_PL

323524-0-1-PL