05 (59) / 2026

CZASOPISMO RYNKU SECURITY

a&S POLSKA

www.aspolska.pl



RAPORT KTO POWIE: STOP?

W chwili próby wygrywają organizacje, które wcześniej przygotowały scenariusze działania i wielokrotnie ćwiczyły reakcję na sytuacje kryzysowe. Kto powinien zauważyć zagrożenie, kto je ocenić, a kto podjąć decyzję?

AGENTURA PROXY ZAGRAŻA OBIEKTOM PRZEMYSŁOWYM

Współczesne zagrożenia często wykraczają poza cyberataki i kwestie techniczne. Równie ważne są analiza zachowań oraz identyfikacja nietypowych zdarzeń w otoczeniu firmy.

PANIKA CZY PEŁNA MOBILIZACJA?

Zatrzymanie produkcji po ataku ransomware nie zawsze oznacza przegraną. Często jest jedynym rozsądnym rozwiązaniem. Warto sobie odpowiedzieć na kilka pytań, zanim pojawi się żądanie okupu.

20 zł
(w tym 8% VAT)

ISSN 2451-5175 05
9 772451 517703

WARSAW SECURITY SUMMIT

nowy wymiar bezpieczeństwa

6 listopada 2026

Crowne Plaza
The Hub Warsaw

WarsawSecuritySummit.pl

Kto powie STOP?

Bezpieczeństwo nigdy nie jest wyłącznie kwestią technologii. Skuteczna ochrona to nie tylko fizyczne zabezpieczenie obiektów i ludzi, ale przede wszystkim umiejętność podejmowania właściwych decyzji często pod presją czasu lub w obliczu olbrzymich finansowych strat. Kto powinien takie decyzje podejmować? Kto zauważy problem, kto oceni ryzyko i kto będzie miał odwagę powiedzieć „STOP" (str. 12), jeśli będzie to oznaczać np. zatrzymanie produkcji i olbrzymie straty? Kto zaryzykuje?

W naszym raporcie przyglądamy się granicom kompetencji i odpowiedzialności oraz temu, kto powinien zauważyć zagrożenie, kto je ocenić, a kto podjąć decyzję. Bo w sytuacji kryzysowej wygrywa nie ta organizacja, która ma najwięcej systemów bezpieczeństwa, lecz ta, która wypracowała i wielokrotnie przetestowała (!) odpowiednie procedury postępowania.

Granice bezpieczeństwa zakładu nie kończą się na jego murach. Coraz częściej „wychodzą" poza jego fizyczny teren. „Dron nad zakładem to już nie tylko incydent" (str. 24) pokazuje, że przestrzeń nad obiektem jest kolejną strefą wymagającą ochrony. Bezzałogowe statki powietrzne mogą służyć do obserwacji i pozyskiwania informacji, dlatego warto odpowiedzieć na pytania: co chronimy, jak szybko jesteśmy w stanie wykryć zagrożenie i kto decyduje o reakcji.

Jeszcze mniej oczywiste może być źródło zagrożenia opisywanego w materiale „Agentura proxy zagraża obiektom przemysłowym" (str. 30). Obserwacja bramy, pytania o dostawy czy próby pozyskania informacji od pracownika mogą być elementami większej operacji prowadzonej przez pośredników. Bezpieczeństwo wymaga więc nie tylko patrzenia na monitory systemów, ale również uważnego przyglądania się ludziom, ich zachowaniu, i temu, co dzieje się wokół organizacji. Zaufanie nie oznacza przecież braku kontroli.

To dotyczy także zdalnego serwisu (str. 36). To rozwiązanie wygodne i często niezbędne, ale oznacza umożliwienie dostępu do firmowej infrastruktury. Kluczowe pytanie brzmi: czy wiemy, kto ma dostęp do naszych systemów? I w jaki sposób z nich korzysta? Zdalny serwis jest wygodny, ale wymaga zachowania wyjątkowej czujności. Tak by wygoda nie skończyła się utratą kontroli.

A co dzieje się wtedy, gdy „STOP" trzeba powiedzieć po ataku ransomware? „Panika czy pełna mobilizacja? Krajobraz po ataku ransomware" (str. 56) pokazuje, że zatrzymanie produkcji nie zawsze oznacza porażkę. Jeśli nie mamy pewności czy dane, parametry procesu i wyniki kontroli jakości są wiarygodne, wyłączenie maszyn może być właśnie działaniem ochronnym. Dlatego proponujemy siedem pytań, na które warto odpowiedzieć, zanim pojawi się żądanie okupu.

W tym wydaniu pokazujemy również, że wiedzę o bezpieczeństwie najlepiej sprawdzać w praktyce. Relacja z jesiennej edycji Security BootCamp (str. 62) jest tego dobrym przykładem. Dwa dni pracy, zadań i wymiany doświadczeń pozwoliły uczestnikom spojrzeć na bezpieczeństwo nie z perspektywy pojedynczego rozwiązania, lecz całego procesu. Bo „STOP" nie jest słowem zarezerwowanym dla jednej osoby, działu czy systemu. To decyzja całej organizacji. Im wcześniej ustalimy, kto może ją podjąć, na jakiej podstawie i co wydarzy się później, tym większa szansa, że w sytuacji kryzysowej nie będziemy się zastanawiać, kto powinien zareagować, tylko po prostu zareagujemy.

O tym, jak zmienia się dziś krajobraz zagrożeń i jakie decyzje stoją przed osobami odpowiedzialnymi za bezpieczeństwo, będziemy również rozmawiać 6 listopada podczas Warsaw Security Summit w Warszawie. Do zobaczenia!

Redakcja

ZŁOTY PARTNER A&S POLSKA

BCS Linc Trusted Solutions VCS

SREBRNY PARTNER A&S POLSKA

HIKVISION

A&S POLSKA WYDANIE ONLINE: aspolska.pl

CZASOPISMO RYNKU SECURITY

a&S POLSKA

05 (59) / 2026



Spis treści

PRODUKTY NUMERU

8 **Najnowsze urządzenia z oferty firm:**
BCS, Hanwha Vision, Hikvision, Linc Polska, TP-Link

RAPORT

12 **Raport: Kto powie STOP?**

PRZEMYSŁ

22 **Inteligentny monitoring w przemyśle 4.0: technologie Hikvision wspierające bezpieczeństwo i sprawność operacyjną**
Michał Michniowski, Hikvision Polska

24 **Dron nad zakładem to już nie tylko incydent. Nowy wymiar ochrony infrastruktury krytycznej**

28 **Drony w ochronie. Technologia, która wspiera człowieka**
– wywiad z Michałem Kalinowskim, Dyrektorem Handlowym Usług Monitoringu i Techniki w Seris Konsalnet

30 **Agentura proxy zagraża obiektom przemysłowym**
Anna Grabowska-Siwiec

35 **Bezpieczeństwo fabryki to nie tylko zadanie ochrony. Kto naprawdę odpowiada za bezpieczeństwo zakładu produkcyjnego?**
Adrian Kosmalski, PZPO

36 **Zdalny serwis jest wygodny. Do czasu**
Monika Żuber-Mamakis

42 **Głos branży** – bezpieczeństwo sektora przemysłowego

REDAKCJA

ADRES REDAKCJI
a&s Polska
ul. Złoczowska 25
03-972 Warszawa
info@aspolska.pl
www.aspolska.pl

PREZES ZARZĄDU
Mariusz Kucharski

REDAKTOR NACZELNA
Marta Dynakowska

Z-CA RED. NACZELNEGO
Jan T. Grusznic

REDAKCJA
Monika Żuber-Mamakis

DZIAŁ REKLAMY
Iwona Krawiec

DZIAŁ PROJEKTÓW SPECJALNYCH
Jolanta A. Kucharska
Aleksandra Czapska

CENTRUM KOMPETENCJI
Jacek Grzechowiak

KOREKTA
Jolanta Kucharska

PROJEKT GRAFICZNY I SKŁAD
Marta Kołodziejak

WYDAWCA
SENS Group Sp. z o.o.
ul. Rondo ONZ 1
00-124 Warszawa
www.sensgroup.pl

Redakcja zastrzega sobie prawo skracania i redagowania nadesłanych tekstów. Tytuły i śródtytuły pochodzą od Redakcji. Opinie autorów nie muszą być tożsame z poglądami Redakcji. Za treść reklam i artykułów partnerów Redakcja nie odpowiada. Przedruki tekstów bez zgody Wydawcy są niedozwolone.

© Copyright by a&s Polska

BCS

MONITORING KTÓRY DZIAŁA



Obraz nieostry?
W monitoringu ważny jest każdy szczegół,
dlatego **warto postawić na** sprzęt, na którym możesz polegać.
Sprawdź **profesjonalne rozwiązania BCS**, które działają.

POLSKA MARKA BCS

bcs.pl
facebook.com/bcspl
instagram/bcskamery

CZASOPISMO RYNKU SECURITY

a&S POLSKA

05 (59) / 2026

Spis treści

RYNEK SECURITY

48 **Od pojedynczych systemów do ekosystemu. Jak zmienia się rynek security**
Ajax Systems

50 **Mobilny dostęp bez wymiany infrastruktury – nowe możliwości rozwiązań HID**
HID Global

CYBERBEZPIECZEŃSTWO

52 **Panika czy pełna mobilizacja? Krajobraz po ataku ransomware**
Monika Żuber-Mamakis

SERWIS INFORMACYJNY

58 **Jesienny Security BootCamp – dwa dni praktyki i wymiany doświadczeń**

62 **Informacje firmowe / nowości rynkowe**

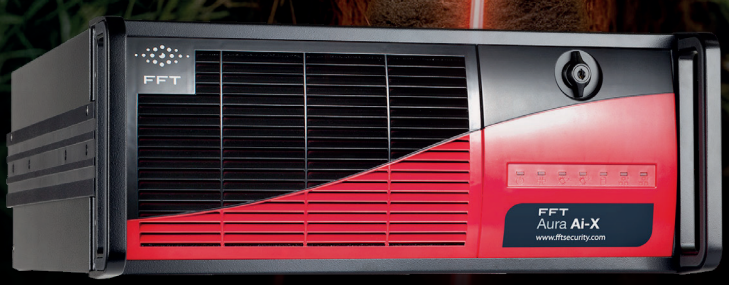


Future Fibre
TECHNOLOGIES

Wcześniejsza detekcja. Szybsza reakcja.

zaawansowana światłowodowa ochrona perymetryczna

- WYKRYWA PRÓBY WTARGNIĘCIA
- DETEKCJA W CZASIE RZECZYWISTYM
- DŁUGIE ODCINKI OCHRONY
- ODPORNOŚĆ NA ZAKŁÓCENIA



OFICJALNY DYSTRYBUTOR

Linc
Trusted Solutions

www.linc.eu

Prezentujemy najnowsze urządzenia z oferty firm

BCS, HANWHA VISION, HIKVISION, LINC POLSKA, TP-LINK











BCS

Kontrolery autonomiczne BCS – możliwości i integracja z BCS Line CMS Pro

Kontrola dostępu to nie tylko otwieranie drzwi za pomocą karty lub kodu. To również możliwość zarządzania uprawnieniami, monitorowania stanu przejść i zdalnego sterowania nimi. Kontrolery autonomiczne BCS łączą te funkcje w kompaktowych urządzeniach, które sprawdzają się zarówno przy pojedynczych wejściach, jak i w rozbudowanych systemach kontroli dostępu.



Model BCS-L-CKA--M1Z(2) integruje czytnik kart, klawiaturę i sterowanie zamkiem w jednej obudowie. Umożliwia także zastosowanie koincydencji karty i kodu, zwiększając poziom zabezpieczenia przejścia.

Z kolei nowy BCS--L-CKA-U2Z pozwala na konfigurację przez przeglądarkę internetową na komputerze lub smartfonie, bez konieczności bezpośredniego dostępu do urządzenia. Kontroler sygnalizuje również próby sabotażu oraz przekroczenie czasu odblokowania drzwi.

Alternatywą dla tradycyjnej karty dostępu może być smartfon. Czytnik BCS-L-CKRS-M2Z z Bluetooth umożliwia korzystanie z telefonu w zasięgu do 5 m, bezprzewodowo łącząc się z kontrolerem.

Możliwości systemu rozszerza integracja z BCS Line CMS Pro, wyposażonym w moduł kontroli dostępu. Administrator może centralnie zarządzać uprawnieniami, monitorować stan drzwi, przeglądać historię zdarzeń i zdalnie sterować przejściami. •

Więcej na: www.bcs.pl

HANWHA VISION

Inteligentne systemy wizyjne dla sektora produkcji

Rozwiązania VSS od Hanwha Vision, oparte na sztucznej inteligencji, pomagają zakładom przemysłowym w pokonywaniu codziennych problemów. Generują precyzyjne metadane i wnioski analityczne, które pozwalają automatyzować procedury *compliance*, zapobiegać awariom i budować solidny fundament dla podejmowania decyzji strategicznych.



Zaawansowana analityka wideo AI umożliwia operatorom identyfikację potencjalnych zagrożeń w czasie rzeczywistym, zanim doprowadzą one do tragedii. Błyskawiczna detekcja skraca czas reakcji służb ratunkowych i gwarantuje dokładną dokumentację incydentów, ułatwiając spełnienie rygorystycznych norm bezpieczeństwa.

Funkcje detekcji i śledzenia obiektów potrafią zidentyfikować wózki widłowe poruszające się w sposób stwarzający zagrożenie lub wjeżdżające do stref wykluczonych, ostrzegając o tym pobliskich pracowników.

Kamery systemu dozorowego potrafią również zweryfikować brak wymaganego sprzętu ochrony osobistej (PPE). Integracja VSS z systemami audio (PA/VA) lub wewnątrzzakładowymi platformami komunikacji umożliwia automatyczne nadawanie komunikatów przypominających o obowiązku noszenia kasków czy kamizelek odblaskowych.

Metadane wideo stanowią potężne źródło rzetelnej wiedzy o codziennych operacjach, „wąskich gardłach" infrastruktury, wydajności parku maszynowego i rotacji towaru. Kadra C-level może wykorzystać te zaawansowane dane analityczne do precyzyjnej optymalizacji grafików pracy i harmonogramów serwisowych, a także do planowania terminowości dostaw. •

Więcej na: www.hanwhavision.com/pl

RACS 5

roger
ASSA ABLOY

Nowoczesna transformacja bez rewolucji

Nowy system, ta sama instalacja.
Wykorzystaj istniejącą infrastrukturę i zyskaj nowe możliwości.

Maksymalne bezpieczeństwo. Minimalny wysiłek.
Protokół OSDP, szyfrowana komunikacja, Grade 4 – najwyższy poziom w standardzie.

Nowoczesność w praktyce: efektywność, komfort, elastyczność.
Wydajna baza SQL, bezpieczna identyfikacja mobilna i wielostanowiskowa architektura.

Jeden system. Pełna kontrola.
Zarządzaj dostępem, monitoruj i wizualizuj zintegrowane systemy bezpieczeństwa – wszystko z jednego miejsca.

Technologia, która myśli jak Ty.
Nowoczesny interfejs, intuicyjna obsługa, pełna kontrola.

Zainwestuj w przyszłość – dziś.
RACS 5 to długoterminowe wsparcie i rozwój.



Experience a safer
and more open world

HIKVISON

Od projektowania po obsługę urządzeń

Hik-Partner Pro i Hik-Partner Pro Designer to rozwiązania stworzone z myślą o instalatorach i integratorach systemów zabezpieczeń, które usprawniają codzienną pracę – od etapu projektowania po obsługę zainstalowanych urządzeń.



Hik-Partner Pro zapewnia dostęp do narzędzi wspierających zarządzanie projektami, urządzeniami i usługami, pomagając szybciej realizować zadania oraz sprawnie zarządzać infrastrukturą klientów. Platforma pozwala również korzystać z funkcji serwisowych i informacji o produktach w jednym miejscu.

Uzupełnieniem jest Hik-Partner Pro Designer – narzędzie przeznaczone do projektowania systemów monitoringu. Ułatwia dobór urządzeń, przygotowanie konfiguracji oraz tworzenie przejrzystych projektów dopasowanych do wymagań konkretnej instalacji. Dzięki integracji procesu projektowego z ekosystemem Hikvision instalator może sprawniej przejść od koncepcji do realizacji.

Połączenie obu narzędzi pozwala uporządkować pracę na kolejnych etapach inwestycji i ograniczyć czas poświęcany na zadania administracyjne. Dla profesjonalistów oznacza to wygodniejszy dostęp do informacji, sprawniejsze przygotowanie instalacji oraz lepszą organizację obsługi klientów. •

Więcej na: www.hikvision.com/pl/

LINC POLSKA

Ochrona przestrzeni powietrznej IK i obiektów wrażliwych

System detekcji bezzałogowych statków powietrznych SENID+ umożliwia pasywne wykrywanie komercyjnych dronów oraz dokładne określenie ich lokalizacji. Odbiera również dane Remote ID emitowane przez nowsze modele dronów. Ponadto system pokazuje lokalizację samolotów na podstawie danych ADS-B. Wszystko to zapewnia operatorowi pełniejszą świadomość sytuacyjną dotyczącą otaczającej go przestrzeni powietrznej.



W przypadku naruszenia wyznaczonej strefy chronionego obiektu operator otrzymuje informacje o latającym obiekcie i jego trasie lotu, a także – w zależności od dostępnych danych – o miejscu startu oraz lokalizacji operatora drona.

Informacja o lokalizacji osoby sterującej dronem jest szczególnie istotna, ponieważ pozwala szybciej zidentyfikować osobę odpowiedzialną za lot i podjąć odpowiednie działania w przypadku naruszenia strefy chronionej.

Sam system jest rozwiązaniem w pełni pasywnym – nie emituje własnych sygnałów i nie wymaga dodatkowych formalności związanych z jego użytkowaniem. Podłączenie odbywa się za pośrednictwem sieci Ethernet z wykorzystaniem PoE++, a dostęp do systemu uzyskuje się bezpośrednio z platformy.

SENID+ to rozwiązanie przeznaczone do ochrony wrażliwych środowisk, takich jak lotniska, zakłady karne czy infrastruktura krytyczna. Jego wdrożenie przebiega szybko, na zasadzie *plug & play*. Zaprojektowane i produkowane w Europie rozwiązanie oferuje sprawdzoną technologię, niezawodne łańcuchy dostaw oraz opłacalne wdrożenie, ograniczające ryzyko geopolityczne. •

Więcej na: www.linc.pl

TP-LINK

TP-Link rozszerza portfolio przełączników Omada Easy Managed

Dwa nowe modele zaprojektowano z myślą o nowoczesnych sieciach wielogigabitowych: ES210XPP-M2 i ES206XPP-M2. Oba urządzenia łączą porty 2,5G, obsługę PoE++ oraz bezpłatne, scentralizowane zarządzanie w chmurze za pośrednictwem Omada Central Essentials.

ES210XPP-M2 oferuje osiem portów RJ45 2,5 Gb/s z PoE++, port RJ45 10 Gb/s oraz slot SFP+ 10 Gb/s. Łączna moc zasilania PoE sięga 200 W, a pojedynczy port może dostarczyć do 90 W. Model sprawdzi się więc w bardziej wymagających instalacjach, np. z punktami dostępowymi Wi-Fi 7 czy systemami monitoringu.



Mniejszy ES206XPP-M2 wyposażono w pięć portów RJ45 2,5 Gb/s, w tym cztery porty PoE++, oraz slot SFP+ 10 Gb/s. Łączny budżet PoE wynosi do 120 W, a moc na pojedynczym porcie – do 90 W.

Oba przełączniki wspierają *Plug-and-Play*, VLAN, QoS, izolację portów, IGMP Snooping i automatyczne zapobieganie pętlom. W trybie autonomicznym dostępna jest także funkcja *PoE Auto Recovery*. Dzięki Omada Central Essentials administrator może monitorować i konfigurować urządzenia z poziomu przeglądarki lub aplikacji, bez dodatkowych opłat licencyjnych.

Metalowa, bezwentylatorowa konstrukcja zapewnia cichą pracę, a pięcioletnia gwarancja producenta zwiększa bezpieczeństwo inwestycji. To rozwiązania dla firm, które chcą szybko rozbudować sieć 2,5G i uprościć zarządzanie infrastrukturą bez rezygnacji z wydajności i elastyczności. Oba modele są już dostępne w sprzedaży na polskim rynku. •

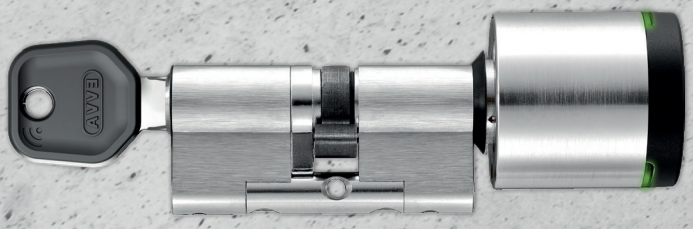
Więcej na: www.tp-link.com/pl/

EVVA
access to security

Witamy w świecie mechanicznych i elektronicznych systemów EVVA

Hybrydowy majstersztyk

Elektronika połączona z mechaniką w jednej wkładce - rzecz nie do podrobienia, ale do zamówienia. W EVVA!







Xesar i AirKey - elektroniczne systemy zamknięć

EVVA jest projektantem i producentem innowacyjnych elektronicznych systemów kontroli dostępu.

Arcydzieła mechaniki

Każdy system mechaniczny jest unikalny zarówno pod względem technologii jak i funkcji. Jednak wszystkie mają jedną wspólną cechę: najwyższą jakość marki.



www.evva.com



Kto powie STOP?

IT widzi sieć, automatyk proces, security ludzi i przestrzeń, serwisant zna urządzenia, a zarząd odpowiada za ciągłość biznesu. Bezpieczeństwo fabryki nie ma jednego właściciela. Co wtedy? Gdzie naprawdę przebiegają granice kompetencji, kto powinien reagować i kto może podjąć decyzję o zatrzymaniu produkcji? To codzienne dylematy zakładów produkcyjnych. W tym raporcie szukamy odpowiedzi i przekładamy je na konkretne rekomendacje.
Sprawdź, czy Twoja organizacja jest na taką sytuację przygotowana.

Na początek fabryka „POL-śrubex”. To fikcyjny zakład produkujący komponenty do sprzętu AGD. Fabryka pracuje w systemie zmianowym, a większość procesu jest zautomatyzowana. Linie produkcyjne korzystają ze sterowników PLC, stacji operatorskich i systemów połączonych z zakładową siecią OT. Część urządzeń jest serwisowana przez zewnętrznych dostawców, którzy w określonych sytuacjach mogą uzyskiwać dostęp zdalny.

Opisane poniżej zdarzenie nie jest rekonstrukcją rzeczywistego ataku.
To scenariusz zbudowany z typowych problemów i zależności występujących w środowiskach przemysłowych.

8:11 Do strefy technicznej wchodzi serwisant firmy obsługującej jedną z maszyn. Wykonuje zaplanowane prace przy urządzeniu i korzysta z własnego laptopa.

8:54 Serwisant kończy pracę i opuszcza teren zakładu. Konto umożliwiające zdalny dostęp do urządzenia pozostaje aktywne.

9:19 Automatyk zauważa niewielką, ale nietypową zmianę jednego z parametrów procesu. Linia nadal pracuje, a wartości mieszczą się w dopuszczalnym zakresie.

9:21 System monitorowania sieci rejestruje nietypową komunikację w środowisku OT. Informacja trafia do IT/SOC.

9:23 Operator linii zgłasza, że urządzenie reaguje inaczej niż zwykle. Parametr procesu ponownie się zmienia.

9:28 IT rekomenduje ograniczenie komunikacji z podejrzanym systemem. Automatyk ostrzega, że gwałtowne odłączenie urządzenia może wpłynąć na proces technologiczny.

9:32 Do analizy włącza się security. Sprawdzane są dane z kontroli dostępu, monitoring oraz informacje dotyczące porannej wizyty serwisanta.

9:35 Potwierdza się, że serwisant opuścił fabrykę ponad pół godziny wcześniej. Jego konto serwisowe nadal jest jednak aktywne i wykorzystywane do komunikacji z systemem.

9:41 Firma serwisowa potwierdza, że jej technik nie prowadzi żadnej zdalnej sesji.

9:46 Nietypowa komunikacja ustaje. Nie wiadomo jednak, czy coś dzieje się w tle i czy można nadal ufać systemowi sterowania.

9:52 Po konsultacji IT, OT i produkcji zapada decyzja o kontrolowanym zatrzymaniu części procesu.

Czy to była dobra decyzja? Czy wnioski wyciągnięto dostatecznie szybko? Kto właściwie powinien powiedzieć „STOP”?

Ilustracje: Marta Kołodziejak / A&S AI Studio

W nowoczesnej fabryce granica między bezpieczeństwem fizycznym, cyberbezpieczeństwem i bezpieczeństwem procesu coraz bardziej się zaciera. System kontroli dostępu jest połączony z siecią, monitoring działa na serwerach, maszyny komunikują się z systemami informatycznymi przedsiębiorstwa, a zewnętrzny serwisant może zdalnie łączyć się z urządzeniem, którego awaria zatrzyma całą produkcję. Jednocześnie odpowiedzialność pozostaje podzielona pomiędzy ludzi, którzy pracują w różnych strukturach organizacyjnych, korzystają z innych narzędzi i inaczej definiują ryzyko.

Kierownik IT może odciąć urządzenie od sieci. Automatyk wie, czy takie odcięcie nie zagrozi procesowi technologicznemu. Security manager sprawdzi, kto fizycznie miał dostęp do infrastruktury. Utrzymanie ruchu będzie chciało jak najszybciej przywrócić produkcję. Integrator zna konfigurację systemu lepiej niż część pracowników zakładu. Zarząd patrzy natomiast na skutki: bezpieczeństwo ludzi, ciągłość działania, odpowiedzialność prawną i każdą godzinę przestoju. Problem zaczyna się wtedy, gdy wszyscy odpowiadają za bezpieczeństwo, ale każdy za jego inny fragment.

Dlatego odporność fabryki nie zależy już wyłącznie od jakości firewalli, kamer, kontroli dostępu czy zabezpieczeń sterowników PLC. Coraz częściej zależy od czegoś znacznie mniej widowiskowego: od tego, czy organizacja wcześniej ustaliła:

- **kto ma zauważyć incydent,**
- **kto ma połączyć informacje z kilku systemów,**
- **kto podejmuje decyzję,**
- **kto w krytycznej chwili może zatrzymać linię produkcyjną.**

Technologie przemysłowe połączyły się szybciej niż struktury organizacyjne

Łatwo powiedzieć, kto odpowiada za działające kamery albo kto administruje siecią komputerową. Znacznie trudniej odpowiedzieć na pytanie, kto jest właścicielem ryzyka w sytuacji, kiedy cyberincydent zaczyna wpływać na fizyczny proces produkcji. National Institute of Standards and Technology zwraca uwagę, że systemy OT należy zabezpieczać z uwzględnieniem ich szczególnych wymagań dotyczących wydajności, niezawodności i przede wszystkim bezpieczeństwa procesu. Do OT zalicza przy tym nie tylko klasyczne systemy sterowania przemysłowego, ale także m.in. systemy automatyki budynkowej czy kontroli dostępu. Granica między światem „informatycznym"a „fizycznym" jest więc już znacznie mniej oczywista, niż sugerowałby schemat organizacyjny przedsiębiorstwa.

SECURITY MANAGER: widzi ludzi i przestrzeń, ale czy widzi proces?

Dla security managera fabryka jest przede wszystkim przestrzenią, którą trzeba chronić. Kto może wejść na teren zakładu? Kto ma dostęp do stref technicznych? Czy osoba poruszająca się po hali ma właściwe uprawnienia? Co pokazują kamery? Czy drzwi do serwerowni, sterowni albo szafy automatyki zostały otwarte? Czy zewnętrzny serwisant rzeczywiście przebywał tylko w miejscu, do którego został skierowany?

Jeżeli ktoś podłączy nieautoryzowane urządzenie do infrastruktury, wykorzysta cudzą kartę, wejdzie do pomieszczenia technicznego albo uzyska fizyczny dostęp do maszyny, ślady mogą pojawić się właśnie w systemach podlegających security managerowi. Tymczasem w wielu organizacjach bezpieczeństwo fizyczne i cyberbezpieczeństwo nadal działają równolegle. Operator CCTV może zobaczyć coś istotnego, ale nie wiedzieć, że w tym samym czasie SOC analizuje alarm dotyczący tej samej części zakładu.

Security manager nie musi znać sposobu programowania sterownika PLC. Powinien jednak wiedzieć**, które miejsca, osoby i zdarzenia są krytyczne dla bezpieczeństwa procesu.** Inaczej może dysponować informacją, która rozwiązuje zagadkę, nie zdając sobie sprawy z jej znaczenia.

Jego rola coraz częściej przesuwa się więc z ochrony obiektu w kierunku ochrony działalności przedsiębiorstwa. Pilnowanie bramy jest zadaniem security. Wiedza, że przez tę bramę wjechał serwisant, który godzinę później uzyskał dostęp do infrastruktury mogącej zatrzymać linię produkcyjną, jest już informacją istotną dla całej organizacji.

UWAGA: RYZYKO

IT widzi jedno. Ochrona – co innego.

Incydent cyfrowy może mieć fizyczny element: wejście osoby z zewnątrz, użycie karty dostępowej, wizytę serwisanta albo dostęp do szafy technicznej. Dlatego logi systemowe, kontrola dostępu, monitoring wizyjny i rejestr wizyt nie powinny być analizowane osobno.





KIEROWNIK I ZESPÓŁ IT:
zagrożenie w sieci nie kończy się na sieci

Dział IT dysponuje zupełnie innym obrazem sytuacji. Widzi konta użytkowników, ruch sieciowy, połączenia zewnętrzne, próby logowania, urządzenia pojawiające się w sieci, podejrzaną komunikację czy infekcję stacji roboczej.

W klasycznym środowisku informatycznym reakcja na taki incydent bywa stosunkowo oczywista: zainfekowane urządzenie można odizolować, użytkownikowi zablokować konto, przerwać podejrzane połączenie, wymusić zmianę hasła albo rozpocząć aktualizację systemu.

W OT te same działania mogą mieć fizyczne konsekwencje.

Odłączenie urządzenia może wpłynąć na sterowanie procesem. Restart systemu może nie być możliwy podczas produkcji. Aktualizacji nie można wykonać tylko dlatego, że pojawiła się poprawka bezpieczeństwa. Urządzenie, które z punktu widzenia specjalisty IT wygląda jak kolejny komputer podłączony do sieci, z punktu widzenia zakładu może odpowiadać za pracę instalacji wartej miliony złotych.

Dlatego kierownik IT może być pierwszą osobą, która wie, że dzieje się coś złego, a jednocześnie bywa tym, kto samodzielnie nie może zdecydować o reakcji.

I właśnie tutaj zaczyna się jedno z najtrudniejszych miejsc styku IT i OT: **IT potrafi rozpoznać zagrożenie, ale OT musi ocenić konsekwencje jego neutralizacji.**



UWAGA: RYZYKO

Odłączenie systemu też może być zagrożeniem.

W środowisku przemysłowym zasada „odłączmy wszystko od sieci" może zatrzymać proces technologiczny albo utrudnić późniejszą analizę zdarzenia. Jeszcze przed incydentem ustal, które elementy infrastruktury można izolować natychmiast, które wymagają zgody i kto może ją wydać.



OT, AUTOMATYCY I UTRZYMANIE RUCHU:
maszyna przede wszystkim ma działać

Automatyk patrzy na fabrykę inaczej niż specjalista cyberbezpieczeństwa. Interesuje go ciśnienie, temperatura, ruch ramienia robota, prędkość taśmy, stan napędu, komunikacja między sterownikiem a urządzeniami wykonawczymi. Wie, co jest normalnym zachowaniem procesu, a co powinno wzbudzić niepokój. To właśnie on może jako pierwszy zauważyć cyberatak, nawet jeśli nie nazwie go „cyberatakiem".

Maszyna zaczyna wykonywać nietypową sekwencję. Parametr zmienił się bez uzasadnienia technologicznego. Sterownik zachowuje się inaczej niż zwykle. Na panelu operatorskim pojawia się wartość, której nikt nie wprowadził. Urządzenie niespodziewanie przechodzi w inny tryb pracy.

Z perspektywy automatyka pierwsze pytanie nie brzmi jednak: „czy ktoś nas zaatakował?", lecz raczej: „co dzieje się z procesem?".

Podobnie działa utrzymanie ruchu. Jego naturalnym zadaniem jest przywrócenie sprawności instalacji. Jeżeli maszyna się zatrzymała, zespół ma ją uruchomić. Jeżeli urządzenie zgłasza błąd, trzeba znaleźć przyczynę i ją usunąć. Jeżeli konieczna jest pomoc producenta, trzeba skontaktować się z serwisem.

I tutaj pojawia się paradoks. Zachowanie całkowicie racjonalne podczas zwykłej awarii może być ryzykowne podczas cyberincydentu. Ponowne uruchomienie urządzenia może zatrzeć część śladów. Podłączenie laptopa serwisowego może stworzyć kolejną drogę komunikacji. Przywrócenie starej konfiguracji może nie usunąć przyczyny problemu.

Dlatego bezpieczeństwa OT nie da się po prostu przekazać informatykom. Potrzebne jest więc miejsce, w którym wiedza cyberbezpieczeństwa spotyka się z wiedzą ludzi rozumiejących proces technologiczny.

DLACZEGO ODWOŁUJEMY SIĘ DO NIST?

W raporcie korzystamy z wytycznych amerykańskiego National Institute of Standards and Technology nie jako ze źródła obowiązującego w Polsce prawa, lecz jako z uznanego technicznego punktu odniesienia dla bezpieczeństwa OT. NIST SP 800-82 to jeden z najbardziej rozbudowanych publicznie dostępnych przewodników po bezpieczeństwie systemów przemysłowych, uwzględniający bezpieczeństwo ludzi i procesu, niezawodność oraz ciągłość działania. Źródła polskie i europejskie wykorzystujemy przede wszystkim do opisu wymogów prawnych i skali zjawiska, a NIST tam, gdzie potrzebne są szczegółowe wskazówki techniczne i organizacyjne.



SOC I MONITORING:
centrum pełne alarmów, które trzeba jeszcze zrozumieć

Teoretycznie naturalnym miejscem do wykrycia zagrożenia powinno być centrum monitorowania. W praktyce wszystko zależy od tego, **co właściwie jest monitorowane.**

SOC może otrzymać informację o podejrzanym ruchu sieciowym. Centrum ochrony – alarm z kontroli dostępu. Dyspozytor techniczny – komunikat z systemu automatyki. Operator produkcji – ostrzeżenie na panelu maszyny. Każdy alarm może wyglądać niegroźnie, dopóki nie zostanie zestawiony z pozostałymi. Czy ktoś analizuje zdarzenia między systemami? Najbardziej zaawansowany monitoring nie pomoże, jeśli każdy zespół obserwuje własny ekran.

DOBRA PRAKTYKA

Nie pytaj dopiero podczas incydentu: „do kogo dzwonimy?"

Osoba, która jako pierwsza zauważy nietypowe zachowanie systemu, powinna mieć prostą ścieżkę eskalacji: kogo informuje, w jakiej kolejności i jak szybko. Taki schemat powinien być znany także produkcji, utrzymaniu ruchu i ochronie, nie tylko IT.

ZARZĄD:
ktoś musi zdecydować, ile ryzyka fabryka jest gotowa zaakceptować

W pewnym momencie incydent przestaje być techniczny. Podejrzane zachowanie sterownika zostało potwierdzone. Nie wiadomo jeszcze, czy rzeczywiście doszło do ataku ani jaki jest jego zakres. Linia nadal działa. Jej zatrzymanie oznacza jednak wielogodzinny przestój, utratę partii produktu albo wysokie koszty ponownego uruchomienia.

To dlatego odpowiedzialność za bezpieczeństwo fabryki ostatecznie trafia na poziom zarządczy. Nie oznacza to, że członek zarządu powinien decydować, który port sieciowy odłączyć albo jak skonfigurować sterownik. Powinien natomiast wcześniej zapewnić, że organizacja wie, kto ma prawo podejmować konkretne decyzje i gdzie przebiega granica akceptowanego ryzyka.

Jeżeli organizacja dopiero podczas ataku ustala, kto może zatrzymać proces, odizolować fragment OT albo rozstrzygnąć spór między IT a produkcją, traci najcenniejszy zasób – czas.

DO ZROBIENIA

Wskaż człowieka, który może powiedzieć „STOP".

Nie wystarczy wiedzieć, kto odpowiada za cyberbezpieczeństwo. Zakład powinien mieć jednoznacznie określone, kto może zdecydować o ograniczeniu lub zatrzymaniu produkcji ze względów bezpieczeństwa i kto przejmuje tę rolę podczas jego nieobecności.

KTO PODEJMUJE DECYZJĘ?

• **KIEROWNIK IT**
może powiedzieć:
ryzyko cybernetyczne jest wysokie.

• **AUTOMATYK:**
proces na razie pozostaje stabilny.

• **DYREKTOR PRODUKCJI:**
zatrzymanie będzie kosztować kilkaset tysięcy złotych.

• **SECURITY MANAGER:**
nie możemy wykluczyć fizycznego naruszenia infrastruktury.

Żadna z tych osób nie dysponuje pełną wiedzą.



INTEGRATOR I SERWISANT: człowiek spoza organizacji, który zna system od środka

Do tej układanki trzeba dodać jeszcze jednego uczestnika. Często dysponuje on ogromną wiedzą o infrastrukturze, choć formalnie w ogóle nie jest pracownikiem zakładu.

Integrator zna system, który wdrożył. Producent maszyny zna jej konfigurację. Firma serwisowa dysponuje oprogramowaniem diagnostycznym. Technik zewnętrzny może mieć uprawnienia administracyjne, dostęp do szafy sterowniczej albo możliwość zdalnego połączenia z urządzeniem. Z biznesowego punktu widzenia jest to wygodne. Z punktu widzenia bezpieczeństwa tworzy kolejną warstwę zależności.

Kluczowe staje się nie tylko to, czy serwisant ma dostęp, ale także kto ten dostęp przyznaje, kto go zatwierdza, na jaki okres, w jaki sposób jest rejestrowany i kto sprawdza, co podczas sesji rzeczywiście wykonano. Jeszcze trudniejsze pytanie pojawia się podczas incydentu. Zakład wykrywa problem w urządzeniu. Najwięcej wiedzy o jego konfiguracji ma producent lub integrator. Naturalnym odruchem jest więc natychmiastowe dopuszczenie go do systemu. Tyle że zanim to nastąpi, ktoś powinien rozstrzygnąć, czy zewnętrzny dostęp pomoże ograniczyć incydent, czy może dodatkowo go skomplikuje.

To szczególnie istotne w zakładach, w których infrastruktura powstawała przez wiele lat. Jedna linia może być obsługiwana przez producenta maszyny, inna przez lokalnego integratora, monitoring przez jeszcze inną firmę, a system kontroli dostępu przez kolejnego dostawcę. Każdy zna swój fragment. Nikt zewnętrzny nie odpowiada jednak za całość.

UWAGA: RYZYKO

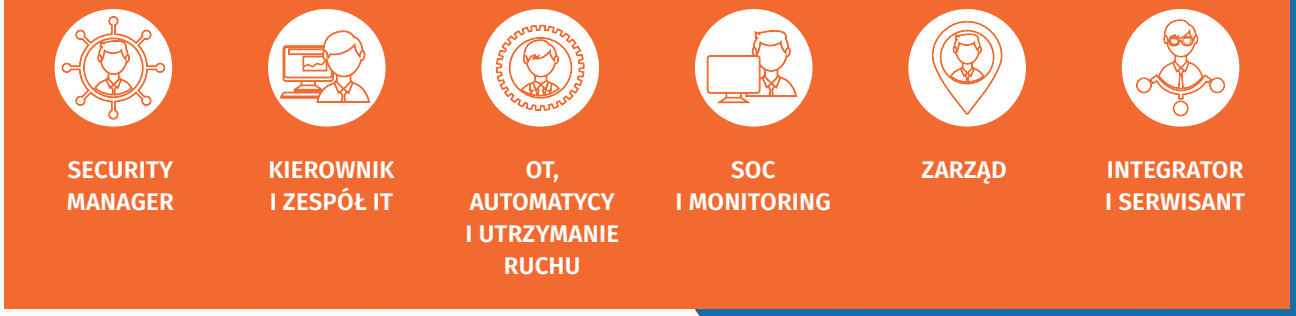
Dostęp, o którym nikt nie pamięta.

Sprawdź wszystkie aktywne połączenia zdalne do systemów IT i OT – także te utworzone dla integratorów, producentów maszyn i serwisantów. Konto, którego właściciela nie potrafisz dziś wskazać, powinno być traktowane jak luka, a nie wygodne rozwiązanie techniczne.

DO ZROBIENIA

Nadaj właściciela każdemu dostępowi zewnętrznemu.

Każdy dostawca mający dostęp do infrastruktury powinien mieć po stronie zakładu konkretną osobę odpowiedzialną za ten dostęp. Ustal także, kto i kiedy go wyłącza – po zakończeniu serwisu, projektu albo współpracy.



Wiele ról, jedna odpowiedzialność

Nie ma nic złego w tym, że bezpieczeństwo fabryki jest podzielone między wiele zespołów. W nowoczesnym zakładzie nie da się go powierzyć jednej osobie. Problem zaczyna się wtedy, gdy razem z obowiązkami podzielona zostaje również **odpowiedzialność za końcowy rezultat.**

Problem zaczyna się wtedy, gdy każdy prawidłowo wykonuje własne zadanie, ale nikt nie łączy tych działań w jeden proces decyzyjny. SOC eskaluje zgodnie z procedurą, utrzymanie ruchu próbuje przywrócić sprawność, serwis czeka na zgodę, a zarząd dowiaduje się o zdarzeniu dopiero wtedy, gdy produkcja już stoi.

Każdy wykonał swoje zadanie. Biznes przegrał.

Kto więc powinien powiedzieć „STOP”?

Najprostsza odpowiedź brzmiałaby: osoba odpowiedzialna za bezpieczeństwo. W fabryce taka odpowiedź właściwie niczego jednak nie rozwiązuje. **Nie ma jednej osoby, która jednocześnie rozumie sieć, proces technologiczny, bezpieczeństwo ludzi, konsekwencje dla produkcji i ryzyko biznesowe.** I nie trzeba takiego stanowiska tworzyć. Potrzebny jest natomiast wcześniej ustalony mechanizm, który odpowiada na cztery pytania:

1. **Kto wykrywa zagrożenie?**
2. **Kto ocenia jego konsekwencje?**
3. **Kto podejmuje decyzję?**
4. **Kto ją wykonuje?**

IT może wykryć nietypową komunikację, ale nie musi wiedzieć, czy odłączenie urządzenia nie stworzy zagrożenia dla procesu. Automatyk może ocenić stan maszyny, ale nie musi znać skali cyberincydentu. Security może ustalić, kto dostał się do chronionej strefy, lecz nie zdecyduje, czy sterownik nadal można uznać za wiarygodny. Dyrektor produkcji zna koszt zatrzymania linii, ale nie powinien samodzielnie rozstrzygać, czy dalsza praca jest bezpieczna.

„STOP” nie powinno być decyzją jednego działu. Powinno być elementem wcześniej uzgodnionej procedury.

Co wydarzyło się w naszej fabryce?

W naszym scenariuszu kolejne sygnały pojawiały się w różnych miejscach: automatyk zauważył zmianę parametru, IT – nietypową komunikację, security potwierdziło aktywność konta nieobecnego serwisanta, a firma serwisowa wykluczyła legalną sesję. Od tego momentu nie mamy już wyłącznie „dziwnego zachowania urządzenia”. Mamy nieautoryzowane wykorzystanie dostępu do infrastruktury OT.

Zablokowanie dostępu zewnętrznego zatrzymuje nietypową komunikację. Nie odpowiada jednak na najważniejsze pytanie: **czy wcześniej zmieniono konfigurację urządzenia i czy można jeszcze ufać temu, co robi system sterowania?** Dlatego decyzję o kontrolowanym zatrzymaniu części procesu można uznać za uzasadnioną. Problem nie polega na tym, że linia została zatrzymana. Problem polega na tym, że kluczowe ustalenia, kto ocenia sytuację, kto konsultuje decyzję i kto może powiedzieć „STOP”, odbywają się już podczas incydentu.

W dobrze przygotowanej organizacji większość tych pytań powinna mieć odpowiedź, **zanim na zegarze wybije 9.19.**

DOBRA PRAKTYKA

Po incydencie nie pytaj tylko „co zawiodło?”.

Zapytaj również: której decyzji nie można było podjąć wystarczająco szybko i dlaczego? Bardzo często problemem nie jest brak technologii, lecz brak osoby z odpowiednim mandatem, informacji albo procedury eskalacji.



KTO ZA CO ODPOWIADA?



IT/SOC – wykrywa zagrożenie w sieci i prowadzi działania izolacyjne w uzgodnionym zakresie.

OT/automatyk – ocenia wpływ incydentu i reakcji na proces technologiczny.

Security – dostarcza informacje o ludziach, dostępie fizycznym i zdarzeniach w chronionych strefach.

Produkcja/kierownik zmiany – wykonuje decyzję po stronie procesu, w tym bezpieczne zatrzymanie linii.

Zarząd lub wskazany decydent – rozstrzyga o poziomie akceptowanego ryzyka biznesowego.

Integrator/serwisant – dostarcza wiedzy technicznej, ale nie jest właścicielem decyzji.

Kto może zatrzymać produkcję?

To pytanie powinno mieć w każdej fabryce dwie odpowiedzi.

Pierwsza dotyczy **bezpieczeństwa ludzi i procesu.** Jeżeli istnieje bezpośrednie zagrożenie dla zdrowia, życia, instalacji albo otoczenia, prawo do podjęcia natychmiastowego działania musi być **delegowane wystarczająco nisko w strukturze organizacji.** Firma, w której o drugiej w nocy kierownik zmiany musi szukać członka zarządu, aby zatrzymać potencjalnie niebezpieczny proces, stworzyła procedurę, która może zadziałać za późno.

Druga odpowiedź dotyczy sytuacji niejednoznacznych, takich jak choćby nasz scenariusz. Proces nadal działa, ale nie wiadomo, czy można ufać systemowi sterowania. Zatrzymanie będzie kosztowne, ale dalsza praca również niesie ryzyko.

Nie wystarczy zapis: „decyzję podejmuje zarząd". Trzeba wiedzieć: **kto konkretnie, na podstawie czyjej rekomendacji, w jakim czasie i co dzieje się wtedy, gdy tej osoby nie ma.**

DOBRA PRAKTYKA

Nazwiska zamiast działów.

W procedurze kryzysowej zapis „powiadomić IT / security / produkcję" to za mało. Wpisz konkretne stanowisko, osobę zastępującą oraz sposób kontaktu poza godzinami pracy. Incydenty nie respektują schematu organizacyjnego ani godzin pracy biurowej.

Najważniejsze nie jest nazwisko. Najważniejszy jest moment

W wielu procedurach bardzo dużo miejsca poświęca się temu, kto jest odpowiedzialny za poszczególne systemy. Znacznie rzadziej ustala się **moment przekazania odpowiedzialności.**

Kiedy alarm SOC przestaje być problemem IT, a staje się incydentem zakładu? Kiedy nietypowa wartość na sterowniku przestaje być problemem automatyka? Kiedy podejrzana aktywność serwisanta przestaje być wyłącznie sprawą security? To właśnie te granice powinny zostać wcześniej zdefiniowane.

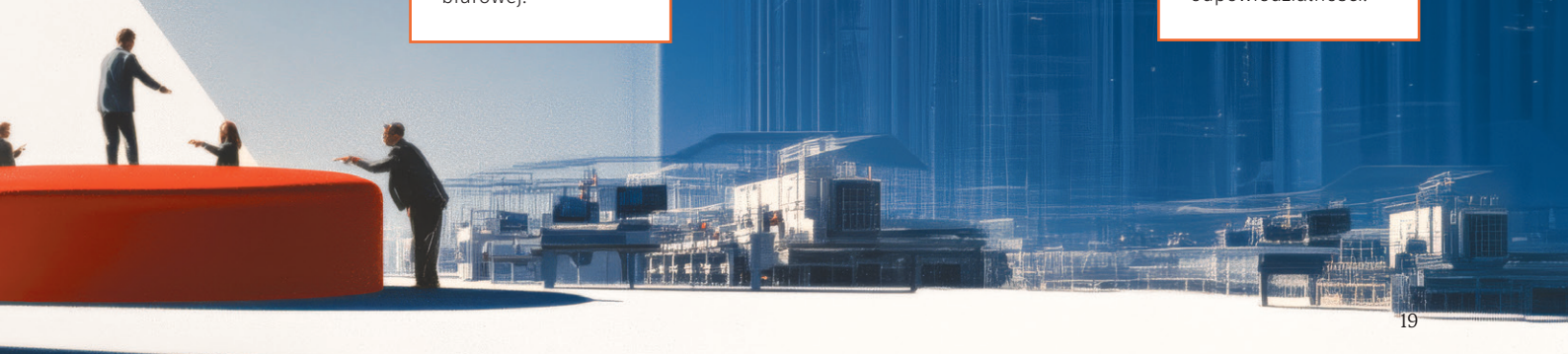
Organizacja nie musi eskalować każdego alarmu do zarządu. Musi natomiast wskazać zdarzenia, których wystąpienie automatycznie uruchamia wspólny tryb działania. Może to być na przykład jednoczesne pojawienie się anomalii w procesie i podejrzanej komunikacji sieciowej, nieautoryzowany dostęp do systemu OT, utrata zaufania do konfiguracji sterownika albo sytuacja, w której IT i OT rekomendują sprzeczne działania.

Wtedy nie powinno już być kilku równoległych incydentów. **Powinien być jeden incydent zakładu i jeden właściciel jego koordynacji.**

UWAGA: RYZYKO

Pierwszy telefon nie powinien uruchamiać dyskusji o obowiązkach.

Jeszcze przed kryzysem ustal, kto ocenia obowiązek zgłoszenia incydentu, kto kontaktuje się z właściwymi instytucjami, kto informuje zarząd, a kto odpowiada za komunikację z pracownikami, klientami i partnerami. W czasie zdarzenia nie powinno się dopiero interpretować podziału odpowiedzialności.





CO CZWARTA FIRMA PRODUKCYJNA MIAŁA INCYDENT

23,9%
polskich przedsiębiorstw z sektora przetwórstwa przemysłowego doświadczyło w 2024 r. incydentu związanego z bezpieczeństwem ICT.

To niemal dokładnie tyle, ile wynosi średnia dla wszystkich polskich przedsiębiorstw – **24%.**

Wśród dużych firm odsetek był jeszcze wyższy i sięgał **38%.**

Jednocześnie audyt bezpieczeństwa własnych systemów informatycznych przeprowadziło w tym samym roku tylko **15,5%** wszystkich badanych przedsiębiorstw.

Wniosek: incydenty nie są zjawiskiem marginalnym. Znacznie rzadsze pozostaje systematyczne sprawdzanie, czy organizacja jest na nie przygotowana.

Źródło: GUS, Społeczeństwo informacyjne w Polsce w 2025 r. (Główny Urząd Statystyczny)



Procedura ma działać o 2.00 w nocy

Najlepszym testem procedury bezpieczeństwa nie jest to, czy dobrze wygląda w dokumentacji. Test brzmi inaczej:

Czy zadziała w niedzielę o drugiej w nocy, kiedy w zakładzie nie ma dyrektora IT, prezesa ani większości osób, które uczestniczyły w jej tworzeniu?

Jeżeli odpowiedź brzmi „nie wiadomo", procedura wymaga poprawy.

Dlatego zakład powinien znać nie tylko nazwiska właścicieli poszczególnych obszarów, lecz także ich zastępców, numery alarmowe, kolejność eskalacji i zakres decyzji, które można podejmować bez oczekiwania na kolejną zgodę.

Nie można projektować reagowania wyłącznie na godziny pracy biura. Produkcja, systemy OT i zagrożenia nie pracują od 9.00 do 17.00.

Ostatecznie pytanie „kto powie STOP?" nie powinno paść po raz pierwszy wtedy, kiedy linia zaczyna zachowywać się inaczej niż zwykle. **Odpowiedź powinna być ustalona dużo wcześniej.** Bo w sytuacji kryzysowej nie wygrywa organizacja, która ma najwięcej systemów bezpieczeństwa. Wygrywa ta, która wie, **kto zauważa, kto ocenia, kto decyduje i kto działa**. •

DO ZROBIENIA

Sprawdź, czy backup naprawdę oznacza możliwość powrotu do pracy.

Nie pytaj wyłącznie, czy kopie zapasowe istnieją. Sprawdź, czy potraficie z nich odtworzyć w wymaganym czasie konkretne elementy potrzebne produkcji – konfiguracje, systemy sterowania, stacje operatorskie i dane niezbędne do wznowienia procesu.

Redakcja „a&s Polska"

TEST ODPORNOŚCI ZAKŁADU

15 pytań, które warto zadać jutro rano. Nie odpowiadaj tylko **TAK/NIE.** Dodaj dwie możliwości: **CZĘŚCIOWO** oraz **NIE WIEM.** Ta ostatnia odpowiedź bywa najcenniejsza – pokazuje obszary, w których organizacja nie potrafi nawet potwierdzić, czy zabezpieczenie istnieje.

PYTANIE	TAK	CZĘŚCIOWO	NIE	NIE WIEM
★ Czy mamy aktualną listę systemów i urządzeń OT działających w zakładzie?				
Czy wiemy, które z nich komunikują się z internetem lub siecią firmową?				
★ Czy znamy wszystkie firmy zewnętrzne posiadające dostęp do naszych systemów?				
Czy każde konto zewnętrzne ma konkretnego właściciela po naszej stronie?				
Czy dostęp serwisowy jest ograniczany do czasu, kiedy rzeczywiście jest potrzebny?				
★ Czy pracownik, który zauważy anomalię, wie dokładnie, kogo i jak szybko powiadomić?				
Czy mamy aktualną listę kontaktów do osób odpowiedzialnych za incydent również poza godzinami pracy?				
★ Czy wiadomo, kto ma prawo zdecydować o zatrzymaniu lub ograniczeniu produkcji?				
Czy ta osoba ma formalnie wyznaczonego zastępcę?				
Czy IT, OT, ochrona i produkcja mają uzgodniony podział odpowiedzialności podczas incydentu?				
Czy potrafimy połączyć informacje z logów IT/OT z kontrolą dostępu, monitoringiem i rejestrem wizyt?				
Czy wiemy, które systemy można bezpiecznie odłączyć podczas incydentu, a których nie wolno wyłączać bez dodatkowej decyzji?				
★ Czy w ostatnim czasie rzeczywiście testowaliśmy odtworzenie systemów potrzebnych do produkcji z kopii zapasowych?				
Czy wiadomo, kto podejmuje decyzję o zgłoszeniu incydentu na zewnątrz i kto dokonuje zgłoszenia?				
Czy w ciągu ostatnich 12 miesięcy przeprowadziliśmy ćwiczenie obejmujące jednocześnie IT/OT, produkcję i security?				

Nie licz punktów. Szukaj czerwonych flag. Pięć pytań oznaczonych ★ dotyczy fundamentów: wiedzy o własnym środowisku, dostępu zewnętrznego, eskalacji, prawa do zatrzymania procesu oraz możliwości odtworzenia systemów. Jeżeli przy którymkolwiek z nich pojawia się NIE albo NIE WIEM, wiadomo już, od czego zacząć porządkowanie.



Inteligentny monitoring w przemyśle 4.0:

technologie Hikvision wspierające bezpieczeństwo i sprawność operacyjną

W zakładzie produkcyjnym, centrum logistycznym i magazynie wysokiego składowania monitoring wizyjny odpowiada dziś za znacznie więcej niż rejestrację obrazu. Operatorzy muszą szybko ocenić, czy alarm dotyczy rzeczywistego zagrożenia, ustalić przebieg zdarzenia na rampie, zweryfikować ruch pojazdu przy bramie i zabezpieczyć materiał do raportu. Przy kilkudziesięciu lub kilkuset kamerach ręczne przeglądanie nagrań angażuje czas i zasoby.

Michał Michniowski

Rozwiązania Hikvision wykorzystujące analitykę obrazu pomagają uporządkować proces weryfikacji. Ich zadaniem jest wskazanie zdarzeń wymagających uwagi, ograniczenie liczby fałszywych alarmów, ułatwienie odnalezienia właściwego fragmentu nagrania oraz powiązanie obrazu z procedurami obowiązującymi w obiekcie. Wartość systemu zależy jednak nie tylko od sztucznej inteligencji, lecz także od jakości obrazu, prawidłowego montażu, konfiguracji, integracji i regularnej oceny wyników.

Obwód zakładu i place zewnętrzne

Ochrona ogrodzenia, placu składowego lub strefy technicznej odbywa się często w zmiennych warunkach. Deszcz, śnieg, ruch roślinności, zwierzęta i refleksy świetlne mogą powodować alarmy, które nie wymagają interwencji. Jeżeli operator otrzymuje zbyt wiele takich powiadomień, rośnie ryzyko opóźnienia reakcji na rzeczywiste zdarzenie.

W tym scenariuszu sprawdza się system **AcuSense.** Technologia wykorzystuje algorytmy uczenia głębokiego do rozróżniania przede wszystkim ludzi i pojazdów od innych obiektów lub ruchów w scenie. Kamera obserwująca ogrodzenie, plac manewrowy, wejście do hali lub dok może dzięki temu generować zdarzenia dla skonfigurowanych typów celów i ograniczać liczbę fałszywych alarmów.

Na zewnętrznych obszarach ważna jest również jakość obrazu po zmroku. Technologie **ColorVu** umożliwiają uzyskanie kolorowego obrazu w bardzo słabym oświetleniu, co może ułatwić ocenę barwy pojazdu, odzieży lub oznaczeń ładunku. **Smart Hybrid Light,** zależnie od modelu, oferuje tryb podczerwieni, światła białego oraz tryb inteligentny, w którym kamera może przełączyć się z IR na światło białe po wykryciu człowieka lub pojazdu. W wybranych kamerach funkcja **Live Guard** pozwala po wykryciu zdarzenia uruchomić ostrzegawcze światło stroboskopowe i komunikat audio. Jest to dodatkowa warstwa aktywnego odstraszania, a nie zamiennik procedur ochrony.

Przy rozległych placach i długich odcinkach perymetru warto rozważyć połączenie kamer panoramicznych, PTZ, radarów i termowizji. Rozwiązania **TandemVu** łączą w jednym urządzeniu szeroki obraz sytuacyjny z kanałem PTZ umożliwiającym szczegółową obserwację wybranego obiektu. W kompatybilnych konfiguracjach radar może przekazać pozycję celu, a kamera PTZ automatycznie skierować się na obszar detekcji i podjąć śledzenie. Termowizja wspiera obserwację przy ograniczonej widoczności, lecz nie zastępuje certyfikowanych systemów ochrony ani sygnalizacji pożarowej.

Brama, parking i ruch pojazdów

Brama zakładowa łączy ochronę obiektu z logistyką. Informacja o czasie wjazdu i wyjazdu pojazdów może być ważna zarówno dla ochrony, jak i działu logistyki.

Dedykowane kamery **ANPR/LPR** Hikvision wspierają odczyt tablic rejestracyjnych i rejestrację ruchu pojazdów. Wynik może zostać powiązany z obrazem, czasem zdarzenia oraz – w ramach odpowiednio zaprojektowanej integracji – z systemem kontroli wjazdu, parkingiem lub automatyką szlabanu. Pozwala to szybciej ustalić, kiedy dany pojazd pojawił się na terenie zakładu i jak przebiegała jego obsługa.

Ilustracje: Magnific



HikCentral może pełnić funkcję wspólnego środowiska dla obrazu, kontroli dostępu, systemu parkingowego i alarmów. Operator otrzymuje informacje w jednym miejscu, a zdarzenie może zostać zapisane w historii systemu. Dzięki temu monitoring wspiera proces obsługi wjazdów i wyjazdów, zamiast działać wyłącznie jako archiwum.

Rampa i magazyn – od zdarzenia do materiału dowodowego

Rampa przeładunkowa jest miejscem, w którym krzyżują się procesy logistyczne, ruch pojazdów i praca ludzi. Dochodzi tu do pomyłek przy wydaniu towaru, uszkodzeń ładunku, kolizji oraz sporów dotyczących odpowiedzialności. Samo nagranie nie wystarcza, jeżeli jego odnalezienie zajmuje wiele godzin.

W tym zastosowaniu kamery **DeepinView** mogą wspierać bardziej zaawansowaną analitykę realizowaną bezpośrednio na urządzeniu, zależnie od modelu i dostępnych funkcji. Mogą generować metadane związane z wykrytymi obiektami i zdarzeniami, co ułatwia późniejsze przeszukiwanie nagrań.

AcuSearch w kompatybilnych systemach przyspiesza wyszukiwanie nagrań przez analizę wskazanego celu. Operator może zaznaczyć osobę lub pojazd w obrazie na żywo albo w odtwarzanym materiale, a system wyszukuje inne wystąpienia podobnego celu w nagraniach. Dostępne zakresy wyszukiwania i filtry zależą od modelu rejestratora, kamery, wersji oprogramowania i konfiguracji.

W nowszych, kompatybilnych rozwiązaniach Hikvision funkcję tę uzupełnia **AcuSeek,** który umożliwia wyszukiwanie nagrań z użyciem zapytań w języku naturalnym, np. opisu osoby, pojazdu lub innego obiektu.

Hala produkcyjna i strefy krytyczne

W hali produkcyjnej monitoring może wspierać ochronę stref ograniczonego dostępu, analizę ruchu ludzi i pojazdów oraz dokumentowanie zdarzeń. W zależności od potrzeb można zastosować AcuSense do klasyfikacji ludzi i pojazdów albo urządzenia DeepinView, gdy wymagany jest bardziej rozbudowany zestaw funkcji analitycznych realizowanych na kamerze.

DeepinView nie należy traktować jako uniwersalnego systemu diagnostyki maszyn. Może wspierać scenariusze widoczne w obrazie, takie jak naruszenie strefy, przekroczenie linii, obecność obiektu w określonym obszarze czy inne funkcje dostępne dla danego modelu. Jeżeli zakład chce analizować konkretną nieprawidłowość procesu, należy sprawdzić, czy urządzenie obsługuje wymagany scenariusz, i przeprowadzić test w rzeczywistych warunkach.

Kamery mogą również wspierać bezpieczeństwo ruchu pieszych i wózków widłowych. Mogą wykrywać wejście człowieka do strefy przeznaczonej dla pojazdów albo pojawienie się obiektu w obszarze, który powinien pozostać wolny. Zdarzenie może trafić do operatora, zostać zapisane do analizy BHP lub uruchomić dodatkową sygnalizację.

W większych halach wiele kamer może generować jednocześnie zdarzenia i metadane. W takiej sytuacji **DeepinMind** może pełnić funkcję centralnego elementu rejestrującego i analitycznego, zależnie od konkretnego modelu. Rozwiązania tej rodziny mogą wspierać analizę wielu kanałów, tworzenie i wykorzystanie metadanych oraz późniejsze wyszukiwanie materiału. Ich dobór powinien uwzględniać liczbę kamer, retencję, przepustowość i planowane funkcje AI.

Architektura systemu i zarządzanie

Wydajny system powinien dzielić zadania pomiędzy urządzenia brzegowe i warstwę centralną. Kamera może realizować szybką detekcję człowieka, pojazdu lub naruszenia strefy, ograniczając opóźnienia i potrzebę centralnego przetwarzania wszystkich strumieni. Rejestrator lub serwer odpowiada za przechowywanie, indeksowanie i wyszukiwanie materiału z wielu kanałów.

W tym modelu DeepinView pełni funkcję zaawansowanej kamery analitycznej, AcuSense wspiera klasyfikację ludzi i pojazdów, a DeepinMind może centralizować analizę i pracę z nagraniami. HikCentral zapewnia warstwę zarządzania urządzeniami, użytkownikami, alarmami i procedurami. Nie każda instalacja wymaga wszystkich tych elementów. Dobór zależy od skali obiektu, liczby kamer, wymagań analitycznych, dostępnej sieci i planowanego rozwoju.

HikCentral może łączyć monitoring z kontrolą dostępu, alarmami, wideodomofonami i systemami parkingowymi. Jeżeli kamera wykryje osobę w strefie ograniczonego dostępu, operator może otrzymać obraz z miejsca zdarzenia, a w zależności od konfiguracji i reguł powiązań także szybko otworzyć podgląd z kamer sąsiednich. Przy odpowiedniej integracji zapis można zestawić z informacją o użyciu identyfikatora, alarmem lub zdarzeniem przy bramie.

Integracja z systemami IT i OT wymaga indywidualnego projektu. Niezbędne są segmentacja sieci, kontrolowane interfejsy, ograniczenie uprawnień, bezpieczny dostęp zdalny, aktualizacje oprogramowania i regularny przegląd logów. System wizyjny nie powinien uzyskiwać szerszego dostępu do środowiska automatyki, niż jest to konieczne do realizacji uzgodnionego scenariusza.

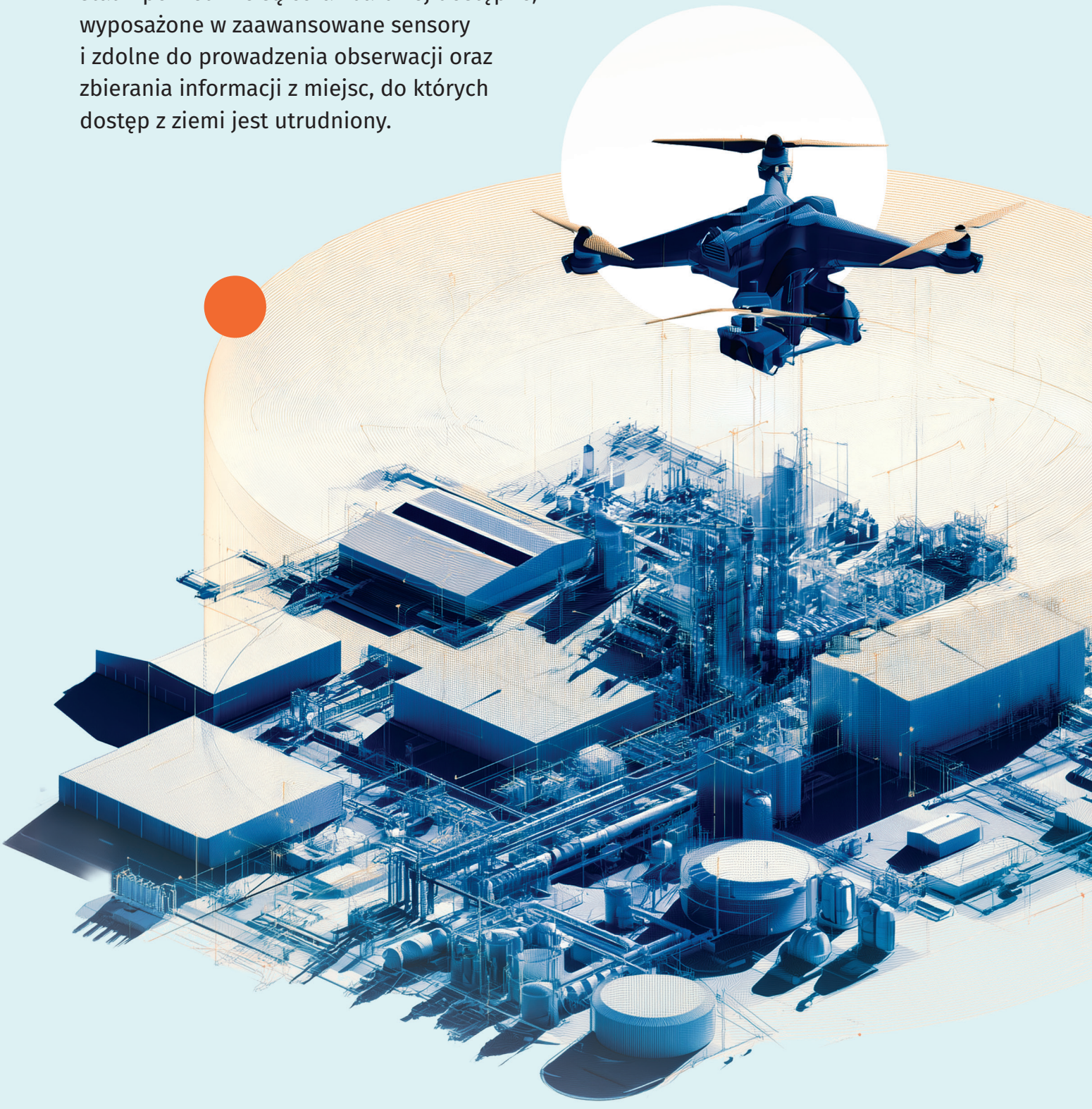
Warunki skutecznego wdrożenia

Przed instalacją należy określić, czy celem jest wykrycie, obserwacja, rozpoznanie, czy identyfikacja obiektu. Następnie dobiera się obiektyw, rozdzielczość, wysokość montażu, oświetlenie, sposób przechowywania i funkcje analityczne.

W obiekcie przemysłowym trzeba uwzględnić zapylenie, wilgoć, drgania, temperaturę, ryzyko korozji i możliwość serwisowania urządzeń. Stabilne zasilanie, zabezpieczenia przeciwprzepięciowe, właściwa pojemność archiwum oraz monitorowanie dysków są równie ważne jak wybór kamery AI. •

Hikvision Poland
ul. Żwirki i Wigury 16B
02-092 Warszawa
www.hikvision.com/europe/
info.pl@hikvision.com

Jeszcze kilka lat temu pojawienie się drona nad terenem zakładu przemysłowego mogło być traktowane jako naruszenie prywatności, ciekawostka lub incydent wymagający zgłoszenia. Dziś sytuacja wygląda inaczej. Bezzałogowe statki powietrzne są coraz bardziej dostępne, wyposażone w zaawansowane sensory i zdolne do prowadzenia obserwacji oraz zbierania informacji z miejsc, do których dostęp z ziemi jest utrudniony.



Dron nad zakładem to już nie tylko incydent

Nowy wymiar ochrony infrastruktury krytycznej

Dla infrastruktury krytycznej i przemysłu pojawiła się konieczność zmiany sposobu myślenia o ochronie. Ogrodzenie, kontrola dostępu czy monitoring nie wystarczą, jeśli potencjalne zagrożenie może pojawić się kilkaset metrów nad chronionym terenem.

Odpowiedzią na rosnącą skalę problemu ma być przedstawiony przez Komisję Europejską w lutym 2026 r. **Plan działania na rzecz ochrony przed dronami i zwalczania dronów.** Dokument koncentruje się na czterech obszarach: zwiększaniu gotowości, rozwijaniu zdolności wykrywania, koordynowaniu reakcji oraz wzmacnianiu europejskich zdolności do przeciwdziałania zagrożeniom.

Od ochrony perymetrycznej do ochrony przestrzeni powietrznej

Tradycyjny model zabezpieczenia obiektu przemysłowego zaczyna się od ogrodzenia. To na jego poziomie funkcjonują systemy ochrony perymetrycznej, CCTV, kontroli dostępu czy detekcji prób wtargnięcia.

Dron całkowicie zmienia tę geometrię. Może ominąć ogrodzenie i bramę, przelecieć nad strefą technologiczną, obserwować instalacje lub śledzić ruch pojazdów. W przypadku zakładów chemicznych, energetycznych, rafinerii, terminali czy magazynów energii może to oznaczać realne zagrożenie bezpieczeństwa operacyjnego.

Dlatego ochrona obiektu powinna obejmować również chronioną przestrzeń powietrzną. Konieczne jest określenie, jakie operacje dronów są dozwolone, które wymagają dodatkowej weryfikacji, a które powinny uruchamiać procedury bezpieczeństwa.

Najpierw wykryć, potem zrozumieć

Jednym z najważniejszych elementów unijnego planu jest rozwijanie zdolności wykrywania, śledzenia i identyfikowania dronów. Dla security managera samo wykrycie obiektu nie jest jednak wystarczające. Trzeba wiedzieć, co wykryto, gdzie znajduje się obiekt, z jakiego kierunku nadlatuje, jaką trasę pokonuje i czy jego zachowanie jest zgodne z oczekiwaniami.

Komisja Europejska wskazuje m.in. na potrzebę agregowania danych w jednym obrazie sytuacji powietrznej. W praktyce oznacza to łączenie informacji z różnych źródeł: radarów, systemów radiowych, kamer, systemów optoelektronicznych, sieci telekomunikacyjnych czy innych dostępnych sensorów.

To podejście jest dobrze znane w nowoczesnym security. Podobnie jak w przypadku PSIM czy zintegrowanych platform VMS, największa wartość nie wynika z pojedynczego urządzenia, lecz z połączenia danych i możliwości ich szybkiej interpretacji.

Interesującym kierunkiem wskazanym przez UE jest również wykorzystanie detekcji komórkowej, w tym anten 5G, do śledzenia obiektów latających. W przyszłości infrastruktura telekomunikacyjna może więc pełnić nie tylko funkcję komunikacyjną, ale również dostarczać informacji wspierających świadomość sytuacyjną.

Antydron to nie tylko „wykrywacz”

W dyskusji o systemach antydronowych często pojawia się prosty schemat: wykryć i zneutralizować. Tymczasem skuteczna ochrona wymaga znacznie szerszego podejścia.

Nie każdy dron nad zakładem oznacza zagrożenie. Może wykonywać legalną inspekcję, być wykorzystywany przez służby lub należeć do uprawnionego operatora. System powinien więc umożliwiać odróżnienie operacji legalnej od potencjalnie złośliwej.

Kluczowe znaczenie ma analiza zachowania. Dron regularnie pojawiający się w pobliżu zakładu, zmieniający trasę, kierujący

Ilustracje: A&S AI Studio



się w stronę określonej instalacji lub wykonujący nietypowe manewry może stanowić znacznie większe ryzyko niż pojedynczy, przypadkowy przelot.

Dlatego system ochrony powinien odpowiadać nie tylko na pytanie: „czy wykryto drona?", ale przede wszystkim: „czy jego obecność stanowi zagrożenie dla tego konkretnego obiektu?"

Integracja zamiast kolejnej wyspy technologicznej

W dużych zakładach problemem nie jest zazwyczaj brak danych, lecz ich rozproszenie. Operator może korzystać z VMS, kontroli dostępu, ochrony perymetrycznej, BMS, systemów alarmowych i platform zarządzania bezpieczeństwem. Jeżeli dołożymy do tego system antydronowy działający niezależnie, reakcja na incydent może być opóźniona.

Znacznie większą wartość daje integracja.

Wykrycie drona może automatycznie skierować kamerę PTZ w określoną strefę, wyświetlić alarm na stanowisku operatora, wskazać lokalizację obiektu na mapie i uruchomić odpowiednią procedurę. Informacja może jednocześnie trafić do osób odpowiedzialnych za bezpieczeństwo.

W przypadku infrastruktury krytycznej system antydronowy powinien być więc traktowany jako element szerszego systemu zarządzania incydentami, a nie pojedyncze urządzenie.

AI wesprze ocenę zagrożenia

Rosnąca liczba danych zwiększa znaczenie sztucznej inteligencji. AI może wspierać klasyfikowanie obiektów, analizowanie ich trajektorii, wykrywanie nietypowych zachowań oraz korelowanie informacji z różnych sensorów.

Szczególnie istotne jest połączenie danych technicznych z kontekstem operacyjnym. Dron nad parkingiem może oznaczać zupełnie inne ryzyko niż obiekt kierujący się w stronę instalacji technologicznej, zbiorników magazynowych czy strefy przechowywania materiałów niebezpiecznych.

AI nie powinna więc zastępować operatora, lecz dostarczać mu informacji potrzebnych do szybszego podjęcia właściwej decyzji.

Technologia to dopiero początek

Nawet najlepszy system detekcji nie zapewni bezpieczeństwa, jeśli organizacja nie będzie wiedziała, co zrobić po wykryciu zagrożenia. Procedury powinny określać, kto otrzymuje alarm, kto dokonuje weryfikacji, kiedy informowana jest ochrona, a kiedy właściwe służby.

Równie ważne są ćwiczenia. Unijny plan działania zakłada organizowanie dużych ćwiczeń dotyczących bezpieczeństwa dronów. Podobne testy powinny być prowadzone również na poziomie poszczególnych obiektów.

Ćwiczenie powinno sprawdzać cały łańcuch reakcji – od detekcji i identyfikacji, przez ocenę zagrożenia, po komunikację i działania ochrony. Dopiero wtedy można zweryfikować, czy technologia, procedury i ludzie rzeczywiście tworzą jeden system.

Bezpieczeństwo zaczyna się nad ogrodzeniem

Plan działania UE pokazuje, że zagrożenia związane z dronami przestają być traktowane jako pojedyncze, lokalne incydenty. Rozwijane są europejskie zdolności wykrywania, identyfikacji, wymiany informacji i reagowania, a coraz większe znaczenie mają technologie, takie jak AI, 5G, radary czy zintegrowane platformy zarządzania.

Dla właścicieli infrastruktury krytycznej i zakładów przemysłowych jest to wyraźny sygnał, że zagrożenie z powietrza powinno stać się stałym elementem oceny ryzyka.

Nie oznacza to konieczności wyposażania każdego obiektu w najbardziej zaawansowany system antydronowy. Oznacza natomiast potrzebę odpowiedzi na podstawowe pytania: jakie strefy są dla nas krytyczne? Jak szybko jesteśmy w stanie wykryć drona? Czy potrafimy odróżnić legalną operację od potencjalnego zagrożenia? Kto podejmuje decyzję o reakcji? Czy nasze systemy bezpieczeństwa potrafią działać jako jeden organizm?

Bo w nowoczesnym zakładzie przemysłowym bezpieczeństwo nie kończy się już na ogrodzeniu. Obejmuje również przestrzeń nad nim – a to właśnie tam pojawia się nowy wymiar ochrony. •

Redakcja „a&s Polska"

ECHODYNE

Oficjalny dystrybutor:
Linc
Trusted Solutions

ZANIM ZOBACZYSZ - RADAR JUŻ WIE.

Inteligentne radary 4D do ochrony obiektów i przestrzeni.



EchoShield®

WIELOZADANIOWY RADAR 4D

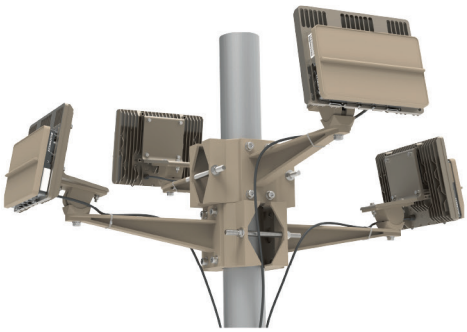
Maksymalny zasieg i identyfikacja



EchoGuard®

KOMPAKTOWY RADAR 4D

Maksymalna skuteczność w kompaktowej formie



IDENTYFIKACJA I ŚLEDZENIE
do 40 obiektów o wysokim oraz do 1000 obiektów o niskim priorytecie

SKUTECZNOŚĆ
identyfikacji dronów do 100%

DOKŁADNOŚĆ ŚLEDZENIA
<0.5° azymut x <0.5° wysokość

RADARY ECHODYNE
używane są już we wszystkich agencjach federalnych USA, jak i w wielu innych obiektach

DRIVE & SCAN
Detekcja, identyfikacja i śledzenie celów podczas przemieszczania radaru

STANDARD MESA®
opatentowana matryca elektronicznie skanowanych metamateriałów

Drony w ochronie
Technologia, która wspiera człowieka



Skąd w Seris zainteresowanie wykorzystaniem dronów w ochronie?

Od kilku lat obserwowaliśmy rozwój technologii bezzałogowych statków powietrznych, podobnie jak wielu innych rozwiązań mogących znaleźć zastosowanie w nowoczesnych usługach ochrony. Interesowały nas jednak nie same urządzenia, ale przede wszystkim ich praktyczna wartość dla klientów.

Punktem wyjścia było pytanie o to, jak skuteczniej chronić duże i złożone obiekty, gdzie tradycyjne patrole oraz systemy stacjonarne nie zawsze zapewniają pełną widoczność i szybki dostęp do informacji. Dotyczy to szczególnie zakładów przemysłowych, obiektów energetycznych, kopalń, centrów logistycznych czy rozległych inwestycji infrastrukturalnych.

Po serii testów i prezentacji realizowanych na przełomie 2024 i 2025 roku przekonaliśmy się, że dron może być realnym wsparciem dla ochrony fizycznej i systemów technicznych. Dziś jesteśmy już na etapie pierwszych wdrożeń i zbierania doświadczeń z codziennej eksploatacji tych rozwiązań.

Czy drony mają zastąpić pracowników ochrony?

To jedno z najczęściej pojawiających się pytań i odpowiedź jest jednoznaczna: nie. Dron nie zastępuje człowieka, lecz dostarcza mu dodatkowych informacji pozwalających podejmować lepsze i szybsze decyzje.

Nawet najbardziej zaawansowany system nie przeprowadzi oceny sytuacji, nie zdecyduje o sposobie reakcji i nie poniesie odpowiedzialności za działania operacyjne. Za te elementy nadal odpowiada człowiek.

W praktyce największa wartość dronów nie polega na ograniczaniu liczby pracowników, ale na zwiększaniu skuteczności ochrony. Dzięki nim można szybciej zweryfikować zagrożenie, uzyskać szerszy obraz sytuacji i efektywniej zarządzać bezpieczeństwem rozległych terenów.

W jakich obiektach drony sprawdzają się najlepiej?

Największy potencjał widzimy wszędzie tam, gdzie chroniony teren jest rozległy lub posiada wiele miejsc trudnych do objęcia stałym nadzorem. Mówimy o zakładach przemysłowych, kopalniach, obiektach energetycznych czy rozbudowanych centrach logistycznych.

W takich lokalizacjach pełne zabezpieczenie każdego fragmentu terenu za pomocą tradycyjnych patroli lub bardzo rozbudowanej infrastruktury monitoringu bywa kosztowne i organizacyjnie wymagające. Dron pozwala szybko skierować obserwację w miejsce wymagające sprawdzenia i skutecznie uzupełnia już funkcjonujące systemy bezpieczeństwa.

Jakie przewagi daje dron w porównaniu z tradycyjnym patrolem?

Przede wszystkim szybkość działania. Patrol pieszy lub zmotoryzowany potrzebuje czasu, aby dotrzeć we wskazane miejsce. Dron może znaleźć się nad nim w kilkadziesiąt sekund i przekazać operatorowi aktualny obraz sytuacji.

Bardzo ważnym elementem są również automatyczne misje patrolowe. Możemy tworzyć różne warianty tras i harmonogramów lotów, dzięki czemu działania nie są przewidywalne dla potencjalnych sprawców.

Ilustracje: A&S AI Studio

Drony coraz częściej wspierają nowoczesne usługi ochrony, szczególnie w przypadku rozległych i wymagających obiektów. Jaką wartość mogą wnieść do codziennej pracy ochrony, gdzie sprawdzają się najlepiej i czy rzeczywiście zmieniają sposób zabezpieczania obiektów? O wykorzystaniu dronów w **Seris Konsalnet** mówi **Michał Kalinowski,** Dyrektor Handlowy Usług Monitoringu i Techniki.



Dron nie służy wyłącznie do reagowania na alarmy. Znaczną część jego pracy stanowią regularne loty kontrolne, podczas których może wykonywać dodatkowe obserwacje wybranych miejsc, zmieniać wysokość lotu czy realizować zbliżenia obrazu. Pozwala to dokładniej oceniać sytuację i szybciej wychwytywać nieprawidłowości.

W przypadku alarmu może natomiast błyskawicznie zweryfikować zdarzenie, szczególnie na obszarach nieobjętych systemem monitoringu wizyjnego. Jeżeli zagrożenie zostanie potwierdzone, operator otrzymuje informacje o liczbie osób, kierunku ich przemieszczania się czy aktualnej lokalizacji jeszcze przed przyjazdem grupy interwencyjnej.

Jak reagowali klienci podczas pierwszych prezentacji?

Reakcje były bardzo pozytywne. Klienci szybko dostrzegali praktyczne możliwości wykorzystania dronów do ochrony swoich obiektów. Oczywiście pojawiały się pytania dotyczące kosztów i organizacji pracy, jednak równie często rozmawialiśmy o skuteczności i zwiększaniu poziomu bezpieczeństwa.

Co ciekawe, część organizacji początkowo skupiała się głównie na potencjalnych oszczędnościach. W trakcie analiz konkretnych przypadków coraz wyraźniej było jednak widać, że kluczową korzyścią jest możliwość znacznie skuteczniejszego monitorowania dużych i trudno dostępnych obszarów. To właśnie ten aspekt najczęściej prowadził do decyzji o rozpoczęciu pilotaży i wdrożeń.

Jak wygląda wdrożenie takiego rozwiązania?

Każdy projekt rozpoczyna się od szczegółowej analizy obiektu i potrzeb klienta. Identyfikujemy obszary wymagające szczególnego nadzoru oraz określamy cele, które mają zostać osiągnięte dzięki wykorzystaniu dronów. Następnie przygotowywane są procedury operacyjne oraz scenariusze lotów.

Dużą wagę przywiązujemy do projektowania automatycznych misji patrolowych. Nie są to jedynie proste przeloty pomiędzy punktami. W zależności od potrzeb dron może zatrzymywać się nad określonym miejscem, wykonywać dodatkową obserwację czy przeprowadzać szczegółową kontrolę wskazanego obszaru.

W zależności od charakterystyki obiektu może wspierać kontrolę przestrzegania zasad bezpieczeństwa, obserwację określonych stref, weryfikację obecności osób czy identyfikację potencjalnych zagrożeń. Ważnym elementem każdego projektu są również szkolenia personelu i spełnienie wszystkich wymogów formalnych związanych z wykonywaniem operacji lotniczych.

Czy pracownicy ochrony obawiali się nowej technologii?

Początkowo zakładaliśmy, że takie obawy mogą się pojawić, jednak praktyka okazała się bardzo pozytywnym zaskoczeniem. Współczesne rozwiązania są intuicyjne i nie wymagają od operatora zaawansowanych umiejętności pilotażu.

Dzięki odpowiedniej konfiguracji pracownik koncentruje się głównie na analizie obrazu i ocenie sytuacji. Bardzo dobrze sprawdza się również współpraca pomiędzy młodszymi pracownikami, którzy szybko przyswajają nowe technologie, a osobami posiadającymi wieloletnie doświadczenie w ochronie. Połączenie tych kompetencji daje bardzo dobre efekty.

W jaki sposób Seris wspiera pracowników korzystających z dronów?

Od początku zakładaliśmy, że sukces projektu zależy zarówno od technologii, jak i od ludzi. Dlatego zapewniamy szkolenia, wsparcie operacyjne oraz możliwość rozwijania kompetencji w bezpiecznych i komfortowych warunkach.

Zapewniamy również odpowiednie zabezpieczenia organizacyjne i ubezpieczeniowe obejmujące sprzęt oraz odpowiedzialność cywilną związaną z realizacją usługi. Dzięki temu nowa technologia staje się dla pracowników nie tylko narzędziem pracy, ale często także źródłem satysfakcji zawodowej i nowych zainteresowań.

Jakie modele wykorzystania dronów oferuje obecnie Seris i jak wygląda przyszłość tej technologii?

Obecnie rozwijamy dwa podstawowe modele działania. Pierwszy zakłada wykorzystanie drona przez pracownika ochrony znajdującego się na chronionym terenie, przy zachowaniu lotów w zasięgu wzroku operatora (VLOS). Drugim rozwiązaniem są stacje dokujące umożliwiające autonomiczny start, lądowanie oraz realizację zaplanowanych misji patrolowych. W tym modelu pracownik ochrony nadal nadzoruje operację, jednak robi to z poziomu centrum operacyjnego, a sam dron wykonuje lot poza zasięgiem jego wzroku (BVLOS).

Patrząc w przyszłość, widzimy duży potencjał w dalszej automatyzacji procesów, rozwoju funkcji wspieranych przez sztuczną inteligencję oraz zdalnym zarządzaniu operacjami lotniczymi. Oznacza to, że lot realizowany na obiekcie w Gdańsku może być nadzorowany z centralnej stacji monitorowania Seris lub centrum operacyjnego znajdującego się w zupełnie innej lokalizacji.

Podchodzimy jednak do tego odpowiedzialnie, koncentrując się na rozwiązaniach, które realnie zwiększają poziom bezpieczeństwa klientów. Naszym celem nie jest wdrażanie technologii dla samej technologii, lecz dostarczanie narzędzi, które pomagają skuteczniej chronić ludzi i mienie. Dziś już wiemy, że drony będą odgrywać coraz większą rolę w nowoczesnych usługach ochrony. •

SERIS KONSALNET
ul. Jana Kazimierza 55
01-267 Warszawa
www.seris.pl

Agentura zagraża obiektom przemysłowym





Zagrożenie dla zakładu przemysłowego nie zawsze zaczyna się od sforsowania ogrodzenia, włamania do systemu lub uszkodzenia instalacji. Często poprzedzają je rozproszone, z pozoru zwyczajne działania: obserwacja bramy wjazdowej, pytania o harmonogram dostaw, próby pozyskania informacji od pracownika lub wykorzystanie firmy zewnętrznej.

mjr dr Anna Grabowska-Siwiec

Gdy tego rodzaju aktywności tworzą spójny wzorzec, można podejrzewać, że są elementem operacji prowadzonej przez pośredników – agenturę proxy. Dla zespołu zarządzania bezpieczeństwem obiektu oznacza to konieczność patrzenia nie tylko na jego granice, lecz także na ludzi, informacje i relacje w jego otoczeniu.

Bezpieczeństwo obiektu przemysłowego kojarzy się zazwyczaj z ochroną fizyczną, systemem kontroli dostępu, monitoringiem wizyjnym, ochroną przeciwpożarową i cyberbezpieczeństwem. Wszystkie te elementy są ważne. Współczesne środowisko zagrożeń wymaga jednak szerszego spojrzenia. Przeciwnik nie musi

proxy



Agentura proxy – co to znaczy?

W artykule termin **„agentura proxy”** oznacza osoby, grupy lub podmioty wykorzystywane do wykonywania zadań na rzecz państwowego zleceniodawcy lub powiązanej z nim struktury w sposób, który utrudnia ujawnienie jego roli i przypisanie odpowiedzialności.
Wykonawcy mogą być świadomymi współpracownikami albo doraźnie rekrutowanymi osobami znającymi tylko fragment zadania. Nie jest to odrębna kategoria prawna, lecz opis modelu działania.

Ilustracje: A&S AI Studio

podejmować bezpośredniego, agresywnego, jednorazowego ataku. Może najpierw cierpliwie zbierać informacje, testować procedury i wykorzystywać osoby lub podmioty, które z jego perspektywy zapewnią dostęp, wiedzę albo możliwość zakłócenia działania obiektu pozostającego w jego zainteresowaniu.

Ten model wrogiej aktywności nabiera szczególnego znaczenia w warunkach zagrożeń hybrydowych, czyli skoordynowanych działań prowadzonych z użyciem środków fizycznych, cybernetycznych, informacyjnych, ekonomicznych i wywiadowczych, często poniżej progu otwartego konfliktu. Wobec infrastruktury krytycznej mogą one obejmować rozpoznanie zabezpieczeń i personelu, próby nieuprawnionego dostępu, zakłócenie dostaw lub transportu, cyberataki na systemy IT i OT, ingerencję w łączność albo fizyczny sabotaż newralgicznych elementów obiektu. Działaniom tym może towarzyszyć dezinformacja, np. rozpowszechnianie fałszywych informacji o awarii, skażeniu lub utracie kontroli nad sytuacją w obiekcie, służące zwiększeniu presji społecznej i podważeniu zaufania do operatora. Wykorzystanie agentury proxy pozwala zleceniodawcy rozproszyć zadania między pośredników, wykorzystać ich lokalną wiedzę i utrudnić wykrycie powiązań oraz przypisanie odpowiedzialności.

Nie oznacza to, że wszelkie przypadki nietypowego działania w otoczeniu zakładu lub obiektu są elementem obcej operacji. Byłoby to twierdzenie nieuprawnione i prowadziłoby do nadmiernego alarmizmu. Oznacza natomiast, że personel odpowiedzialny za bezpieczeństwo powinien umieć rejestrować i oceniać anomalie, nawet drobne, zwłaszcza gdy dotyczą obszarów kluczowych dla ciągłości działania przedsiębiorstwa.

Agentura proxy: pośrednik zamiast bezpośredniego sprawcy

W klasycznym rozumieniu agent kojarzy się z osobą świadomie współpracującą z obcym wywiadem. W tym tekście pojęcie agentury proxy jest używane w szerszym znaczeniu. Obejmuje osoby, grupy lub podmioty wykorzystywane przez zleceniodawcę do realizacji określonych działań, bez bezpośredniego ujawniania jego roli. Część wykonawców może znać prawdziwy cel operacji, inni wykonują tylko pojedyncze zadanie i nie mają wiedzy o całym przedsięwzięciu. Bezpośrednia relacja z prowadzącą operację służbą może istnieć, ale nie jest konieczna; kontakt może odbywać się przez pośrednika, komunikator internetowy lub strukturę przestępczą.

Pośrednikiem może być osoba pozyskana przez Internet, lokalny kontakt, pracownik pozyskany do współpracy i mający dostęp do określonych informacji, osoba działająca w firmie podwykonawczej, pośrednik biznesowy albo wykonawca pozornie legalnego zlecenia. W praktyce bezpieczeństwa trzeba odróżnić taki mechanizm od zwykłej działalności przestępczej, błędu pracownika czy rutynowej aktywności gospodarczej. Zawsze potrzebna jest także ocena oparta na faktach, a nie na domysłach.

Model działania przez pośredników daje organizatorowi operacji kilka korzyści. Po pierwsze zwiększa dystans między zleceniodawcą a wykonawcą, co może utrudniać atrybucję. Po drugie pozwala podzielić zadania na niewielkie części, co utrudnia rozpoznanie całej operacji, ponieważ poszczególne działania mogą wyglądać na niepowiązane. Jedna osoba może obserwować obiekt, druga sprawdzać możliwość wejścia pod określonym pretekstem, a trzecia przekazywać dane. Po trzecie wykorzystuje lokalną znajomość języka, terenu, zwyczajów oraz procedur organizacyjnych.

W wykorzystaniu agentury proxy ważnym mechanizmem jest segmentacja wiedzy (zasada *need-to-know*, czyli udzielenie dostępu wyłącznie do informacji niezbędnych do wykonania zadania). Wykonawca otrzymuje tylko tyle informacji, ile potrzebuje do realizacji konkretnego zadania. Z perspektywy ochrony obiektu oznacza to, że pojedynczy incydent może nie ujawniać zamiaru sprawcy. Znaczenia nabiera łączenie sygnałów: powtarzalnych obserwacji, nietypowych zapytań, niezgodności w dokumentach, prób obejścia procedur albo zainteresowania informacjami, które nie są potrzebne do deklarowanego celu.

Dlaczego obiekty przemysłowe są atrakcyjnym celem?

Zgodnie z ustawą o zarządzaniu kryzysowym infrastruktura krytyczna obejmuje systemy oraz wchodzące w ich skład, powiązane ze sobą funkcjonalnie obiekty – w tym obiekty budowlane – urządzenia, instalacje i usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz sprawnego funkcjonowania administracji publicznej, instytucji i przedsiębiorców. Od 4 lipca 2026 r. ustawa posługuje się także pojęciem podmiotu krytycznego, czyli operatora infrastruktury krytycznej wpisanego do wykazu podmiotów krytycznych. Z perspektywy bezpieczeństwa istotne są jednak również przedsiębiorstwa, które nie mają takiego statusu, lecz pełnią strategiczną funkcję w łańcuchu dostaw, produkcji, logistyce lub świadczeniu usług niezbędnych innym podmiotom.

Zakład przemysłowy może być atrakcyjnym celem dla zewnętrznego agresora, gdy ograniczenie jego pracy wywoła skutki wykraczające poza teren przedsiębiorstwa. W grupie ryzyka pozostają obiekty zależne od ciągłości zasilania, dostaw surowców, sprawnego transportu, automatyki przemysłowej lub wyspecjalizowanego personelu. Duże znaczenie dla uznania obiektu za strategiczny, a tym samym dla jego atrakcyjności jako potencjalnego celu, może mieć również obecność na jego terenie substancji niebezpiecznych, sąsiedztwo innych zakładów, powiązanie z infrastrukturą transportową albo rola w produkcji komponentów o ograniczonej dostępności.

Warto pamiętać, że celem nie musi być trwałe zniszczenie obiektu. Dla sprawcy wystarczające może okazać się czasowe zakłócenie pracy, wywołanie kosztownego przestoju, wymuszenie ewakuacji, przetestowanie procedur bezpieczeństwa albo obniżenie zaufania do przedsiębiorstwa. Skutek materialny może zostać dodatkowo wzmocniony przez dezinformację: fałszywe informacje o skali awarii, rzekomym zagrożeniu zdrowotnym lub braku kontroli nad sytuacją.

Od 4 lipca 2026 r. w polskim systemie ochrony infrastruktury krytycznej obowiązują także przepisy wdrażające unijną dyrektywę CER, które wprowadziły m.in. pojęcie odporności podmiotu krytycznego. Narodowy Program Ochrony Infrastruktury Krytycznej oraz jego załącznik zawierający standardy, dobre praktyki i rekomendacje pozostają ważnym punktem odniesienia dla



operatorów infrastruktury krytycznej. Mogą być również użyteczne dla przedsiębiorstw, które chcą odejść od myślenia wyłącznie o ochronie obwodowej.

Od rozpoznania do zakłócenia

Pierwszym etapem potencjalnej operacji z wykorzystaniem agentury proxy jest zwykle rozpoznanie. Może ono obejmować analizę publicznie dostępnych danych (OSINT), w tym stron internetowych, materiałów rekrutacyjnych, komunikatów prasowych, mediów społecznościowych i zdjęć. Źródłem cennych informacji może być także obserwacja ruchu pojazdów, rytmu dostaw, zmian pracowniczych czy prac serwisowych. Wiele z tych danych jest neutralnych samo w sobie. Ich znaczenie z punktu widzenia bezpieczeństwa rośnie, gdy są gromadzone systematycznie i łączone z informacjami uzyskanymi w inny sposób.

Następnie sprawca może szukać słabych punktów. Często są nimi nie tyle urządzenia, ile procedury i ludzie. Krytyczne mogą okazać się: nadmierne zaufanie do osoby podającej się za pracownika serwisu, rutynowe przepuszczanie dostawcy, zbyt szeroki dostęp dla podwykonawcy, udzielanie informacji telefonicznie lub w Internecie, brak aktualnej listy osób uprawnionych oraz presja czasu w sytuacji awaryjnej. Działania przygotowawcze mogą przyjmować postać socjotechniki. Przykładem jest podszywanie się pod kontrahenta, kuriera, przedstawiciela firmy serwisowej lub potencjalnego kandydata do pracy. Inny mechanizm to rozproszone pozyskiwanie danych: różne osoby zadają pojedyncze pytania, które dopiero po połączeniu tworzą obraz zabezpieczeń, logistyki albo organizacji pracy.

Pozyskane w ten sposób dane mogą zostać wykorzystane do przygotowania zakłóceń fizycznych, logistycznych, informacyjnych lub cybernetycznych. Zdarzenia te mogą się wzajemnie wzmacniać: incydent w systemie teleinformatycznym może ograniczyć widoczność monitoringu lub dostęp do danych, a fizycznej awarii może towarzyszyć kampania dezinformacyjna. Dlatego w ocenie ryzyka trzeba uwzględniać takie powiązania, w tym możliwość cybersabotażu i działań wymierzonych w usługi kluczowe.

Jak budować odporność?

Odpowiedzią na ryzyko wykorzystania agentury proxy wobec infrastruktury krytycznej nie jest tworzenie atmosfery podejrzliwości wobec pracowników i partnerów. Skuteczna ochrona opiera się na jasnych i skutecznych procedurach, czytelnym podziale odpowiedzialności i zdolności do wykrywania anomalii.

Najważniejszą kwestią jest określenie, co w organizacji i jej obiektach ma rzeczywiście krytyczne znaczenie dla ciągłości działania. Bieżącej analizie należy poddawać nie tylko pojedyncze obiekty fizyczne i urządzenia, ale także procesy produkcyjne, gromadzone i przesyłane dane, dostawców, punkty styku między IT i OT, osoby z uprzywilejowanym dostępem oraz zależności logistyczne. Warto zadać pytanie: co stanie się, jeśli dany element przestanie działać przez godzinę, dobę lub tydzień?

Konieczne jest również systemowe wzmacnianie bezpieczeństwa kadry zarządzającej i pracowników. Pracownicy ochrony, recepcji, administracji, utrzymania ruchu, logistyki, IT i OT powinni wiedzieć, jakie informacje są wrażliwe oraz jak reagować na nietypowe prośby. Regularne szkolenia powinny obejmować praktyczne sytuacje: weryfikację tożsamości, zasady udzielania informacji i odbioru przesyłek, współpracę z firmami serwisowymi i procedury zgłaszania podejrzanych zdarzeń.

W sposób przemyślany należy również zarządzać dostępem do obiektu firm zewnętrznych. Podwykonawca może być ważnym elementem bezpieczeństwa, ale także źródłem ryzyka, jeśli nie określono zasad weryfikacji, zakresu uprawnień, nadzoru



i odbioru prac. Uprawnienia powinny być ograniczone do niezbędnego zakresu i czasu. Szczególnej kontroli wymagają działania wykonywane poza standardowymi godzinami pracy obiektu, w okresach awarii, remontów lub zwiększonego ruchu. Osoba z zewnątrz nie powinna pozostawać bez nadzoru w strefach, do których nie ma samodzielnych uprawnień dostępu.

Kluczowa jest również współpraca ochrony fizycznej, zespołu cyberbezpieczeństwa i bezpieczeństwa informacji. Zespół ochrony musi rozumieć, że nietypowe zdarzenie fizyczne może mieć wymiar cyfrowy; zespoły IT i OT powinny zaś wiedzieć, że incydent sieciowy może być poprzedzony próbą pozyskania informacji lub dostępu na terenie zakładu. W obszarze cyberbezpieczeństwa znaczenie mają szybkie reagowanie na incydenty oraz monitorowanie podatności i prób ich wykorzystywania. Dla przedsiębiorstw oznacza to potrzebę szybkiego obiegu informacji między ogniwami odpowiedzialnymi za bezpieczeństwo.

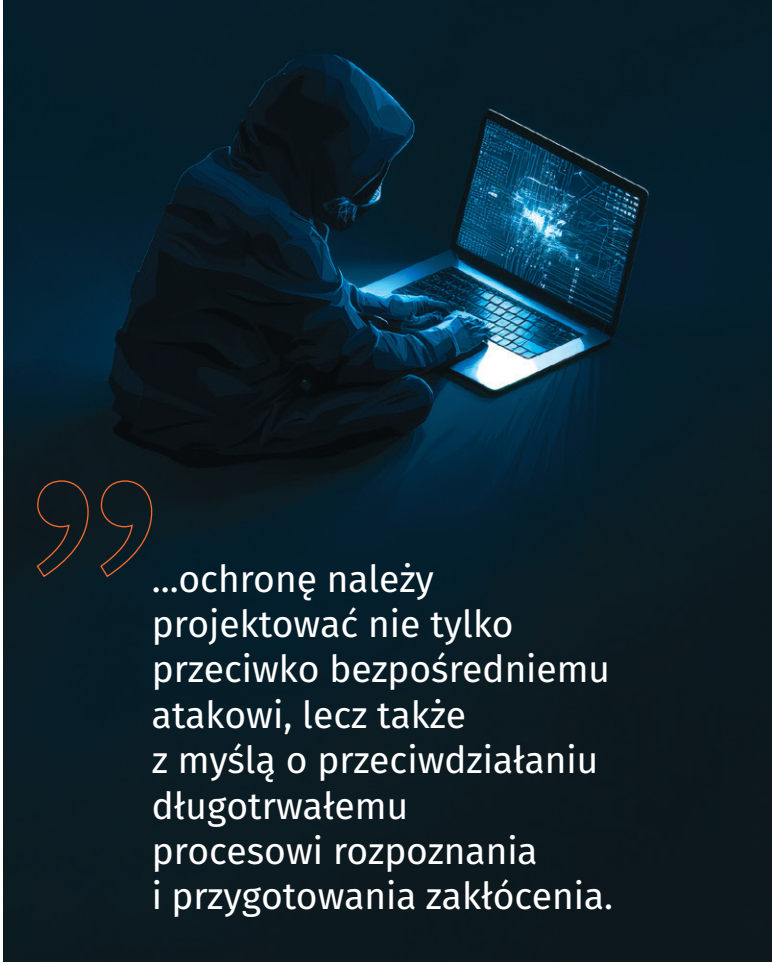
Niezwykle ważne są proste mechanizmy zgłaszania nieprawidłowości i nietypowych sytuacji. Pracownik nie powinien sam przesądzać, czy ma do czynienia z przestępstwem, błędem, czy działaniem obcego podmiotu. Powinien wiedzieć, gdzie przekazać obserwację i jakie dane zapisać.

Warto również ćwiczyć scenariusze na wypadek kryzysu. Właściwej i szybkiej reakcji wymagają nie tylko wtargnięcie albo pożar, lecz także incydent fizyczny połączony z awarią systemu, nieuprawniony dostęp pracownika firmy zewnętrznej, podejrzana aktywność w pobliżu obiektu lub fałszywa informacja o zagrożeniu. Ćwiczenia pozwalają ujawnić luki w komunikacji, odpowiedzialności i czasie reakcji. Warto je znaleźć, zanim dojdzie do rzeczywistego kryzysu.

Wnioski

Agentura proxy powinna być dziś traktowana jako jedno z kluczowych narzędzi presji hybrydowej wobec Polski. Od rozpoczęcia pełnoskalowej agresji Rosji na Ukrainę Polska stała się nie tylko państwem frontowym NATO, lecz także zasadniczym zapleczem logistycznym, tranzytowym, politycznym i społecznym wsparcia dla Ukrainy. To sprawia, że szczególnego znaczenia nabierają obiekty przemysłowe, transportowe, energetyczne, teleinformatyczne i magazynowe. Do najwrażliwszych należą zwłaszcza te, których zakłócenie mogłoby ograniczyć ciągłość dostaw, podnieść koszty funkcjonowania państwa, wywołać niepokój społeczny lub osłabić gotowość do dalszego wspierania Ukrainy. Po 2022 r. polskie służby i prokuratura ujawniały kolejne przypadki działań rozpoznawczych, dywersyjnych, sabotażowych i informacyjnych prowadzonych na rzecz rosyjskich służb specjalnych.

W takim środowisku agentura proxy umożliwia organizatorowi operacji działanie „na dystans": rozpoznanie obiektu, pozyskanie informacji, testowanie procedur, zakłócanie transportu lub realizację działań sabotażowych mogą przeprowadzać lokalni pośrednicy, osoby rekrutowane online, wykonawcy drobnych zleceń, podmioty przestępcze albo uczestnicy kampanii informacyjnych. Rozproszenie zadań, ograniczanie wiedzy poszczególnych wykonawców i wykorzystywanie pozornie zwyczajnych aktywności utrudniają szybkie rozpoznanie wspólnego schematu oraz jednoznaczne przypisanie odpowiedzialności. Dla operatorów infrastruktury krytycznej oznacza to, że ochronę należy projektować nie tylko przeciwko bezpośredniemu atakowi, lecz także z myślą o przeciwdziałaniu długotrwałemu procesowi rozpoznania i przygotowania zakłócenia.



...ochronę należy projektować nie tylko przeciwko bezpośredniemu atakowi, lecz także z myślą o przeciwdziałaniu długotrwałemu procesowi rozpoznania i przygotowania zakłócenia.

Najważniejszym zadaniem organizacji jest zatem budowanie odporności operacyjnej:

- konsekwentna ochrona informacji,
- weryfikacja personelu i podwykonawców,
- kontrola dostępu,
- bezpieczeństwo łańcucha dostaw,
- integracja ochrony fizycznej z cyberbezpieczeństwem
- sprawne zgłaszanie i analizowanie anomalii.

Nie chodzi o traktowanie każdego incydentu jako operacji obcego wywiadu, lecz o zdolność dostrzeżenia, kiedy pojedyncze, pozornie niepowiązane zdarzenia układają się we wzorzec mogący zagrażać ciągłości działania. W realiach presji hybrydowej skuteczna ochrona IK jest zarazem ochroną przedsiębiorstwa, bezpieczeństwa państwa i zdolności Polski do utrzymania wsparcia dla Ukrainy. •

mjr dr Anna Grabowska-Siwiec
Emerytowana oficer kontrwywiadu ABW. Adiunkt na Wydziale Stosunków Międzynarodowych Uniwersytetu w Białymstoku, badaczka i ekspertka w obszarze bezpieczeństwa państwa. Specjalizuje się w problematyce wywiadu i kontrwywiadu, zagrożeń hybrydowych oraz bezpieczeństwa informacyjnego. Autorka publikacji naukowych i analiz eksperckich oraz trenerka prowadząca szkolenia dla przedstawicieli administracji publicznej, biznesu i organizacji społecznych. Temat agentury proxy szerzej analizuje w swojej najnowszej książce *„Agentura proxy. Analiza przypadków, modeli działania, wpływ na bezpieczeństwo Polski"*, która ukaże się pod koniec roku.



Bezpieczeństwo fabryki to nie tylko zadanie ochrony.

Kto naprawdę odpowiada za bezpieczeństwo zakładu produkcyjnego?

Współczesny zakład produkcyjny to złożony organizm, którego sprawne funkcjonowanie zależy od wielu wzajemnie powiązanych elementów. Linie technologiczne, systemy informatyczne, infrastruktura techniczna, pracownicy oraz partnerzy zewnętrzni tworzą środowisko, w którym nawet niewielkie zdarzenie może prowadzić do zakłóceń produkcji, strat finansowych lub zagrożenia zdrowia i życia ludzi.

Adrian Kosmalski

Mimo to w wielu organizacjach nadal funkcjonuje przekonanie, że za bezpieczeństwo odpowiada przede wszystkim dział ochrony. W rzeczywistości jest ono efektem współpracy wielu obszarów organizacji i nie może być skutecznie realizowane przez jeden dział.

Bezpieczeństwo jako wspólna odpowiedzialność

Przez lata bezpieczeństwo zakładów produkcyjnych kojarzono głównie z ochroną fizyczną, kontrolą dostępu czy monitoringiem. Obecnie przedsiębiorstwa muszą mierzyć się również z cyberatakami, awariami infrastruktury, błędami ludzkimi, zagrożeniami pożarowymi oraz ryzykiem związanym z działalnością podwykonawców.

Dlatego coraz większego znaczenia nabiera zintegrowane podejście do bezpieczeństwa, w którym działania różnych działów są koordynowane w ramach wspólnej strategii zarządzania ryzykiem.

Zarząd wyznacza kierunek

Najwyższy poziom odpowiedzialności za bezpieczeństwo spoczywa na kierownictwie organizacji. To zarząd określa priorytety, zatwierdza polityki bezpieczeństwa oraz podejmuje decyzje dotyczące inwestycji w zabezpieczenia i procedury.

Zaangażowanie kadry zarządzającej wpływa również na kulturę bezpieczeństwa. Pracownicy szybko oceniają, czy bezpieczeństwo jest rzeczywistą wartością organizacji, czy jedynie formalnym obowiązkiem wynikającym z przepisów.

Kluczowa rola działów technicznych

W zakładach produkcyjnych niezwykle ważną funkcję pełnią działy utrzymania ciągłości działania i infrastruktury technicznej. Odpowiadają one za sprawność urządzeń, instalacji i systemów niezbędnych do prowadzenia działalności.

Brak odpowiedniej konserwacji, opóźnione przeglądy czy niewystarczający nadzór nad stanem technicznym mogą prowadzić do awarii, przestojów produkcyjnych oraz zagrożeń dla ludzi i środowiska.

Ochrona fizyczna i cyberbezpieczeństwo

Ochrona fizyczna nadal pozostaje jednym z filarów bezpieczeństwa zakładu. Jej zadaniem jest kontrola dostępu, monitorowanie zdarzeń i reagowanie na sytuacje kryzysowe. Coraz częściej działania te wspierają zaawansowane systemy monitoringu i analityki obrazu.

Równocześnie rozwój technologii sprawił, że bezpieczeństwo fizyczne i cyberbezpieczeństwo zaczęły się przenikać. Nieuprawniony dostęp do systemów informatycznych lub przemysłowych może prowadzić do zakłócenia pracy urządzeń, utraty danych czy zatrzymania produkcji. Dlatego skuteczne zarządzanie ryzykiem wymaga ścisłej współpracy ochrony, działów IT i specjalistów automatyki przemysłowej.

Znaczenie pracowników i firm zewnętrznych

Nawet najlepsze zabezpieczenia nie wyeliminują błędów ludzkich. Nieprzestrzeganie procedur, pozostawienie otwartych przejść czy ignorowanie sygnałów ostrzegawczych może prowadzić do poważnych konsekwencji. Dlatego budowanie świadomości bezpieczeństwa poprzez szkolenia i komunikację powinno być procesem ciągłym.

Istotną rolę odgrywają również podwykonawcy i firmy zewnętrzne, które uzyskują dostęp do infrastruktury oraz obszarów o podwyższonym ryzyku. Niezbędne są więc jasne procedury, odpowiedni nadzór i kontrola dostępu.

Skuteczność zależy od współpracy

Pytanie o to, kto odpowiada za bezpieczeństwo fabryki, nie ma jednej odpowiedzi. Zarząd wyznacza kierunek działań, działy techniczne dbają o niezawodność infrastruktury, specjaliści IT chronią środowisko cyfrowe, ochrona reaguje na zagrożenia, a pracownicy i podwykonawcy stosują obowiązujące procedury.

Dopiero współpraca wszystkich tych uczestników pozwala stworzyć skuteczny system bezpieczeństwa odpowiadający na wyzwania współczesnego przemysłu. W praktyce bezpieczeństwo nie jest zadaniem jednego działu, lecz wspólną odpowiedzialnością całej organizacji. •

Polski Związek Pracodawców Ochrona
ul. Koszykowa 61, 00-667 Warszawa
www.pzpochrona.pl
biuro@pzpochrona.pl

Ilustracje: Magnific

Zdalny serwis jest wygodny DO CZASU

Zdalny dostęp serwisowy jest jednym z tych wynalazków, których zalety docenia się szczególnie wtedy, gdy coś przestaje działać. Technik nie musi jechać przez pół Polski, by zdiagnozować awarię, zmienić konfigurację, zainstalować aktualizację albo przywrócić usługę. Kilka kliknięć i serwisant pracuje przy firmowym systemie niemal tak, jakby siedział obok. Czasem nawet skuteczniej, bo nie musi szukać miejsca do zaparkowania.

Monika Żuber-Mamakis

Problem w tym, że zdalna pomoc wymaga, by firma lub osoba potrzebująca pomocy, świadomie, z premedytacją wpuściła do swojego komputera, a często i całej sieci, kogoś z zewnątrz. Pisząc kogoś z zewnątrz, mamy na myśli zdalnego serwisanta. Może to być osoba zatrudniona przez firmę, tylko pracująca zdalnie. Ale równie dobrze może być to pracownik firmy świadczącej usługę. Jeżeli potrzebująca zdalnej pomocy organizacja nie do końca wie, kto tej pomocy udziela, kto ze zdalnego dostępu korzysta i za pomocą jakich programów, to zachowuje się tak, jakby na oścież otworzyła drzwi, a klucze do magazynu z towarem zostawiła pod wycieraczką. Nieroztropnie. Nie chodzi jednak, by rezygnować ze zdalnego serwisu. Chodzi o to, by szybkość naprawy nie oznaczała równie szybkiej utraty kontroli.

Serwisant bez walizki

Zdalny serwisant nie zawsze naprawia robota w hali. Może konfigurować kamerę, centralę kontroli dostępu, system zarządzania budynkiem, kasę, aparaturę medyczną, serwer albo program księgowy. Może być pracownikiem pomocy technicznej, administratorem dostawcy zarządzanych usług informatycznych (MSP, *Managed Service Provider*), integratorem, technikiem producenta lub podwykonawcą, o którego istnieniu klient dowiaduje się dopiero podczas incydentu.

Równie długa jest lista sposobów połączenia. Wirtualna sieć prywatna (VPN, *Virtual Private Network*), protokół pulpitu zdalnego (RDP, *Remote Desktop Protocol*), stały agent do zdalnego monitorowania i zarządzania (RMM, *Remote Monitoring and Management*), panel producenta w chmurze, a nawet aplikacja uruchamiana jednorazowo przez użytkownika. Każde z tych rozwiązań inaczej sprawdza tożsamość, przyznaje uprawnienia, zapisuje zdarzenia i instaluje aktualizacje. Wspólny jest tylko sposób dostępu do danych: spoza firmy.

Wytyczne amerykańskich i izraelskich instytucji dotyczące zabezpieczania oprogramowania zdalnego dostępu



obejmują systemy informatyczne, automatykę przemysłową i systemy sterowania, ale także pomoc techniczną, usługi chmurowe oraz firmy MSP. Autorzy zwracają uwagę na dość niewygodną prawdę: funkcje potrzebne administratorowi przydają się również włamywaczowi. Pozwalają obserwować urządzenie, wykonywać polecenia, przesyłać pliki i utrzymywać dostęp bez instalowania podejrzanego programu napisanego specjalnie do ataku. Narzędzie pozostaje legalne. Zmienia się tylko człowiek, który trzyma mysz.

Zależność od zewnętrznych firm trudno już uznać za problem marginalny. Autorzy ***Verizon Data Breach Investigations Report 2026*** (DBIR, raportu z dochodzeń dotyczących naruszeń danych) przeanalizowali ponad 31 tys. incydentów w 145 państwach, w tym co najmniej 22 tys. potwierdzonych naruszeń danych. Udział stron trzecich w naruszeniach wzrósł w badanym zbiorze o 60% i sięgnął 48%. To kategoria znacznie szersza niż zdalny serwis. Pokazuje jednak, że granice firmy kończą się dziś dużo dalej niż jej sieć i recepcja.

Policzmy wszystkie drzwi

Zdalny dostęp ma pewną szczególną właściwość: potrafi rozmnażać się po cichu. Jeden dostawca otrzymuje dostęp przez VPN, drugi stawia na TeamViewera, trzeci prosi o AnyDesk, bo „tak będzie szybciej". Po roku firma ma pięć wejść serwisowych, choć z każdego z nich korzysta inny użytkownik i w zasadzie nikt nie panuje nad wszystkimi.

Dlatego pierwszym zadaniem jest inwentaryzacja już używanych narzędzi, kont i agentów. Trzeba ustalić, kto za nie odpowiada, którym dostawcom je udostępniono i do jakich systemów można za ich pomocą dotrzeć. Lista dopuszczonych rozwiązań powinna być krótka, a odstępstwa od niej widoczne. Inaczej oficjalna procedura istnieje głównie po to, by można ją było omijać.

Legalny program nie staje się bezpieczny dlatego, że ma znane logo. W 2022 r. cyberprzestępcy podszywali się pod pomoc techniczną i nakłaniali odbiorców do uruchamiania przenośnych wersji ScreenConnect oraz AnyDesk. **Amerykańska Agencja ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury (CISA, *Cybersecurity and Infrastructure Security Agency)* wykryła powiązaną aktywność w wielu sieciach federalnych**. Programy działały bez instalacji i bez uprawnień administratora, a jako legalne narzędzia zwykle nie uruchamiały klasycznych alarmów antywirusowych. W tej kampanii służyły do oszustw finansowych. Ten sam dostęp może jednak otworzyć drogę do kradzieży danych, szpiegostwa lub przygotowania ataku ransomware.

Wspomniane wytyczne zalecają identyfikowanie zatwierdzonych programów RMM, blokowanie pozostałych i prowadzenie połączeń przez zarządzane punkty dostępu. Jeżeli dział bezpieczeństwa zna jedną platformę, a w sieci działa pięć, cztery pozostałe nie są zapasowym sposobem świadczenia usługi. Są niespodzianką. A niespodzianki w cyberbezpieczeństwie rzadko mają kokardę.



RDP czeka na chętnych

Polskie dane dobrze pokazują, jak kończy się pozostawienie zdalnego wejścia bez należytego nadzoru. W 2025 r. CERT Polska zarejestrował **260 783 incydenty bezpieczeństwa, o 152% więcej niż rok wcześniej.** Wśród nich było 179 incydentów ransomware, czyli o 21 proc. więcej niż w 2024 r. Dane obejmują cały kraj i wszystkie rodzaje organizacji, nie tylko firmy korzystające ze zdalnego serwisu. Szczegółowa analiza przynosi jednak ważną wskazówkę.

W **Raporcie rocznym CERT Polska za 2025 r**. wskazano, że w zdecydowanej większości zdarzeń, w których logi pozwoliły ustalić drogę napastników, wykorzystano usługi zdalnego dostępu bez uwierzytelniania dwuskładnikowego. W 46 zgłoszeniach dotyczących ransomware ofiara miała publicznie dostępną usługę RDP. Liczba może być zaniżona, ponieważ część zgłoszeń nie zawierała danych o infrastrukturze. W dwóch przypadkach od wystawienia RDP do Internetu do złamania hasła i infekcji minęły niespełna dwa tygodnie.

Nie każdy taki incydent zaczyna się od konta serwisanta. Dla zespołu bezpieczeństwa mechanizm jest jednak podobny. Zdalny dostęp serwisowy jest dodatkowym wejściem do firmowych systemów. To, czy będzie bezpieczny, zależy od sposobu uwierzytelniania, zakresu przyznanych uprawnień, aktualności oprogramowania oraz możliwości wykrywania nadużyć. Firma może ufać kontrahentowi, ale nie powinna automatycznie ufać każdemu połączeniu wykonanemu z jego konta – hasło mogło zostać wykradzione, a komputer serwisanta zainfekowany.

Krótki termin ważności ma sens

Najbezpieczniejsze konto serwisowe to takie, z którego nikt nie korzysta. W tym przypadku bezczynność jest zaletą. Dostęp powinien być uruchamiany na podstawie konkretnego zgłoszenia, dla imiennie wskazanej osoby i tylko na czas potrzebny do wykonania zadania. Po zakończeniu prac wygasa automatycznie. Jeśli naprawa się przedłuża, ktoś po stronie klienta świadomie przedłuża również zgodę.

Wspólne konto „SERWIS" może być wygodne, dopóki nie trzeba ustalić, kto naprawdę się zalogował. Hasło przekazywane kolejnym technikom potrafi przeżyć zakończenie umowy, zmianę pracodawcy, a niekiedy także urządzenie, dla którego zostało utworzone. Każda osoba powinna korzystać z własnej tożsamości, a dostęp uprzywilejowany wymagać uwierzytelniania wieloskładnikowego (MFA, *Multi-Factor Authentication*), najlepiej odpornego na wyłudzanie danych logowania.

Zasada jest znana. Gorzej z wykonaniem. W analizowanych przez autorów **DBIR 2026 ekspozycjach środowisk chmurowych** pełne usunięcie braku albo błędnej konfiguracji MFA potwierdzono tylko u 23% zewnętrznych dostawców. Dostęp czasowy i MFA warto więc wpisać do umowy, ale na tym nie kończyć. Ankieta bezpieczeństwa przyjmie niemal każdą odpowiedź. System już niekoniecznie.

Jedno zadanie zamiast całej sieci

Serwisant kamery nie potrzebuje dostępu do systemu kadrowego. Technik windy nie musi zaglądać do serwera kopii zapasowych, a administrator programu księgowego do centrali kontroli dostępu. Wszystko wydaje się oczywiste, dopóki taka osoba nie otrzyma dostępu do firmowej sieci przez zwykły VPN.

Zasada stosowania minimalnych uprawnień ogranicza zarówno funkcje, jak i zasięg dostępu do właściwego systemu, konkretnego urządzenia lub do przeprowadzenia w określonym terminie niezbędnych operacji. Jeśli diagnoza wymaga wyłącznie podglądu, konto nie powinno pozwalać na zmianę konfiguracji. Połączenie warto prowadzić przez kontrolowaną stację pośredniczącą lub środowisko wirtualne. Można wtedy oddzielić komputer serwisanta od zasobów firmy, narzucić zestaw dozwolonych aplikacji oraz ograniczyć kopiowanie plików i zawartości schowka.

Potrzebna jest również segmentacja sieci. Bez niej uprawnienia bywają wąskie tylko na ekranie logowania, a dalszy ruch po firmowych systemach stoi otworem. Przekonała się o tym sieć handlowa Target w 2013 r. Napastnicy posłużyli się danymi dostępowymi firmy obsługującej instalacje chłodnicze oraz ogrzewanie, wentylację i klimatyzację (HVAC, *Heating, Ventilation and Air Conditioning*). Konto nie służyło do sterowania temperaturą w sklepach, lecz między innymi do rozliczeń i obsługi projektów.

Analiza komisji Senatu Stanów Zjednoczonych wskazywała, że niedostateczna izolacja mogła umożliwić przejście do wrażliwszych części sieci. Target potwierdził narażenie danych około 40 mln kart płatniczych, a osobny zbiór danych kontaktowych obejmował do 70 mln osób. Stanowisko wpisane na identyfikatorze dostawcy nie zatrzymuje ruchu w sieci. Do tego nadal potrzebne są reguły dostępu.

Serwisant pracuje, system pamięta

Informacja, że konto „SERWIS" zalogowało się o 10.17, nie jest jeszcze historią sesji. To zaledwie jej tytuł. Pełny zapis powinien pozwolić ustalić tożsamość osoby i jej pracodawcy, urządzenie źródłowe, adres IP, czas rozpoczęcia i zakończenia, numer zgłoszenia, system docelowy, wykonane polecenia, przesłane pliki oraz zmiany konfiguracji. W systemach o dużym znaczeniu uzasadnione może być nagranie obrazu sesji albo przynajmniej poleceń administracyjnych.

Wytyczne dotyczące zabezpieczania oprogramowania zdalnego dostępu zalecają, by klient zachował wgląd w aktywność serwisanta, monitorował i audytował jego konta, a narzędzie RMM nie pozwalało usuwać ani zmieniać dzienników zdarzeń. Dobrą praktyką jest również zatwierdzanie rozpoczęcia sesji przez osobę po stronie klienta oraz alarm, gdy połączenie następuje poza uzgodnionym oknem, z nowego kraju lub do nietypowego zasobu.

Nagranie nie służy temu, by ktoś przez trzy godziny patrzył technikowi na ręce. Ma pozwolić wykryć nietypowe działania i później rozstrzygnąć, czy zmianę wykonał serwisant, jego skrypt, czy osoba używająca skradzionej tożsamości. Jeżeli zapis może obejmować dane osobowe pracowników lub klientów, należy określić jego cel, zakres, okres przechowywania oraz krąg osób uprawnionych do odtworzenia, zgodnie z zasadami **ogólnego rozporządzenia o ochronie danych (RODO).** Bezpieczeństwo nie zwalnia z ochrony prywatności. Nawet jeśli nagranie jest bardzo interesujące.

Dostawca też wymaga kontroli

Można wzorowo chronić konto po stronie klienta, a mimo to paść ofiarą ataku prowadzonego przez platformę serwisową. Serwisant nie robi nic ryzykownego, jego hasło nigdzie nie wypłynęło, a do ataku i tak dochodzi. Pokazał to incydent BeyondTrust z 2024 r.

Napastnicy wykorzystali nieznaną wcześniej lukę w aplikacji innej firmy, aby dostać się do chmurowych zasobów BeyondTrust. Stamtąd wykradli należący do dostawcy infrastrukturalny klucz dostępu do interfejsu programowania aplikacji (API, *Application Programming Interface*). Umożliwiał on resetowanie lokalnych haseł w środowiskach usługi Remote Support. Nie był to więc klucz konkretnego technika, lecz cyfrowe poświadczenie do technicznego zaplecza platformy.

Za jego pomocą napastnicy dostali się do stacji roboczych wybranych klientów. Amerykański Departament Skarbu poinformował, że uzyskali dostęp do części nieutajnionych dokumentów, i **uznał zdarzenie za poważny incydent. BeyondTrust podał później, że incydent dotknął 17 klientów;** firma unieważniła klucz i odizolowała zaatakowane środowiska. Ten przypadek nie obciąża konkretnego serwisanta. Obciąża model zaufania, w którym infrastruktura dostawcy staje się częścią drogi do systemów klienta.

> W Raporcie rocznym CERT Polska za 2025 r. wskazano, że w zdecydowanej większości zdarzeń, w których logi pozwoliły ustalić drogę napastników, wykorzystano usługi zdalnego dostępu bez uwierzytelniania dwuskładnikowego.

Jeszcze większy zasięg może mieć atak na dostawcę obsługującego kolejnych usługodawców. Po incydencie Kaseya VSA z lipca 2021 r. producent podał, że naruszenie objęło **mniej niż 60 jego bezpośrednich klientów korzystających z lokalnej wersji systemu oraz mniej niż 1500 firm obsługiwanych dalej przez część z nich.** Zaufane narzędzie administracyjne stało się kanałem dystrybucji ransomware.

Dostęp zdalny jest zatem jednocześnie problemem tożsamości, konfiguracji i podatności. W DBIR 2026 wykorzystanie luk odpowiadało za 31% początkowych wejść w analizowanych naruszeniach, a nadużycie poświadczeń za 13%. Tylko 26% krytycznych podatności obecnych w prowadzonym przez CISA katalogu znanych luk aktywnie wykorzystywanych w atakach zostało w badanym zbiorze całkowicie usuniętych. Mediana pełnej naprawy wyniosła 43 dni. Serwer zdalnego dostępu dostępny z Internetu nie powinien czekać w zwykłej kolejce aktualizacji. Napastnicy nie przestrzegają harmonogramu prac utrzymaniowych.

Umowa przed incydentem

Umowa serwisowa zwykle bardzo dokładnie opisuje czas reakcji i dostępność serwisanta. Znacznie rzadziej wyjaśnia, za pomocą jakich narzędzi będzie się on łączyć zdalnie oraz czy korzysta z podwykonawców, kto zatwierdza ich konta, gdzie trafiają logi, jak szybko klient zostanie powiadomiony o naruszeniu i kto może natychmiast odebrać uprawnienia do zdalnego dostępu. Zdanie, że usługodawca „stosuje dobre praktyki", brzmi uspokajająco. Ale tak dokładnie, to jakie?

Podział obowiązków powinien być konkretny. Dostawca odpowiada za bezpieczeństwo swoich urządzeń, personelu, kont i narzędzi. Klient kontroluje segmentację własnej sieci, zakres przyznanych praw, zatwierdzanie sesji i odbieranie dostępu. Obie strony muszą uzgodnić sposób zgłaszania incydentów, ochronę

Ilustracje: Marta Kołodziejak / A&S AI Studio

Paszport sesji serwisowej

Zanim na ekranie pojawi się komunikat „połączono", zgłoszenie powinno odpowiedzieć na poniższe pytania. Puste pole oznacza, że organizacja nie wie jeszcze dokładnie, komu, po co albo na jakich warunkach otwiera dostęp.

- **Kto się łączy?** Imię, nazwisko, firma i imienne konto bez współdzielonego hasła.
- **Na czyje zlecenie?** Numer zgłoszenia oraz osoba zatwierdzająca po stronie klienta.
- **Po co?** Konkretny zakres diagnozy, naprawy lub aktualizacji.
- **Dokąd?** Wskazane urządzenie, aplikacja albo wydzielona grupa zasobów.
- **Na jak długo?** Godzina rozpoczęcia oraz automatyczne wygaśnięcie dostępu.
- **Z jakiego urządzenia?** Sprzęt zarządzany przez dostawcę i spełniający uzgodnione wymagania.
- **Jaką drogą?** Zatwierdzone narzędzie, kontrolowany punkt wejścia i MFA.
- **Z jakimi prawami?** Podgląd lub zmiana konfiguracji, z osobną zgodą na przesyłanie plików i uruchamianie skryptów masowych.
- **Co będzie zapisywane?** Czas, cel i przebieg sesji, wykonane polecenia, transfery oraz wprowadzone zmiany.
- **Jaki będzie sposób zamknięcia zgłoszenia?** Wylogowanie, odebranie uprawnień, potwierdzenie zmian i zachowanie logów.

materiału dowodowego, odtwarzanie usługi oraz zasady angażowania podwykonawców. **Wytyczne dotyczące zdalnego dostępu zalecają umowne określenie obowiązków informacyjnych** oraz zachowanie przez klienta możliwości monitorowania i audytowania kont dostawcy.

Jeżeli serwisant przetwarza dane osobowe w imieniu klienta, relację trzeba ocenić również na gruncie RODO. Europejska Rada Ochrony Danych przypomina, że administrator powinien znać podmioty przetwarzające i dalszych podwykonawców, wybierać firmy dające wystarczające gwarancje oraz okresowo je weryfikować. Obowiązek jest ciągły, a zakres kontroli zależy od ryzyka.

W sektorze finansowym **unijne rozporządzenie o operacyjnej odporności cyfrowej sektora finansowego (DORA, *Digital Operational Resilience Act*)** wymaga włączenia ryzyka związanego z zewnętrznymi dostawcami usług informatycznych do ram zarządzania ryzykiem. Umowa z firmą zewnętrzną nie zwalnia instytucji finansowej z odpowiedzialności za zgodność. Outsourcing bywa skutecznym sposobem wykonywania zadań. Nie jest sposobem na outsourcing odpowiedzialności.

Prawo nie zna zdalnego alibi

Od 3 kwietnia 2026 r. obowiązuje w Polsce **nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa,** wdrażająca dyrektywę NIS2 (*Network and Information Systems Directive 2,* drugą dyrektywę w sprawie bezpieczeństwa sieci i systemów informacyjnych). Regulacja nie obejmuje automatycznie każdej firmy korzystającej ze zdalnego serwisu. Status podmiotu kluczowego lub ważnego zależy między innymi od sektora, rodzaju działalności i wielkości organizacji. Ustawa pokazuje jednak kierunek, w którym zmierza rynkowy standard.

Podmioty objęte regulacją muszą uwzględniać bezpieczeństwo łańcucha dostaw, kontrolę dostępu, zarządzanie aktywami, aktualizacje i tam, gdzie jest to uzasadnione MFA. Powinny brać pod uwagę podatności dostawcy oraz jakość jego produktów i usług. Ustawa definiuje dostawcę usług zarządzanych jako podmiot, który instaluje, eksploatuje lub konserwuje systemy, wspierając klienta na miejscu albo zdalnie. Kierownik podmiotu kluczowego lub ważnego zachowuje odpowiedzialność także wtedy, gdy część obowiązków powierzono innej osobie.

Podobną zasadę zawiera **art. 21 dyrektywy NIS2,** który wymienia bezpieczeństwo łańcucha dostaw oraz relacji z bezpośrednimi dostawcami i usługodawcami wśród środków zarządzania ryzykiem. Usługę można kupić na zewnątrz. Jednak odpowiedzialności za to, komu i na jakich warunkach firma daje dostęp do własnych systemów, zawsze jednak pozostaje na jej barkach. Nie da się jej ani oddać, ani sprzedać.

Klucz bardzo jednorazowy na jedną wizytę

Zdalny serwis jest wygodny. Nie ma sensu z niego rezygnować tylko z obawy przed ewentualnym ryzykiem. Po prostu wystarczy pozbawić go trzech cech, szczególnie wygodnych dla napastnika: anonimowości, stałości i nieograniczonego zasięgu. Imienne konto z MFA, dostęp przyznawany na czas zgłoszenia, wąskie uprawnienia, kontrolowany punkt wejścia i zapis działań nie utrudnią dobrze zorganizowanej usługi. Utrudnią natomiast działanie osobie, która zechce podszyć się pod zdalnego serwisanta.

To prawda, że zazwyczaj najsłabszym ogniwem jest człowiek. Dotyczy to także pracy zdalnej, tyle że nie chodzi o ludzkie niedociągnięcia, a raczej o fakt, iż firma zna nazwę dostawcy, lecz nie zna osób, kont, urządzeń i podwykonawców korzystających z jego dostępu. Przecież jeśli nawet prywatnie zapraszamy kogoś do domu, nie oznacza przecież, że dajemy mu klucz na zawsze i do wszystkiego. •

POLON-ALFA



CNBOP-PIB

PIERWSZY W POLSCE **CERTYFIKOWANY**

PANEL OBSŁUGI DLA STRAŻY POŻARNEJ

POSP 6000

- **PEŁNA INTEGRACJA Z SYSTEMEM SYGNALIZACJI POŻAROWEJ**
  Panel współpracuje bezpośrednio z centralą – wszystkie dane są przesyłane w czasie rzeczywistym, zapewniając aktualny obraz sytuacji.
- **NATYCHMIASTOWY DOSTĘP DO KLUCZOWYCH INFORMACJI**
  Panel instalowany w odległości maks. 5 m od wejścia głównego umożliwia szybkie podjęcie działań już od pierwszych sekund akcji ratowniczej.
- **WSPARCIE DLA WSZYSTKICH SŁUŻB RATOWNICZYCH**
  Intuicyjna obsługa i przejrzystość informacji wspierają działania zarówno straży pożarnej, jak i operatorów technicznych czy personelu ochrony.

POLON-ALFA | 85-861 Bydgoszcz, ul. Glinki 155 | www.polon-alfa.com



Głos branży

Monitoring z zaawansowaną analityką

MARCIN ZUCHNIAK
BCS



Cyberbezpieczeństwo przestaje dotyczyć wyłącznie komputerów, serwerów i danych. Rozwój sztucznej inteligencji (AI), analityki obrazu, dronów i urządzeń IoT sprawia, że świat cyfrowy coraz mocniej łączy się z fizycznym. Kamera już nie tylko rejestruje obraz – może go analizować, interpretować, wykrywać zagrożenia i inicjować określone działania. To otwiera ogromne możliwości, ale również tworzy nową klasę zagrożeń.

Jeszcze niedawno system CCTV przede wszystkim rejestrował obraz, a człowiek decydował, co się na nim znajduje. Dziś AI potrafi wykrywać ludzi, pojazdy, wtargnięcia, pozostawione przedmioty czy nietypowe zachowania.

Pojawia się więc pytanie: co się stanie, jeśli ktoś nie zaatakuje samej kamery, lecz sposób, w jaki interpretuje ona rzeczywistość?

Urządzenie może działać technicznie prawidłowo, a mimo to przekazywać błędne informacje. To nowa kategoria zagrożeń – atak na „zmysły" systemu AI.

W klasycznym cyberataku celem były dane, konta lub serwery. W inteligentnym systemie bezpieczeństwa konsekwencje mogą być znacznie bardziej namacalne i nieprzewidywalne.

Wyobraźmy sobie monitoring obiektu, w którym AI wykrywa intruza i automatycznie uruchamia alarm. Jeżeli algorytm zostanie wprowadzony w błąd, system może nie tylko nie zauważyć zagrożenia, ale również podjąć niewłaściwą decyzję.

Jeszcze większe znaczenie ma to w przypadku urządzeń autonomicznych. Kamera z AI podejmuje decyzję i wykonuje określone działanie.

Ten schemat może w przyszłości sterować drzwiami, szlabanem, automatyką budynku, a nawet autonomicznym dronem. W tym momencie cyberbezpieczeństwo staje się cyberbezpieczeństwem fizycznym.

Współczesny system monitoringu wizyjnego może obejmować kamery, serwery, VMS, analitykę AI, sieć, chmurę i integrację z innymi systemami. Dlatego nie wystarczy już zapytać: „Czy kamera jest bezpieczna?". Trzeba zapytać: „Czy bezpieczny jest cały łańcuch przetwarzania informacji?".

To podejście jest szczególnie istotne w profesjonalnych rozwiązaniach, takich jak BCS Ultra czy BCS FLEX, gdzie monitoring może być łączony z zaawansowaną analityką, automatyką i innymi systemami bezpieczeństwa.

Sztuczna inteligencja będzie pomagała nie tylko bronić systemów. Będzie również wykorzystywana przez atakujących – do rozpoznania infrastruktury, wyszukiwania podatności, phishingu czy socjotechniki.

Dlatego podstawowe zasady pozostają kluczowe: aktualne oprogramowanie, silne uwierzytelnianie, segmentacja sieci, kontrola uprawnień i świadome zarządzanie urządzeniami.

Przyszłość branży to nie tylko ochrona obrazu i danych. To również ochrona wiarygodności informacji, decyzji podejmowanych przez AI oraz fizycznych skutków tych decyzji.

Najważniejsze pytanie przyszłości może więc brzmieć:

Czy możemy ufać temu, co nasz system zobaczył, zrozumiał i postanowił zrobić? •

Cyberatak, sabotaż, dron, awaria czy przerwanie łańcucha dostaw mogą dziś uruchomić zdarzenia, których skutki wykraczają daleko poza pojedynczy incydent. W świecie, w którym zagrożenia coraz częściej łączą się ze sobą, odporność zakładu staje się równie ważna jak jego bieżąca ochrona. Jak zatem budować bezpieczeństwo, które sprawdzi się nie tylko w normalnych warunkach, ale również wtedy, gdy zawiodą standardowe scenariusze? Czy kluczowa jest technologia, integracja systemów, procedury, a może przede wszystkim ludzie i kultura bezpieczeństwa? O to, co dziś naprawdę decyduje o odporności zakładu przemysłowego, zapytaliśmy ekspertów. Ich odpowiedzi pokazują różne perspektywy, ale wspólny kierunek jest wyraźny: **bezpieczeństwo trzeba traktować jako proces, a nie gotowy system.**



Odporność organizacji na zagrożenia



GRZEGORZ MISIAK
Corning

Co jest dziś kluczowe w budowaniu odporności zakładu przemysłowego na współczesne zagrożenia? Na tak postawione pytanie można odpowiedzieć: każdy element ma swoje znaczenie – w zależności od warunków i kontekstu.

Peter Drucker powiedział kiedyś, że rolą menedżerów, zarządu jest podejmowanie ryzyka w prowadzeniu biznesu, ale – podkreślał on – ryzyka właściwego. Próba całkowitego wyeliminowania ryzyka prowadzi do stagnacji. Z drugiej strony nadmierne ryzykowanie nie różni się od hazardu i jest przejawem niekompetencji.

W idealnej sytuacji osoba odpowiedzialna za bezpieczeństwo powinna dostarczać, oparte na analizach, informacje pozwalające zarządowi z jednej strony w pełni świadomie brać pod uwagę ryzyka związane z bezpieczeństwem prowadzonego biznesu, a z drugiej – unikać ryzyk, na które nie może sobie pozwolić.

Oczywiście każda organizacja będzie miała inne ryzyka, inny będzie też poziom ich akceptowalności czy sposoby ich ograniczenia.

I tu wracamy do podstaw, czyli czegoś, co określiłbym jako dynamiczną lub ciągłą analizę ryzyka, uwzględniającą wiele zmiennych elementów, począwszy od lokalizacji zakładu, materiałów używanych do produkcji czy produktu końcowego.

W dzisiejszym dynamicznym środowisku parametry zewnętrzne zmieniają się bardzo często i bardzo szybko, dlatego praktycznie codziennie powinniśmy dodawać do naszej analizy nowe elementy i weryfikować, jak wpływa to na naszą organizację.

Przykładem może być zwiększająca się liczba przypadków pożarów, uszkodzeń infrastruktury czy sabotażu. Czy dotyczy to zakładów o profilu podobnym do naszego? Czy analizujemy te przypadki na bieżąco? Czy przypadki te zdarzają się w miejscach mających ze sobą coś wspólnego, czy zupełnie przypadkowych?

Taka ciągła analiza powinna pozwolić na proaktywne działania wyprzedzające, a nie reaktywne, podejmowane dopiero wówczas, gdy incydent zdarzy się „u nas".

Oczywiście ważnym elementem jest system ochrony oparty na „minimalnych standardach", które są wystarczające dla funkcjonowania zakładu w normalnych warunkach.

I tutaj powinniśmy wziąć pod uwagę kulturę organizacyjną, kulturę bezpieczeństwa: na ile możemy się opierać na naszych pracownikach, na ich świadomości i odpowiedzialności, a na ile działania opierać na systemie bezpieczeństwa.

Dodatkowym elementem systemu bezpieczeństwa powinny być szkolenia zespołu ochrony i testy systemu sprawdzające jego odporność na różne zdarzenia i incydenty.

Podsumowując: nie ma jednego elementu, który decydowałby o odporności organizacji na zagrożenia. Każda organizacja jest inna i każda nie tylko powinna świadomie wybrać elementy, na których chce oprzeć swoje bezpieczeństwo, ale także nie wahać się ich zmieniać, ulepszać czy odrzucać w miarę zmieniających się warunków. System bezpieczeństwa nie powinien być postrzegany jako mechanizm, a jako proces. •

Bezpieczeństwo jako zintegrowany ekosystem

JAROSŁAW DURKACZ
Polpharma



Współczesny zakład przemysłowy funkcjonuje w środowisku coraz bardziej złożonych zagrożeń. Obok klasycznych ryzyk, takich jak awarie techniczne, pożary czy błędy ludzkie, pojawiają się zagrożenia cybernetyczne, sabotaż, zakłócenia łańcuchów dostaw, ekstremalne zjawiska pogodowe oraz napięcia geopolityczne. W takich warunkach odporność organizacji przestaje być wyłącznie domeną działów bezpieczeństwa. Staje się jednym z kluczowych elementów strategii biznesowej.

Często pojawia się pytanie, co ma dziś największe znaczenie: nowoczesne technologie, integracja systemów, odpowiednie procedury czy właściwie przygotowani ludzie. W mojej opinii wszystkie te elementy są ważne, ale same w sobie nie gwarantują bezpieczeństwa. Nawet najbardziej zaawansowany monitoring, system kontroli dostępu czy rozwiązania oparte na sztucznej inteligencji nie zapewnią odporności, jeśli organizacja nie potrafi właściwie interpretować sygnałów ostrzegawczych i reagować na pojawiające się zagrożenia.

Dlatego fundamentem nowoczesnej odporności jest zdolność do przewidywania. Organizacja musi stale analizować otoczenie, identyfikować słabe punkty, monitorować trendy oraz rozumieć zależności pomiędzy procesami technologicznymi, bezpieczeństwem fizycznym, cyberbezpieczeństwem i ciągłością działania. Celem nie jest wyeliminowanie każdego zagrożenia, lecz zbudowanie systemu, który pozwoli wykryć je odpowiednio wcześnie i ograniczyć skutki incydentu.

Równie istotna jest szybkość reakcji. O sile organizacji nie decyduje brak incydentów, lecz sposób, w jaki sobie z nimi radzi. Zakład odporny to taki, który posiada jasne procedury, przeszkolony personel, sprawne kanały komunikacji oraz zdolność do podejmowania decyzji pod presją czasu. Technologia powinna wspierać te działania, dostarczając informacji i automatyzując procesy, ale nie może zastąpić kompetencji ludzi.

W praktyce najwyższy poziom odporności osiągają organizacje, które traktują bezpieczeństwo jako zintegrowany ekosystem. Łączą nowoczesne technologie, skuteczne procedury, świadomy personel oraz kulturę ciągłego doskonalenia. •

Bezpieczeństwo pracowników ochrony w branży przemysłowej

DOMINIKA KACZMARCZYK-ŻÓŁCIAK
Specjalista ds. BHP



Pracownik ochrony w zakładzie przemysłowym wykonuje swoje zadania w otoczeniu maszyn, instalacji, hałasu, substancji chemicznych i procesów technologicznych. Dlatego standardowe przygotowanie do pracy w ochronie nie wystarczy. Bezpieczeństwo trzeba zorganizować pod konkretny obiekt.

Najlepiej zacząć od wizji lokalnej. Przed rozpoczęciem usługi przedstawiciel firmy ochrony wraz z osobą odpowiedzialną za bezpieczeństwo w zakładzie powinien przejść wszystkie posterunki i trasy obchodów. Trzeba wskazać strefy niebezpieczne, miejsca z zakazem wejścia, wymagane środki ochrony indywidualnej oraz zagrożenia, z którymi pracownik może zetknąć się podczas normalnej pracy i interwencji. Te informacje powinny znaleźć odzwierciedlenie w ocenie ryzyka zawodowego. Uniwersalna karta ryzyka, stosowana na każdym obiekcie, nie spełni swojej funkcji.

Drugim krokiem jest praktyczny instruktaż obiektowy. Nowemu pracownikowi należy pokazać bezpieczne trasy, wyjścia ewakuacyjne, punkty zbiórki oraz sposób alarmowania. Jeżeli na hali obowiązują ochronniki słuchu, okulary, hełm czy określone obuwie, należy wyposażyć w nie również ochronę, jeśli pracownik wchodzi do tej strefy.

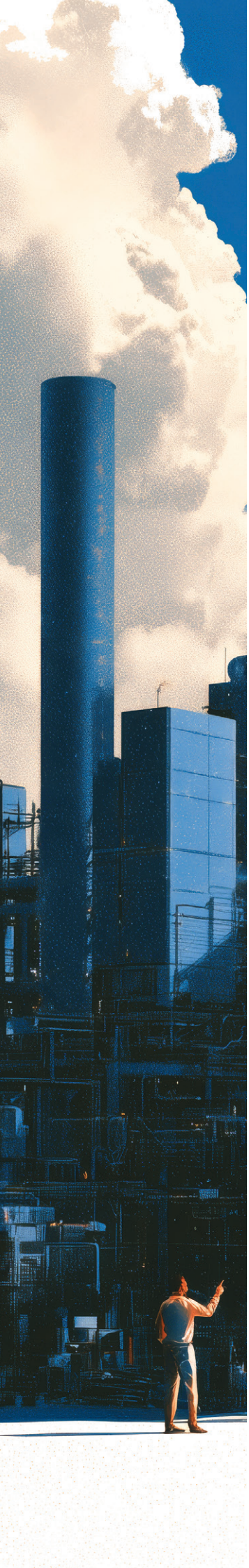
Trzeci element to jasne procedury reagowania. Pracownik powinien wiedzieć nie tylko, co zrobić, ale również czego robić nie wolno. Przy wycieku nieznanej substancji nie powinien podchodzić, aby ustalić jego źródło. Powinien zabezpieczyć dostęp i uruchomić ustaloną procedurę alarmową. Podobnie przy awarii maszyny czy instalacji – zadaniem ochrony nie jest usuwanie awarii, lecz właściwe przekazanie informacji i zabezpieczenie strefy.

Dobrym rozwiązaniem jest krótka karta postępowania awaryjnego dostępna na posterunku: kogo powiadomić, pod jaki numer zadzwonić, co zabezpieczyć, gdzie kierować ludzi i kiedy bezwzględnie nie wchodzić do zagrożonej strefy. Procedury warto również ćwiczyć.

Ostatnia zasada to aktualizacja. Nowa linia technologiczna, remont, zmiana trasy obchodu czy rozpoczęcie prac szczególnie niebezpiecznych powinny oznaczać ponowną ocenę wpływu tych zmian na pracę ochrony.

Dobre BHP w ochronie przemysłowej można więc sprowadzić do prostego schematu: poznaj obiekt, oceń rzeczywiste zagrożenia, przygotuj pracownika, określ granice jego działania i reaguj na zmiany. Dokumentacja jest ważna, ale bezpieczeństwo zaczyna się tam, gdzie zapisane zasady rzeczywiście działają na obiekcie. •





Kluczowa jest świadomość zagrożeń



TOMASZ GONTA
Animex Foods

Budowanie odporności zakładu przemysłowego na współczesne zagrożenia nie może sprowadzać się wyłącznie do wyboru odpowiednich technologii czy wdrożenia kolejnych systemów zabezpieczeń. Kluczowa jest przede wszystkim świadomość, że zagrożenia globalne i lokalne coraz częściej wzajemnie się przenikają i mogą oddziaływać na zakład w sposób pośredni, a ich skutki mogą wykraczać daleko poza pojedynczy incydent.

Dlatego punktem wyjścia powinno być systematyczne rozpoznawanie zagrożeń, analiza ich wzajemnych zależności oraz ocena tego, w jaki sposób mogą one wpłynąć na ciągłość działania organizacji.

Dopiero na tej podstawie należy dobierać środki ochrony technicznej i organizacyjnej. Przy ich wyborze cena nie powinna być jedynym, a często nawet podstawowym kryterium, co jest często spotykanym błędem. Ważniejsze są jakość, niezawodność, możliwość integracji z pozostałymi systemami, cykl życia rozwiązania, a także jego pochodzenie i związane z nim ryzyka dotyczące bezpieczeństwa.

Równie ważne jest przygotowanie ludzi. Procedury muszą być nie tylko opracowane, ale przede wszystkim znane, przećwiczone i regularnie weryfikowane. Zespoły odpowiedzialne za ochronę obiektu powinny być szkolone i testowane w warunkach możliwie zbliżonych do rzeczywistych, z wykorzystaniem różnych scenariuszy i założeń. Pozwala to sprawdzić nie tylko czas reakcji, ale również komunikację, współpracę i zdolność do podejmowania decyzji w warunkach presji i niepełnej informacji.

Ostatecznie odporność zakładu tworzą jednak nie same systemy i procedury, lecz ludzie oraz kultura bezpieczeństwa. Często mówi się, że najsłabszym ogniwem jest człowiek.

Organizacja odporna to taka, w której każdy rozumie swoją rolę w ochronie zakładu, potrafi rozpoznać sygnały ostrzegawcze i wie, jak reagować. Połączenie świadomości zagrożeń, właściwie dobranych technologii, przygotowanych zespołów i kultury bezpieczeństwa daje największą szansę na przewidywanie zagrożeń, ograniczenie ich skutków i szybki powrót do normalnego funkcjonowania po incydencie. •

Jak zbudować odporność zakładu



WINCENTY IGNATOWSKI
Cemex

Współczesny zakład przemysłowy funkcjonuje w środowisku zagrożeń znacznie bardziej złożonym niż jeszcze kilka lat temu. Kradzież, sabotaż czy nieuprawnione wejście nadal pozostają realnym ryzykiem, ale coraz częściej łączą się z cyberatakami, dezinformacją, zakłóceniami infrastruktury, awariami oraz zagrożeniami hybrydowymi. W przypadku obiektów położonych relatywnie blisko wschodniej granicy należy brać pod uwagę również skutki zdarzeń militarnych, w tym intencjonalnego lub przypadkowego użycia dronów czy rakiet oraz zakłóceń GPS i łączności.

Dlatego odporności zakładu nie można budować wyłącznie poprzez instalowanie kolejnych kamer, systemów kontroli dostępu czy innych zabezpieczeń technicznych. Technologia jest niezbędna, ale jej wartość ujawnia się dopiero wtedy, gdy CCTV, kontrola dostępu, systemy alarmowe, analityka obrazu, AI i centrum operacyjne SOC tworzą jeden spójny ekosystem pozwalający szybko wykryć zdarzenie, zweryfikować je, ocenić ryzyko i uruchomić właściwą reakcję.

Równie istotne są procedury i ludzie. Nawet najlepszy system nie zastąpi operatora, który potrafi właściwie ocenić sytuację, ani menedżera zdolnego podjąć szybką decyzję. Procedury muszą być proste, znane i regularnie ćwiczone, także dla scenariuszy trudnych do przewidzenia: blackoutu, utraty łączności, równoczesnych incydentów czy działania przy ograniczonych zasobach.

Kluczowa staje się jednak zdolność przewidywania. Security Manager powinien stale analizować otoczenie, identyfikować słabe sygnały i przygotowywać organizację, zanim incydent przerodzi się w kryzys.

Technologia daje możliwości. Integracja systemów daje obraz sytuacji. Procedury nadają działaniu porządek, a ludzie pozwalają wykorzystać te narzędzia w praktyce. Prawdziwa odporność zaczyna się jednak wtedy, gdy organizacja potrafi połączyć te elementy pod presją czasu, właściwie zinterpretować niepełne informacje i podjąć decyzję, zanim zdarzenie stanie się kryzysem. •

Budowanie kultury bezpieczeństwa



TOMASZ GUZIKOWSKI
QEMETICA Global Solutions

W dyskusji o bezpieczeństwie zakładów przemysłowych bardzo często koncentrujemy się na technologiach: systemach kontroli dostępu, monitoringu wizyjnym, cyberbezpieczeństwie, rozwiązaniach OT czy nowoczesnych platformach zarządzania incydentami. Wszystkie te elementy są oczywiście niezwykle ważne, ale z mojego doświadczenia wynika, że same technologie nie budują odporności organizacji.

Prawdziwa odporność zakładu przemysłowego jest wynikiem połączenia czterech elementów: właściwie dobranych technologii, zintegrowanych procesów, dobrze przygotowanych ludzi oraz zdolności do przewidywania zagrożeń i skutecznego reagowania na incydenty.

Współczesne zagrożenia rzadko występują w izolacji. Awaria techniczna może stać się incydentem bezpieczeństwa, cyberatak może doprowadzić do zatrzymania produkcji, a zakłócenia w łańcuchu dostaw mogą przełożyć się na problemy operacyjne i finansowe. Dlatego bezpieczeństwo nie może być dziś postrzegane przez pryzmat pojedynczych systemów czy działów organizacji.

W mojej ocenie kluczowe znaczenie ma zdolność organizacji do identyfikacji zagrożeń, zanim przekształcą się one w kryzys. To właśnie umiejętność przewidywania ryzyka staje się obecnie najcenniejszym zasobem. Nie chodzi wyłącznie o analizę historycznych zdarzeń, ale o monitorowanie trendów geopolitycznych, zmian regulacyjnych, zagrożeń cybernetycznych, problemów w łańcuchach dostaw czy potencjalnych zagrożeń dla infrastruktury krytycznej.

Nie oznacza to jednak, że można przewidzieć wszystko. Dlatego równie ważna jest gotowość do szybkiego reagowania. Organizacje odporne nie są tymi, które nigdy nie doświadczają incydentów. Są nimi te, które potrafią szybko wykryć problem, ograniczyć jego skutki oraz skutecznie wrócić do normalnego funkcjonowania.

W praktyce oznacza to konieczność budowania kultury bezpieczeństwa obejmującej całą organizację. Nawet najlepsze procedury pozostaną martwe, jeśli pracownicy nie będą rozumieli swojej roli w systemie bezpieczeństwa. Dlatego coraz większe znaczenie mają szkolenia, ćwiczenia kryzysowe, testy odporności oraz regularna weryfikacja planów ciągłości działania.

Istotne jest również odejście od tradycyjnego podziału na bezpieczeństwo fizyczne, techniczne i cyberbezpieczeństwo. W zakładach przemysłowych wszystkie te obszary są dziś ze sobą nierozerwalnie związane. Skuteczna ochrona wymaga ich integracji oraz wspólnego spojrzenia na ryzyko. Coraz częściej mówimy nie o security, cyber czy safety oddzielnie, ale o szeroko rozumianej odporności organizacyjnej.

Regulacje takie jak NIS2 czy CER dodatkowo wzmacniają ten trend. Pokazują one wyraźnie, że od przedsiębiorstw oczekuje się nie tylko ochrony zasobów, ale również zdolności do utrzymania kluczowych funkcji w sytuacjach kryzysowych. Odporność staje się więc nie tylko kwestią bezpieczeństwa, lecz także elementem przewagi konkurencyjnej i odpowiedzialności biznesowej.

Podsumowując, gdybym miał wskazać jeden najważniejszy czynnik budowania odporności współczesnego zakładu przemysłowego, nie byłaby to konkretna technologia ani pojedyncza procedura. Byłaby to zdolność organizacji do ciągłego rozumienia zmieniających się zagrożeń, podejmowania właściwych działań wyprzedzających oraz skutecznego reagowania wtedy, gdy mimo wszystko dojdzie do incydentu. To właśnie połączenie świadomości, przygotowania i elastyczności decyduje dziś o rzeczywistej odporności przedsiębiorstwa. Wnioski te są spójne z aktualnym podejściem QEMETICA do zarządzania ryzykiem i odpornością, opartym na analizie ryzyka, monitorowaniu zagrożeń, ciągłości działania oraz zintegrowanym podejściu do zagrożeń cybernetycznych, fizycznych i związanych z łańcuchem dostaw. •

> Technologia jest dziś niezbędnym narzędziem bezpieczeństwa, ale o odporności organizacji decydują ludzie, procesy oraz zdolność przewidywania i adaptacji do zagrożeń, których jeszcze nie znamy.





Skuteczna ochrona IK

ARTUR NOWAKOWSKI
Linc Polska



Coraz częściej widzimy, że bezpieczeństwo obiektów infrastruktury krytycznej (IK) oraz obiektów szczególnie ważnych dla obronności państwa jest testowane na różne sposoby. Jeszcze nie tak dawno w rozmowach z osobami odpowiedzialnymi za ochronę nikt nie przypuszczał, że zagrożenia, które kilka tygodni temu wydawały się mało prawdopodobne, staną się realne.

Przykładów jest wiele: ataki na infrastrukturę energetyczną w Niemczech oraz próby zakłócenia funkcjonowania kolei w Polsce, Holandii, Francji i we Włoszech. Wymienić należy też pożary i akty sabotażu wymierzone w obiekty przemysłu obronnego w Polsce, Estonii i Bułgarii oraz incydent z dronem wyposażonym w ładunek wybuchowy, znalezionym na lotnisku w Niemczech, w pobliżu ukraińskiego Antonowa.

To wszystko pokazuje, że wojna hybrydowa może dotyczyć każdego państwa i każdego obiektu. Plany ochrony obiektów IK wymagają dziś ponownej analizy i aktualizacji, adekwatnie do obecnego poziomu zagrożeń.

Od zawsze twierdzę, że jeżeli już coś robić, to robić to dobrze i nie akceptować „bylejakości". Szczególnie w przypadku tak istotnych obiektów skutecznym rozwiązaniem jest podejście warstwowe. I nie chodzi tylko o warstwy wykrywania, ale również o elementy oporu fizycznego, które z jednej strony dają możliwość wczesnego wykrycia intruza, z drugiej, będąc realną przeszkodą, wydłużają czas potrzebny na wtargnięcie na chroniony obiekt.

Najlepszym przykładem będzie tutaj ogrodzenie. Powszechnie stosowany, dostępny w przystępnej cenie płot panelowy? Trzy cięcia nożycami, dziesięć sekund i ogrodzenie zostaje sforsowane. Jeżeli ktoś liczy na to, że jest to skuteczna przeszkoda, być może warto zrewidować takie założenie.

Aby ogrodzenie rzeczywiście spełniało swoją funkcję, musi realnie opóźniać wtargnięcie intruza. Powinno być wytrzymałe i odpowiednio wysokie, a w zależności od wymaganego poziomu ochrony może być również zwieńczone drutem ostrzowym oraz uzupełnione napłotowym systemem wykrywania wtargnięć i wideoweryfikacją, które pozwalają wykryć próbę sforsowania, jeszcze zanim intruz dostanie się na teren obiektu. Informacja ta, przekazana bezzwłocznie ochronie, daje jej coś niezwykle cennego: czas na odpowiednią reakcję.

W przypadku dronów wyzwania wyglądają nieco inaczej. Realny atak z ich wykorzystaniem może być poprzedzony użyciem drona zwiadowczego. Wówczas system detekcyjny RF może dostarczyć informacji o tym, że nad obiektem znajduje się dron, a także wskazać pozycję jego operatora. Nie każdy dron musi jednak emitować sygnały radiowe. Dlatego kolejną warstwę powinien stanowić radar, pozwalający wykrywać i śledzić obiekty w przestrzeni powietrznej niezależnie od ich emisji.

Dziś mierzymy się z szeroko rozumianą dywersją: zarówno sabotażem, jak i cyberatakami. Aby móc skutecznie się bronić, musimy być odporni na te najbardziej szkodliwe zagrożenia. Podejście wielowarstwowe jest właściwą drogą do osiągnięcia tego celu. Nie wystarczy wiedzieć, że ktoś próbuje się dostać na teren obiektu. Trzeba mieć czas, aby sprawnie i skutecznie zareagować i przeciwdziałać zagrożeniu. •



Od pojedynczych systemów do ekosystemu

Jak zmienia się rynek security

W ciągu pięciu lat rynek security przeszedł wyraźną transformację – od pojedynczych urządzeń i systemów do zintegrowanych ekosystemów. Rozwój Ajax Systems dobrze pokazuje, jak zmieniły się technologie, oczekiwania profesjonalistów i sposób myślenia o bezpieczeństwie.

Jeszcze kilka lat temu rozmowa o profesjonalnym systemie bezpieczeństwa bardzo często zaczynała się od samych parametrów urządzeń. Zasięg komunikacji, czas pracy baterii, rozdzielczość kamer, liczba obsługiwanych stref czy sposób transmisji były naturalnymi punktami odniesienia przy porównywaniu rozwiązań.

Dzisiaj parametry nadal mają znaczenie, ale rzadziej wystarczają do oceny całego systemu. Instalator patrzy na czas montażu, konfigurację oraz późniejszy serwis, oczekuje elastyczności w skomplikowanych wdrożeniach. Agencja ochrony zwraca uwagę na sprawne zarządzanie dużą liczbą obiektów. Użytkownik szuka intuicyjnej aplikacji, estetyki i wygody. Inwestor analizuje natomiast nie tylko cenę sprzętu, ale także koszt wykonania instalacji i jej utrzymania. W efekcie rynek security przechodzi od myślenia o pojedynczych urządzeniach do spójnego ekosystemu bezpieczeństwa.

Pięć lat to w technologii bardzo dużo

Dobrym przykładem tej zmiany jest rozwój Ajax Systems. Kiedy w 2021 r. na łamach „a&s Polska" prezentowano Ajax polskim profesjonalistom, marka była opisywana przede wszystkim jako profesjonalny bezprzewodowy system alarmowy. Portfolio obejmowało 33 urządzenia – centrale, czujki ruchu, pożaru i zalania, syreny, klawiatury oraz elementy automatyki.

Fundamentami Ajax były technologia radiowa Jeweller, prostota instalacji, aplikacja mobilna oraz charakterystyczne wzornictwo wpisujące się w hasło *When security is art*.

Pięć lat później porównanie tamtego systemu z dzisiejszym portfolio pokazuje skalę rozwoju całej branży. Ajax nie jest już wyłącznie rozwiązaniem do ochrony domów i mieszkań. To w pełni profesjonalny system dedykowany dużym obiektom komercyjnym, przemysłowym i biznesowym. Dzisiejszy ekosystem obejmuje rozwiązania bezprzewodowe, przewodowe i hybrydowe, monitoring wizyjny, ochronę przeciwpożarową, automatykę oraz rozbudowane środowisko software'owe.

Bezprzewodowo czy przewodowo? Pytanie jest dziś inne

Przez lata dyskusja dotycząca systemów alarmowych sprowadzała się do wyboru między rozwiązaniem przewodowym a bezprzewodowym. Dziś właściwe pytanie brzmi: jaka technologia będzie najbardziej odpowiednia dla konkretnego obiektu, projektu i potrzeb klienta?

Komunikacja radiowa pozostaje fundamentem Ajax, przełamując dotychczasowe bariery branżowe. Przełomowym momentem było wprowadzenie pierwszego na świecie bezprzewodowego systemu bezpieczeństwa z certyfikacją Grade 3. Rozwiązanie to udowodniło, że technologia bezprzewodowa może spełniać najwyższe wymogi bezpieczeństwa dla obiektów o podwyższonym ryzyku (banki, salony jubilerskie, obiekty użyteczności publicznej), gwarantując krótki czas instalacji i elastyczność rozbudowy.

Jednocześnie rozwój technologii Fibra pozwolił Ajax wejść w świat instalacji przewodowych, a rozwiązania hybrydowe umożliwiają łączenie obu światów w ramach jednego systemu. To ogromna zaleta przy modernizacji istniejących obiektów, gdzie można wykorzystać ułożone wcześniej okablowanie i uzupełnić je o bezprzewodowe czujki bez kosztownego remontu. Dla profesjonalisty oznacza to pełną swobodę – to technologia zostaje dobrana do wymagań projektu, od małego lokalu po duży obiekt komercyjny.

Od produktów do jednolitego ekosystemu

Jeszcze większa zmiana dotyczy sposobu, w jaki patrzymy na bezpieczeństwo całego obiektu. Przez lata poszczególne technologie funkcjonowały jako niezależne wyspy: SSWiN, monitoring wizyjny, systemy ppoż. czy automatyka budynkowa były projektowane i instalowane w odrębnych środowiskach.

Dziś profesjonaliści i użytkownicy oczekują jednego, spójnego ekosystemu. Ochrona przed włamaniem pozostaje fundamentem Ajax, ale obok niej pojawiły się autorskie rozwiązania monitoringu wizyjnego, technologie przewodowe i hybrydowe, profesjonalna ochrona przeciwpożarowa oraz automatyka.

Wspólnym mianownikiem staje się software. Kluczową przewagą jest brak konieczności przełączania się między wieloma aplikacjami. Wszystkimi elementami zintegrowanego ekosystemu zarządza się z poziomu jednej aplikacji, co eliminuje chaos i podnosi wygodę użytkowania.

Ma to również wymiar biznesowy. Relacja instalatora z klientem nie kończy się wraz z uruchomieniem alarmu. Ten sam klient może potrzebować monitoringu wizyjnego, ochrony ppoż., automatyki czy późniejszej rozbudowy. Rozmowa przestaje dotyczyć pojedynczej centrali lub czujki – dotyczy całego środowiska bezpieczeństwa obiektu.

Hardware to dziś za mało

Jedną z największych zmian ostatnich lat jest rosnące znaczenie oprogramowania oraz wsparcia dla partnerów. Dla profesjonalisty liczy się cały cykl życia systemu: projekt, instalacja, konfiguracja, diagnostyka, monitoring, serwis, zarządzanie i późniejsza rozbudowa.

Rozwiązania takie jak Ajax PRO czy PRO Desktop pozwalają efektywnie zarządzać systemami klientów i wspierają codzienną pracę instalatorów oraz agencji ochrony. Hardware i software stanowią dziś jedną całość.

Ma to praktyczne znaczenie. Czas instalatora staje się jednym z najcenniejszych zasobów branży. Jeśli system można szybciej zainstalować i skonfigurować, a część czynności wykonywać zdalnie, technologia wpływa bezpośrednio na ekonomikę pracy – liczbę obsługiwanych klientów, koszty serwisu i rentowność projektów. Sama jakość urządzenia już nie wystarcza. Liczy się cały proces – od projektu, przez instalację, po późniejsze zarządzanie.

EN54 – bezprzewodowa rewolucja w profesjonalnym segmencie ppoż.

Szczególnie dobrym przykładem tego, jak zmienia się zakres ekosystemów bezpieczeństwa, jest ochrona przeciwpożarowa.

Dla Ajax wejście w obszar profesjonalnych systemów sygnalizacji pożarowej EN54 jest jednym z najważniejszych etapów rozwoju. Linia obejmuje centralę oraz adresowalne urządzenia przeznaczone do budowy profesjonalnego systemu ppoż. Na polskim rynku kluczowe znaczenie ma również uzyskanie dokumentów CNBOP-PIB.

Bezprzewodowy system EN54 stanowi ogromną wartość dla rynku. Dla instalatorów i inwestorów oznacza to rewolucję w czasie realizacji i oszczędności finansowe. Brak konieczności układania kilometrów trudnopalnych kabli oraz wiercenia drastycznie skraca czas montażu i pozwala na wdrażanie certyfikowanej ochrony ppoż. w obiektach zabytkowych, biurach czy hotelach – bez wyłączania ich z codziennego użytku.

Wejście w regulowany segment systemów sygnalizacji pożarowej pokazuje drogę, jaką przeszedł Ajax – od marki kojarzonej z systemem alarmowym do dostawcy technologii obejmującej kolejne obszary profesjonalnego bezpieczeństwa w ramach jednego ekosystemu.

Technologia, której nie trzeba ukrywać

Zmieniła się technologia, ale jeden z elementów filozofii Ajax pozostał niezmienny – design nadal jest częścią produktu. Systemy bezpieczeństwa montowane są w domach, biurach, hotelach czy obiektach komercyjnych, stanowiąc widoczny element przestrzeni.

Wzornictwo nie zastąpi parametrów technicznych ani certyfikatów, ale tworzy dobre doświadczenie użytkownika, podobnie jak intuicyjna aplikacja czy prostota obsługi. Dlatego hasło *When security is art* pozostaje aktualne także dzisiaj.

Technologia się zmienia. Relacje i edukacja pozostają najważniejsze

Nawet najlepszy ekosystem technologiczny nie zastąpi bezpośredniej współpracy z ludźmi, którzy projektują, instalują i obsługują systemy bezpieczeństwa.

Rozwojowi portfolio Ajax towarzyszy zwiększanie aktywności na polskim rynku, rozbudowa lokalnego zespołu oraz zacieśnianie relacji z instalatorami, integratorami, agencjami ochrony i projektantami.

Inwestujemy również w stały rozwój naszych partnerów. Służą temu dedykowane narzędzia: Partner Portal (dostęp do zasobów marketingowych i biznesowych wspierających rozwój firm) oraz platforma Ajax Academy (edukacja i podnoszenie kwalifikacji z zakresu norm i technologii). Elementem tego podejścia był tegoroczny Ajax Poland Roadshow w Warszawie, Krakowie, Poznaniu i Gdańsku, gdzie prezentowaliśmy w praktyce możliwości ekosystemu.

Pięć lat po pierwszej prezentacji Ajax na łamach „a&s Polska" wracamy do tej historii w zupełnie innym miejscu. W 2021 r. opowiadaliśmy o profesjonalnym bezprzewodowym systemie alarmowym. Dzisiaj mówimy o jednolitym ekosystemie bezpieczeństwa. I ta droga najlepiej pokazuje kierunek, w którym zmierza cała branża.

– *Naszym celem w Polsce jest teraz nie tylko zwiększanie obecności Ajax, ale przede wszystkim pokazanie profesjonalnemu rynkowi, jak szeroko zmieniły się możliwości tego ekosystemu. Chcemy być bliżej instalatorów, integratorów, agencji ochrony i projektantów oraz wspólnie z nimi rozwijać kolejne zastosowania Ajax* – podkreśla Jarosław Grzybowski, Country Manager Poland, Ajax Systems. •



Ajax Systems Poland Sp. z o.o.
ul. Grzybowska 12/14, lok. B5
00-132 Warszawa
https://ajax.systems/pl/



Mobilny dostęp bez wymiany infrastruktury

Nowe możliwości rozwiązań HID

Wykorzystanie istniejących kluczy Seos®, rozszerzona obsługa portfeli cyfrowych oraz mobilne zarządzanie czytnikami pozwalają organizacjom sprawniej przechodzić na mobilne poświadczenia dostępu.

Transformacja cyfrowa systemów kontroli dostępu nie musi oznaczać wymiany istniejącej infrastruktury. Nowe funkcje rozwiązań HID umożliwiają wykorzystanie już zainstalowanych czytników i kluczy Seos®, ograniczając zakres prac związanych z wdrożeniem mobilnych poświadczeń.

Mobilne poświadczenia z wykorzystaniem istniejących czytników

Jednym z istotnych wyzwań podczas wdrażania mobilnego dostępu jest dostosowanie infrastruktury znajdującej się już w obiekcie. Wymiana dużej liczby czytników oznacza dodatkowe koszty, prace instalacyjne oraz konieczność koordynowania dostępu do chronionych obszarów.

Aplikacja **HID Mobile Access** została rozszerzona o funkcję pozwalającą czytnikom HID przygotowanym do obsługi dostępu mobilnego korzystać z istniejących kluczy **Seos®**. Dotyczy to m.in. czytników **HID Signo™** oraz **iCLASS® SE™**.

W praktyce oznacza to możliwość przejścia na mobilne poświadczenia bez wymiany czytników i bez ich ponownej konfiguracji. Nie jest również wymagana aktualizacja firmware'u ani dodatkowa wizyta ekipy serwisowej w obiekcie. Organizacja może więc wykorzystać istniejącą infrastrukturę, jednocześnie rozszerzając sposób, w jaki użytkownicy uzyskują dostęp. Takie podejście pozwala skrócić proces wdrożenia oraz ograniczyć jego koszty, przy zachowaniu mechanizmów bezpieczeństwa stosowanych przez HID.

Dostęp w cyfrowym portfelu

Rozszerzeniu ulega również obsługa cyfrowych portfeli. Liczba wdrożeń kart dostępu w Apple oraz Google Wallet rośnie, więc kolejnym naturalnym krokiem jest dodanie funkcjonalności Samsung Wallet – zwiększając liczbę dostępnych sposobów przechowywania mobilnych poświadczeń HID Mobile Access.

Wykorzystanie portfeli cyfrowych, z których użytkownicy korzystają już na co dzień, upraszcza korzystanie z mobilnego dostępu. Poświadczenie może być przechowywane w urządzeniu mobilnym wraz z innymi cyfrowymi elementami wykorzystywanymi przez użytkownika, co ułatwia jego wdrożenie w organizacji.

Zarządzanie czytnikiem z urządzenia mobilnego

Kolejnym elementem rozwiązania jest **HID Linq™ Mobile**, które rozszerza możliwości zarządzania kompatybilnymi czytnikami bezpośrednio z urządzenia mobilnego.

Administrator może w terenie konfigurować i aktualizować czytniki oraz przygotowywać je do obsługi mobilnych poświadczeń. W ramach tego procesu możliwe jest m.in. przeprowadzanie aktualizacji firmware'u, konfiguracja czytnika oraz włączanie obsługi mobilnego dostępu.

Komunikacja z czytnikiem wykorzystuje **Bluetooth® Low Energy (BLE)** oraz **NFC**. Ogranicza to konieczność fizycznego podłączania urządzeń lub dodatkowego wyposażenia, tym samym zmniejsza nakład pracy potrzebny do przygotowania infrastruktury.

Etapowe przejście na mobilny dostęp

Rozwiązania HID pozwalają połączyć istniejącą infrastrukturę kontroli dostępu z rozwiązaniami mobilnymi. Organizacja nie musi więc podejmować decyzji o całkowitym przejściu z kart na poświadczenia mobilne w jednym etapie.

Możliwe jest stopniowe wdrażanie mobilnego dostępu, z wykorzystaniem dotychczasowych inwestycji w czytniki i system kontroli dostępu. Pozwala to dopasować tempo transformacji do potrzeb operacyjnych organizacji, a jednocześnie przygotować infrastrukturę na dalszy rozwój.

Połączenie obsługi istniejących kluczy Seos®, cyfrowych portfeli oraz mobilnego zarządzania czytnikami tworzy rozwiązanie, które ułatwia techniczną stronę migracji do mobilnych poświadczeń. Dla organizacji oznacza to możliwość rozwijania funkcjonalności kontroli dostępu bez konieczności rozpoczynania modernizacji infrastruktury od podstaw. •

HID jest globalnym dostawcą rozwiązań do kontroli dostępu, identyfikacji i zarządzania tożsamością. Oferuje m.in. systemy kontroli dostępu, karty i identyfikatory mobilne, rozwiązania biometryczne oraz technologie RFID do identyfikacji i śledzenia zasobów. Z produktów HID korzystają przedsiębiorstwa, banki, szpitale, uczelnie i instytucje publiczne. Firma ma siedzibę w Austin w Teksasie, zatrudnia ponad 4500 pracowników i działa w ponad 100 krajach. HID należy do grupy ASSA ABLOY. Więcej informacji: www.hidglobal.com

HID Global (Polski oddział)
ul. Krakowska 280
32-080 Zabierzów
Eximius Park 200

Zaprojektowany, by robić wrażenie

Czytnik Signo do montażu podtynkowego – rozwiązanie, na które czekaliście.

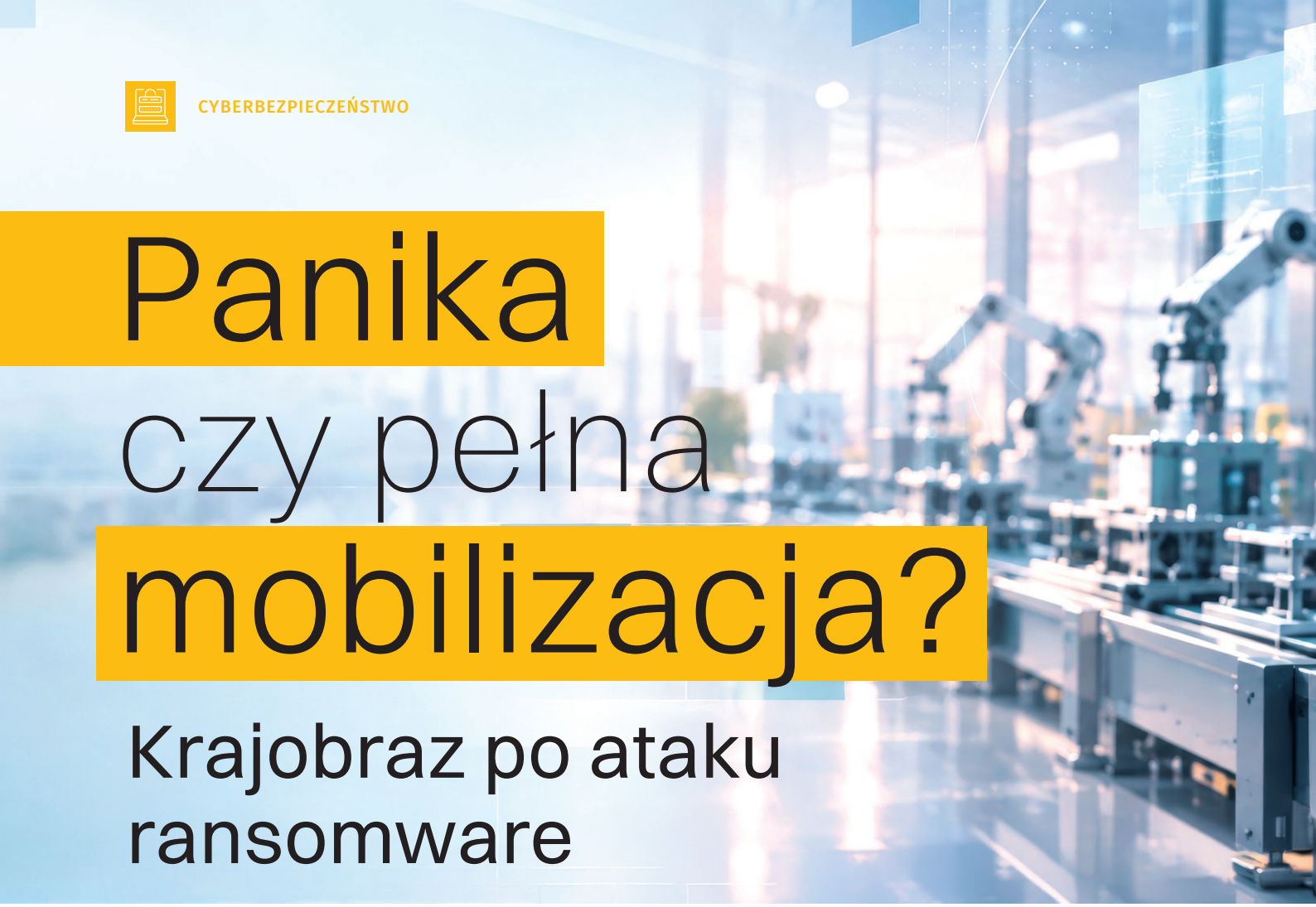


Każdy widoczny element budynku jest efektem świadomej decyzji projektowej. Nie inaczej jest w przypadku czytników systemów kontroli dostępu. HID Signo Décor stanowi odpowiedź na oczekiwania projektantów i architektów: to czytnik Signo przystosowany do montażu podtynkowego, dzięki czemu idealnie wtapia się w architekturę obiektu.
Jednocześnie oferuje wszystko to, czego można oczekiwać od serii Signo: ten sam poziom bezpieczeństwa, obsługę mobilnych poświadczeń oraz funkcje zdalnego zarządzania.

Dostępny w kolorze białym lub czarnym, pasującym do każdego otoczenia.

HID

Przyjrzyj się bliżej »
campaigns.hidglobal.com/signo



Panika czy pełna mobilizacja?

Krajobraz po ataku ransomware

Atak ransomware nie musi zaszyfrować wszystkich systemów ani dotrzeć do sterowników, aby zatrzymać fabrykę. Wystarczy, że odbierze firmie pewność, czy zlecenia, receptury, parametry procesu, wyniki kontroli jakości i dane telemetryczne są prawidłowe. Kontynuowanie produkcji bez tej pewności grozi wytworzeniem wadliwego produktu, uszkodzeniem instalacji, a nawet zagrożeniem dla ludzi. Wyłączenie maszyn jest wtedy działaniem ochronnym, nie kapitulacją.

Monika Żuber-Mamakis

2 września 2025 r. Jaguar Land Rover poinformował, że po cyberincydencie prewencyjnie wyłączył globalne systemy, co poważnie zakłóciło sprzedaż i produkcję. Produkcja była wznawiana etapami od 8 października, a do normalnego poziomu wróciła w połowie listopada. JLR wykazał 196 mln funtów kosztów związanych z incydentem. Przychody spadły o 24 proc. rok do roku; oprócz postoju wpłynęły na to wygaszanie starszych modeli Jaguara oraz cła w USA.

JLR nie potwierdził, że był to atak ransomware, choć nie przeczył, że był to atak cyfrowy. Przypominamy o tym zdarzeniu, ponieważ pokazuje, że do zatrzymania produkcji nie trzeba naruszyć systemów sterowania. Wystarczy odebrać firmie zaufanie do danych łączących zamówienia, surowce, maszyny, kontrolę jakości i logistykę.

System naczyń połączonych

Według raportu Threat Landscape 2025 Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) przemysł odpowiadał za niespełna 3 proc. z 4875 analizowanych incydentów od lipca 2024 do czerwca 2025 r. Wynik zaniża przewaga licznych, zwykle mniej dotkliwych ataków na administrację. W samym przemyśle cyberprzestępczość stanowiła jednak 59,3 proc. odnotowanej aktywności. Na producentów przypadło też 14,9 proc. zgłoszonych ataków ransomware w Unii Europejskiej – najwięcej ze wszystkich sektorów.

Raport nie obejmuje informacji o wszystkich atakach, jakie miały miejsce w Europie. ENISA opiera się na źródłach publicznych i dobrowolnych zgłoszeniach. Pokazuje jednak wyraźną prawidłowość: im więcej kosztuje każda godzina postoju, tym większą presję mogą wywrzeć przestępcy.

Badanie Sophos z 2025 r. objęło 332 zaatakowane organizacje produkcyjne. Dane zaszyfrowano w 40 proc. przypadków, a w kolejnych 10 proc. poprzestano na kradzieży informacji i wymuszeniu. Średnie żądanie wyniosło 1,2 mln USD, płatność 1 mln USD, a koszt odtworzenia działalności – bez okupu – 1,3 mln USD. Wyników z 17 państw nie należy jednak traktować jako kosztu typowej polskiej fabryki.



Ilustracje: A&S AI Studio

Czasami trzeba powiedzieć „stop”

W firmach produkcyjnych nie ma uniwersalnego przycisku „stop”, który wyłączałby wszystkie systemy i zamrażał procesy. Każde wyłączenie produkcji wymaga odpowiedzi na szereg ważnych pytań. Pierwsze z nich brzmi nie: „czy serwer plików jest zaszyfrowany?”, lecz: „czy proces fizyczny pozostaje obserwowalny, sterowalny i bezpieczny?”. W przewodniku po bezpieczeństwie technologii operacyjnej (OT, *Operational Technology*) Narodowy Instytut Standaryzacji i Technologii (NIST, *National Institute of Standards and Technology*) wskazuje, że reakcja może oznaczać monitorowanie albo pełne wyłączenie systemu i procesu. Automatyczne odłączenie wszystkiego bywa równie ryzykowne jak bezrefleksyjna kontynuacja produkcji.

Produkcję trzeba zatrzymać, gdy zakład traci wiarygodny obraz procesu, wskazania cyfrowe nie zgadzają się z niezależnymi pomiarami, pojawiają się nieautoryzowane zmiany konfiguracji lub anomalne polecenia albo naruszono bezpieczeństwo stacji inżynierskiej bądź systemu bezpieczeństwa funkcjonalnego (SIS, *Safety Instrumented System*). Powodem może być także brak pewności co do receptury, surowca lub parametrów jakościowych: sprawna maszyna nadal może wtedy wytwarzać wadliwy produkt.

Najpierw proces należy doprowadzić do stanu bezpiecznego, a dopiero potem izolować strefy, blokować komunikację i zdalny dostęp, chronić kopie zapasowe oraz zabezpieczać ślady. Kolejność ustalają wspólnie specjaliści OT i cyberbezpieczeństwa. W instalacji ciągłej pochopne odłączenie sieci może zniszczyć partię, uszkodzić urządzenia lub pozbawić operatora informacji o ciśnieniu i temperaturze. Doskonale widać to w hutnictwie. Wielki piec pracuje nieprzerwanie, a jego wyłączenie jest skomplikowane i kosztowne.

W raporcie o stanie bezpieczeństwa teleinformatycznego Niemiec z 2014 r. cyberatak na hutę został opisany przez Federalny Urząd Bezpieczeństwa Teleinformatycznego (BSI, *Bundesamt für Sicherheit in der Informationstechnik*), odpowiedzialny w Niemczech za cyberbezpieczeństwo. Napastnicy przedostali się z sieci biurowej do produkcyjnej i zakłócili sterowanie. Pieca nie udało się wyłączyć w sposób kontrolowany, co doprowadziło do poważnych uszkodzeń. Nie był to atak ransomware, ale przykład pokazuje, dlaczego takiej decyzji nie może podejmować sam dział informatyczny.

Podczas ataku ransomware na BlueScope Steel w 2020 r. część systemów wyłączono, lecz wielki piec w hucie Port Kembla przełączono na obsługę ręczną. Produkcja stali trwała, choć walcownia taśm gorących czasowo stanęła. W OT odłączenie sieci może więc być początkiem poważnych problemów, a nie ich końcem.

W kajeciku i na karteczkach, czyli tryb ręczny

„Tryb ręczny” często pojawia się w planach ciągłości działania bez wyjaśnienia. Tymczasem może oznaczać lokalne sterowanie procesem - za pomocą fizycznych przełączników, ręcznych zaworów, niezależnych wskaźników i obchodów operatorskich – albo ręczną obsługę biznesu: papierowe zlecenia, telefoniczne potwierdzanie dostaw, etykiety i faktury. Jedno nie zastępuje drugiego. Linia może być sprawna, ale stać, bo magazyn nie wie, co wydać; system planowania zasobów przedsiębiorstwa (ERP, *Enterprise Resource Planning*) może działać, choć operator stracił wiarygodny obraz procesu.

NIST zaleca niecyfrowe mechanizmy obserwacji i kontroli. Analogowy manometr może dostarczyć wiarygodnych danych, gdy interfejs człowiek-maszyna (HMI, *Human-Machine Interface*) nie działa, a ręczny zawór pozwoli opanować urządzenie. Taka praca jest jednak wolniejsza i wymaga większej obsady. Trzeba ją regularnie ćwiczyć – także z uczestnikami łańcucha dostaw – zamiast liczyć na improwizację podczas incydentu.

Po ataku z 19 marca 2019 r. Norsk Hydro utrzymał większość produkcji dzięki pracochłonnym procedurom ręcznym. Komputery i serwery sprawdzano, czyszczono i bezpiecznie przywracano, a dane odzyskiwano z kopii. Norsk Hydro oszacowało później łączny koszt na około 800 mln koron norweskich. Tryb ręczny umożliwił pracę, ale nie był rozwiązaniem bezkosztowym.

Praca ręczna może też dotyczyć procesów biznesowych. Po cyberataku w sierpniu 2023 r. amerykański producent środków czystości Clorox uruchomił ręczną obsługę zamówień. Jak podał w raporcie przekazanym amerykańskiej Komisji Papierów Wartościowych i Giełd (SEC), pozwoliło to obsługiwać klientów z mniejszą wydajnością. Przychody kwartalne spadły z 1,740 do 1,386 mld USD, a dodatkowe koszty związane z reakcją na incydent wyniosły 24 mln USD.

Informatycy, automatycy, specjaliści bezpieczeństwa i zarząd – każdy ciągnie w swoją stronę

Cyberatak łatwo zamienia współpracę w chocholi taniec: informatycy chcą odłączyć systemy, automatycy utrzymać proces, specjaliści cyberbezpieczeństwa zabezpieczyć dowody, operacje pytają o wysyłki, a finanse liczą straty. Każdy widzi tylko część sytuacji, dlatego podział ról trzeba ustalić przed incydentem.

Według NIST plan reakcji powinien obejmować koordynatora incydentu, kierownictwo operacyjne, specjalistów bezpieczeństwa procesowego, zespoły automatyki i informatyczne, ochronę

SIEDEM PYTAŃ, ZANIM UCICHNIE HALA

Samo zadanie pytań nie wystarczy. Odpowiedzi powinny być zapisane, uzgodnione i przećwiczone, zanim na ekranach pojawi się żądanie okupu. Poniższy schemat nie zastępuje zakładowej procedury, ale pokazuje, co powinna ona rozstrzygać.

1. Kto może zarządzić bezpieczne zatrzymanie procesu i kto go zastępuje poza pierwszą zmianą?

Decyzja nie może krążyć między dyrektorem zakładu, szefem informatyki i kierownikiem produkcji. Procedura powinna wskazywać stanowisko decyzyjne i zastępcę dostępnego nocą, w weekend i podczas urlopu. Zespół cyberbezpieczeństwa ocenia zagrożenie i zaleca izolację, lecz sposób zatrzymania procesu ustalają osoby odpowiedzialne za produkcję i bezpieczeństwo procesowe. Inaczej wyłącza się serwer, inaczej piec, mieszalnik czy linię lakierniczą.

2. Jak odizolować systemy informatyczne, OT oraz zdalne dostępy bez utraty widoczności i sterowalności procesu?

Odcięcie wszystkiego może pozbawić operatorów telemetrii, alarmów lub możliwości kontrolowanego zatrzymania instalacji. Zakład powinien wcześniej ustalić kolejność izolowania: kont i połączeń zdalnych, styku systemów informatycznych z OT, zainfekowanych segmentów i urządzeń. Potrzebne są aktualne schematy sieci, opisane punkty odcięcia i przećwiczone scenariusze. Izolować agresywnie, zatrzymywać rozważnie.

3. Które linie i operacje mogą działać wyłącznie lokalnie lub być obsługiwane ręcznie, przy jakiej obsadzie i przez jaki czas?

Tryb ręczny nie cofa fabryki do bezpieczniejszych czasów. Plan powinien określać, które procesy można prowadzić bez HMI, systemu realizacji produkcji (MES, ***Manufacturing Execution System)*** lub łączności z siecią, ilu ludzi potrzeba, jak długo mogą tak pracować oraz jak wykonywać pomiary i pilnować granic bezpieczeństwa oraz jakości. Jeśli ostatni operator znający ręczne sterowanie odszedł na emeryturę, zakład ma legendę o trybie awaryjnym, nie procedurę.

4. Czy plany, numery telefonów i instrukcje są dostępne offline?

Plan reakcji przechowywany wyłącznie na zaszyfrowanym serwerze niewiele pomoże. W bezpiecznej postaci offline powinny być dostępne: lista osób decyzyjnych, numery telefonów, kontakty do dostawców, schematy sieci, inwentaryzacja najważniejszych urządzeń oraz instrukcje izolowania i zatrzymywania instalacji. Warto przygotować również alternatywny kanał komunikacji na wypadek niedostępności poczty i komunikatorów firmowych. Dokumentacja papierowa nadal ma swoje zalety. O ile jest aktualna i nie zawiera haseł zapisanych na okładce.

5. Czy kopie zapasowe obejmują także przemysłową pamięć zakładu?

Kopia serwerów biurowych to za mało. Trzeba zachować logikę PLC, konfiguracje HMI i systemów nadzoru oraz akwizycji danych (SCADA, ***Supervisory Control and Data Acquisition)***, receptury, parametry napędów, obrazy stacji inżynierskich, reguły zapór, konfiguracje przełączników, licencje i zgodne wersje oprogramowania układowego. Co najmniej jedna kopia powinna być odseparowana od środowiska produkcyjnego i odporna na modyfikację. Najważniejszy jest jednak test odtworzenia: kopia, której nikt nie próbował przywrócić, pozostaje obietnicą.

6. Kto daje zgodę na ponowne uruchomienie produkcji?

Restart powinien być wspólną decyzją, a nie triumfalnym kliknięciem administratora, który właśnie odtworzył serwer. Zespół bezpieczeństwa musi potwierdzić usunięcie mechanizmów przetrwania napastnika i zabezpieczenie kont; OT — poprawność konfiguracji i sterowania; służby techniczne – bezpieczeństwo instalacji; dział jakości – zgodność pierwszych partii produktu z wymogami jakościowymi. Produkcję najlepiej wznawiać etapami: od wydzielonego środowiska lub jednej linii, przy zwiększonym monitorowaniu. Zielone światło musi mieć kilka odcieni.

7. Ile naprawdę kosztuje godzina postoju każdej linii?

Nie wystarczy podzielić rocznych przychodów przez liczbę godzin pracy. Trzeba uwzględnić utraconą marżę, surowce i produkcję w toku przeznaczone do utylizacji, koszt czyszczenia oraz rozruchu instalacji, bezczynność pracowników, nadgodziny, transport ekspresowy, kary umowne i skutki dla dostawców. A nawet utratę reputacji. Kalkulację należy przygotować osobno dla najważniejszych linii, ponieważ godzina postoju wąskiego gardła może kosztować wielokrotnie więcej niż zatrzymanie pozostałej części zakładu. Taka wiedza pozwala ustalić kolejność odtwarzania – i przekłada cyberbezpieczeństwo na język zrozumiały dla zarządu.

Zgodnie z zaleceniami NIST dotyczącymi bezpieczeństwa OT procedury reagowania muszą uwzględniać szczególne wymagania środowiska przemysłowego: bezpieczeństwo ludzi i procesu, niezawodność oraz dostępność instalacji. Dlatego odpowiedzi będą inne w hucie, inne w mleczarni, a jeszcze inne na linii montażu elektroniki. Powinny jednak istnieć przed incydentem.

Jeżeli odpowiedź na którekolwiek z tych pytań zaczyna się od słów „ustalimy w razie potrzeby”, fabryka nie ma jeszcze planu. Ma nadzieję.

fizyczną, prawników, finanse oraz dostawców. Koordynator organizuje wymianę informacji, lecz nie zastępuje ekspertów: produkcja ocenia stan procesu, cyberbezpieczeństwo – czystość środowiska, bezpieczeństwo procesowe – ryzyko, a jakość dopuszcza produkt.

Zgodę na wznowienie produkcji przygotowuje kilka osób. Dyrektor ds. bezpieczeństwa informacji (CISO, *Chief Information Security Officer*) potwierdza powstrzymanie ataku; kierownik automatyki – poprawność konfiguracji sterowników i urządzeń; dyrektor produkcji – gotowość procesu i personelu; specjalista bezpieczeństwa procesowego – sprawność zabezpieczeń; kierownik jakości – poprawność receptur i identyfikowalność partii.

Po uzyskaniu tych potwierdzeń dyrektor zakładu lub osoba wskazana w planie formalnie zezwala na uruchomienie określonej instalacji. Decyzja powinna wskazywać zakres i tryb wznowienia pracy oraz warunki ponownego zatrzymania procesu. Koordynator incydentu pilnuje procedury, ale sam nie wydaje zgody.

Plan musi wskazywać osoby odpowiedzialne i ich zastępców oraz pozostawać dostępny mimo awarii sieci – na papierze lub w systemie odseparowanym od zaatakowanego środowiska. Taką formę zaleca NIST w przewodniku dotyczącym bezpieczeństwa technologii operacyjnej.

Zapłata okupu i wznowienie produkcji to odrębne decyzje. Po ataku ransomware w 2021 r. JBS USA, amerykańska część koncernu mięsnego, zapłacił 11 mln USD, choć większość zakładów już działała. JBS tłumaczył tę decyzję potrzebą ograniczenia możliwych następstw ataku i ryzyka wycieku danych. Przelew jest decyzją prawną i biznesową; nie dowodzi, że systemy są czyste, ani nie uzasadnia uruchomienia linii.

Polityka małych kroków

Przywrócony serwer nie oznacza wznowienia produkcji. Trzeba potwierdzić odcięcie napastnika, odbudować środowisko z wiarygodnych źródeł oraz porównać logikę programowalnych sterowników logicznych (PLC, *Programmable Logic Controller*), konfiguracje HMI, receptury, reguły zapór i parametry urządzeń ze stanem zatwierdzonym. Kopie powinny obejmować również obrazy systemów, programy, konfiguracje, nośniki instalacyjne i klucze licencyjne. Kopia nietestowana pozostaje nadzieją.

Po odtworzeniu systemów następuje walidacja fizyczna. Nie można mechanicznie przywrócić wcześniejszych ustawień: zawór otwarty przed incydentem po postoju może zagrozić chłodzeniu lub ciśnieniu. Uruchamianie powinno zacząć się od instalacji pomocniczych, a następnie objąć próbę z ograniczoną prędkością, partię testową oraz kontrolę bezpieczeństwa i jakości. Do powrotu do pełnej produkcji potrzebny jest wzmożony monitoring.

Tak wracał JLR: najpierw uruchomił wybrane systemy sprzedaży, logistyki, części i płatności, potem zakład napędów, montaż baterii, tłocznię, lakiernię i kolejne linie. Wprowadził też ręczne płatności i program finansowania dostawców o wartości 500 mln funtów. Wznowienie produkcji obejmuje również płynność firm po drugiej stronie bramy.

Ile kosztuje cisza?

Cisza w hali oznacza wymierne straty, ale nie istnieje wiarygodna „średnia cena dnia postoju fabryki". Huta, mleczarnia, lakiernia i montownia elektroniki różnią się marżą, zapasami, kosztami wygaszenia oraz tolerancją na przestój. Dlatego własny koszt



godziny i dnia trzeba policzyć dla konkretnego procesu, a dane rynkowe traktować jedynie jako punkt odniesienia.

Rachunek powinien obejmować utraconą marżę, odpad i produkcję w toku, płace za czas bezczynności, nadgodziny, transport ekspresowy, kary umowne, informatykę śledczą, odbudowę systemów, komunikację kryzysową, roszczenia i straty dostawców. Koszty reakcji, utraconą sprzedaż i skutki makroekonomiczne należy liczyć osobno – opisują różne zjawiska.

Okup bywa najbardziej widocznym składnikiem rachunku, ale nie zawsze największym.

Przykłady pokazują różne miary strat. Norsk Hydro oszacował łączny koszt na 800 mln koron norweskich, a Clorox wykazał 24 mln USD dodatkowych kosztów przy kwartalnej sprzedaży niższej o 354 mln USD rok do roku. JLR podał 196 mln funtów kosztów bezpośrednio związanych z cyberatakiem. Jego przychody spadły o 24%, a wolne przepływy pieniężne były ujemne i wyniosły 791 mln funtów – firma wydała więc o tyle więcej gotówki, niż wygenerowała. Cyberatak nie był jedyną przyczyną: JLR wskazywał również na cła w USA i wygaszanie starszych modeli Jaguara.

Skalę ryzyka ilustruje symulacja Kaspersky i VDC Research. Gdyby wykryte w przemyśle próby ransomware się powiodły, koszt wynagrodzeń bezczynnych pracowników mógłby w pierwszych trzech kwartałach 2025 r. przekroczyć 18 mld USD na świecie, w tym 4,4 mld USD w Europie. Nie są to rzeczywiste straty: wszystkie uwzględnione próby zablokowano. Model oparto m.in. na liczbie firm, zatrudnieniu, płacach i średnim, 13-dniowym zakłóceniu po rzeczywistym ataku.

KSC wchodzi na produkcję

Nie wiadomo, ile ataków ransomware zatrzymało produkcję w Polsce. CERT Polska otrzymał jednak w 2025 r. 658 320 zgłoszeń, na podstawie których zarejestrował 260 783 unikalne incydenty – o 152% więcej niż rok wcześniej. Złośliwe oprogramowanie odpowiadało za blisko 3500 incydentów, a ransomware za 179. Są to dane dla całego kraju, nie tylko przemysłu, dlatego nie należy ich porównywać wprost z sektorowymi statystykami ENISA.

Od 3 kwietnia 2026 r. obowiązuje nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC), wdrażająca dyrektywę w sprawie bezpieczeństwa sieci i systemów informatycznych (NIS2, *Network and Information Systems Directive 2*). Do sektorów ważnych zaliczono m.in. produkcję elektroniki, urządzeń elektrycznych, maszyn, pojazdów, innego sprzętu transportowego i wybranych wyrobów medycznych. Nie obejmuje to każdej fabryki: decydują rodzaj działalności, wielkość przedsiębiorstwa i reguły kwalifikacji.

W podmiocie kluczowym lub ważnym cyberbezpieczeństwo nie jest wyłącznie zadaniem działu informatycznego. Ustawa o krajowym systemie cyberbezpieczeństwa przypisuje odpowiedzialność kierownikowi podmiotu – w spółce kapitałowej co do zasady zarządowi. Jeżeli zarząd jest wieloosobowy i nie wskazano odpowiedzialnego członka, odpowiadają wszyscy. Powierzenie zadań pracownikowi lub firmie zewnętrznej nie zwalnia ich z tej odpowiedzialności.

Kierownik decyduje o przygotowaniu, wdrożeniu i nadzorowaniu systemu zarządzania bezpieczeństwem informacji (SZBI), planuje środki finansowe, rozdziela zadania i kontroluje ich wykonanie. On oraz osoba, której powierzył część obowiązków, muszą raz w roku odbyć udokumentowane szkolenie.

UDZIAŁ ODNOTOWANYCH INCYDENTÓW WEDŁUG SEKTORÓW

SEKTOR	UDZIAŁ INCYDENTÓW
Administracja publiczna	38,2%
Sektor nieokreślony	28,5%
Transport	7,5%
Infrastruktura i usługi cyfrowe	4,8%
Finanse	4,5%
Przemysł	2,9%
Media i rozrywka	2,3%
Usługi biznesowe	2,2%
Energetyka	1,7%
Edukacja	1,7%
Ochrona zdrowia	1,2%

Źródło: zbiór danych ENISA.

Po wykryciu incydentu poważnego podmiot wysyła do właściwego sektorowego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT, *Computer Security Incident Response Team*) wczesne ostrzeżenie – najpóźniej w ciągu 24 godzin – oraz pełne zgłoszenie w ciągu 72 godzin. Sprawozdanie końcowe należy przekazać zasadniczo w ciągu miesiąca; CSIRT może wcześniej zażądać raportu okresowego.

Terminy te nie rozstrzygają, kiedy uruchomić linię, lecz wpływają na przygotowanie zakładu. W pierwszych godzinach trzeba chronić ludzi i proces, izolować zagrożone systemy, zabezpieczać dowody, oceniać wpływ incydentu i gromadzić dane do zgłoszenia. Bez ćwiczeń i współpracy informatyków, automatyków, prawników oraz zarządu 24 godziny mogą upłynąć, zanim firma ustali, co się wydarzyło.

Odporność nie oznacza gwarancji nieprzerwanej produkcji, lecz przygotowanie na jej zatrzymanie. Plan powinien określać, kto podejmuje taką decyzję, które procesy można prowadzić ręcznie, jak długo łańcuch dostaw zniesie zakłócenia, z jakich kopii odtworzyć systemy oraz jakie warunki spełnić przed wznowieniem pracy. Ustalenia te trzeba sprawdzić podczas ćwiczeń obejmujących również nocną zmianę, logistykę, utrzymanie ruchu, dostawcę automatyki i finanse.

Ransomware jest oprogramowaniem, lecz paraliż zakładu wynika z połączenia problemów technicznych i organizacyjnych. Przestępcy wykorzystują podatności systemów, zależność procesów od danych, niejasny podział odpowiedzialności i presję czasu. Nie wystarczy więc kolejny produkt bezpieczeństwa. Potrzebna jest zdolność do kontrolowanego ograniczenia produkcji, bezpiecznego zatrzymania instalacji i wznowienia pracy dopiero po potwierdzeniu bezpieczeństwa systemów. •

ALNET SYSTEMS

Polskie profesjonalne zintegrowane rozwiązania VMS
Ponad 200 000 instalacji na całym świecie
Jesteśmy z Wami od 2003 roku



www.alnetsystems.com



Jesienny Security BootCamp
dwa dni praktyki i wymiany doświadczeń

Realne scenariusze, praktyczne zadania, aktualne zagrożenia i technologie wspierające bezpieczeństwo – tak wyglądała **jesienna edycja Security BootCampu,** która odbyła się 1-2 października w Folwarku Wąsowo. Dwudniowe szkolenie zgromadziło osoby odpowiedzialne za bezpieczeństwo organizacji: security i risk managerów, specjalistów ds. ochrony, facility management oraz compliance.

Jedenasta już edycja BootCampu miała praktyczny i angażujący charakter, a wspaniała, jesienna pogoda sprzyjała zarówno zdobywaniu wiedzy, jak i integracji. Uczestnicy odwiedzali stanowiska przygotowane przez poszczególnych partnerów: Hanwha Vision, Ifter, Inner Range, Securitas i STID. Na każdym stoisku czekało inne zadanie – wymagające nie tylko poznania prezentowanych rozwiązań, ale przede wszystkim analizy sytuacji, podjęcia decyzji i znalezienia odpowiedzi na konkretny problem związany z bezpieczeństwem.

Taka formuła pozwoliła uczestnikom nie tylko poznać nowe technologie, ale także sprawdzać je w działaniu i konfrontować wiedzę z praktyką.



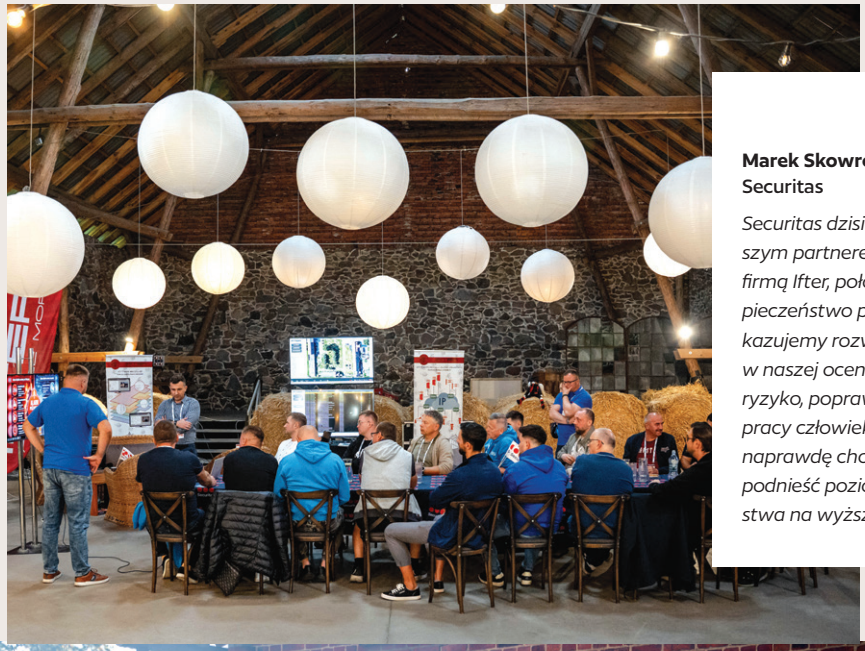
Mariusz Kucharski
a&s Polska

Jesteśmy w dziewiętnastowiecznym folwarku Wąsowo, w sercu Wielkopolski, w przepięknym ceglanym kompleksie. To tutaj właśnie odbywały się konkurencje techniczne dla szefów bezpieczeństwa z firm, instytucji i organizacji z całego kraju. Bezpiecznicy rywalizowali o miano najlepszej ekipy pod względem technicznym i pod względem wiedzy na temat bezpieczeństwa oraz zabezpieczeń.



Od alarmu do decyzji

Na stanowisku przygotowanym przez **Securitas i IFTER** skoncentrowano się na optymalizacji procesów związanych z bezpieczeństwem pożarowym. Na przykładzie Ifter EQU Fire System Integrator uczestnicy mierzyli się z zadaniami dotyczącymi obsługi zdarzeń – od pojawienia się alarmu, przez jego weryfikację, po podjęcie odpowiednich działań operacyjnych.





Marek Skowronek
Securitas

Securitas dzisiaj, razem z naszym partnerem biznesowym firmą Ifter, położył na stół bezpieczeństwo pożarowe. Pokazujemy rozwiązanie, które w naszej ocenie optymalizuje ryzyko, poprawia efektywność pracy człowieka, bo o to tak naprawdę chodzi, i pozwala podnieść poziom bezpieczeństwa na wyższy level.



Wojciech Barański
Port Polska

Spotkać się, dotknąć i spróbować zepsuć wszelkiego rodzaju produkty, których będziemy używać. Spróbować, jak to działa, zobaczyć, jak to działa i czy działa.





Grzegorz Krawętowski
Ifter

Z mojego punktu widzenia uważam, że to najlepszy sposób na pokazanie tego, jak praktycznie działa nasz system. Klient może go po prostu dotknąć, sprawdzić, zobaczyć, a także usłyszeć. Uważam, że to coś świetnego. Na pewno nie jestem tutaj ostatni raz.







Piotr Andrzejczak
3M

BootCamp to dla mnie przede wszystkim okazja do spotkań z różnymi firmami i ludźmi, a także do wymiany doświadczeń.

VMS jak pilot do telewizora?

Hanwha Vision postawiła uczestników przed wyzwaniem związanym z projektowaniem i obsługą systemów VMS. Punktem wyjścia była prosta analogia: dobry system powinien być tak intuicyjny jak pilot do telewizora. Zadanie pozwalało spojrzeć na VMS z perspektywy zarówno użytkownika, jak i instalatora, zwracając uwagę na funkcjonalność, wygodę obsługi, skalowalność i niezawodność.





Łukasz Lik
Hanwha Vision

Pomyślałem, że tym razem zainspirujemy się popularnym serialem z platformy streamingowej i zorganizujemy grę w klimacie szlacheckim. Przygotowaliśmy więc grę terenową z zagadkami w tym klimacie. Uczestnicy sami musieli testować system bezpieczeństwa. Analiza obrazu detekowała zdarzenia, system na nie reagował i prowadził użytkowników przez kolejne etapy. Chcieliśmy w ten sposób pokazać, jak nasze systemy wspierają podejmowanie decyzji, poszerzają świadomość operacyjną, tak aby nasi klienci mogli sami je przetestować.



Małgorzata Fornal
Dussmann Polska

Dla mnie jest to rewelacyjny pomysł na stworzenie tego typu warsztatów. Jestem niesamowicie zadowolona, że tutaj jestem, bo mogę się nauczyć bardzo wielu przydatnych rzeczy, jak i poznać nowości, które tak bardzo w tym naszym świecie w pogoni za nowinkami są istotne.



Bezpieczeństwo end-to-end

Na stanowisku **Inner Range** uczestnicy analizowali bezpieczeństwo systemu kontroli dostępu. Ich zadaniem było spojrzenie na cały system – od identyfikatora i czytnika, przez kontrolery i sieć, aż po serwery, dane i administratorów – oraz wskazanie potencjalnie słabych punktów.



Bartłomiej Bilski
Inner Range

Wielu z dzisiejszych gości nie znało naszego systemu i byli zaskoczeni tym, gdzie nasze systemy funkcjonują. Ci co znali, wiedzieli, że są np. w Muzeum Sztuki Nowoczesnej czy w Warsaw Tower, a to bardzo ciekawe budynki, wręcz ikoniczne dla Warszawy. Dla nas, a szczególnie dla mnie, jest to bardzo ciekawe doświadczenie, to coś zupełnie nowego, zwłaszcza ta formuła.



STid rozszerzyło temat kontroli dostępu poza drzwi budynku. Uczestnicy pracowali nad scenariuszami dotyczącymi bezpieczeństwa pojazdów, parkingów, stref logistycznych i przewożonego ładunku, szukając sposobów na ograniczenie ryzyka nieautoryzowanego dostępu, kradzieży czy ingerencji w transport.



Piotr Karpiński
STid

Warto edukować ludzi. Nadal jest jeszcze wiele do powiedzenia na temat tego, co tak naprawdę już nas zaskakuje w obszarze bezpieczeństwa oraz dyrektyw, które zaczynają nas obowiązywać. NIS 2 i ustawa o KSC mogą nam w tym jedynie pomóc, a jednocześnie niestety otwierają oczy wszystkim na skalę wyzwań, z jakimi musimy się zmierzyć.

Pavel Dolezal
STid

Wydarzenie to jest szczególnie interesujące, ponieważ uczestniczy w nim grono ekspertów reprezentujących organizacje będące użytkownikami końcowymi. Przygotowana przez nas prezentacja ma dla nich istotne znaczenie w kontekście zagadnień związanych z bezpieczeństwem.



Człowiek w centrum zagrożeń

Drugi dzień szkolenia poświęcono zagrożeniom wewnętrznym. **Mjr dr Anna Grabowska-Siwiec,** były oficer kontrwywiadu ABW, poprowadziła zajęcia dotyczące sabotażu, szpiegostwa gospodarczego oraz ochrony informacji. Uczestnicy analizowali ryzyka związane z nieuprawnionym pozyskiwaniem, wykorzystywaniem i ujawnianiem informacji przez pracowników, współpracowników, kontrahentów i inne osoby posiadające dostęp do zasobów organizacji.

Anna Grabowska-Siwiec

W mojej opinii najważniejszym przesłaniem tego szkolenia jest przekonanie, że to, czego najbardziej się obawiamy, jest mało prawdopodobne. Z kolei tam, gdzie spodziewamy się czegoś spektakularnego, zazwyczaj nic takiego się nie wydarza. To właśnie sprawia, że stajemy się nieco mniej czujni. W organizacji istnieje wiele obszarów, którym powinniśmy się uważnie przyjrzeć. Musimy również poszukiwać osób, które będą w stanie kompetentnie dbać o jej bezpieczeństwo.





Arkadiusz Mojżyszek
Lidl

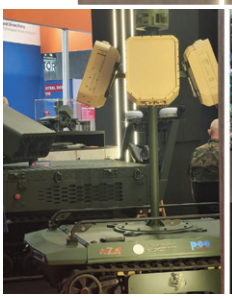
Najbardziej nas zainteresowała kwestia kontroli dostępu. Jesteśmy akurat w trakcie modyfikacji w tym zakresie. Współpracujemy także na co dzień z firmą Securitas, więc tutaj mamy sporo wspólnego, jeżeli chodzi o ten proces.

To właśnie praktyczny charakter Security BootCampu, możliwość wymiany doświadczeń i bezpośredniej konfrontacji z realnymi scenariuszami sprawiły, że dwa dni szkolenia stały się nie tylko źródłem wiedzy, ale również intensywnym treningiem reagowania na sytuacje, z którymi osoby odpowiedzialne za bezpieczeństwo mogą spotkać się w swojej codziennej pracy.

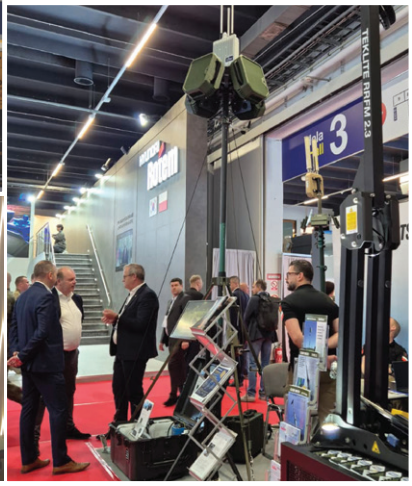
Linc Polska

MSPO 2026 – technologie w obliczu realnych zagrożeń









W tym roku w Kielcach nie rozmawialiśmy o teoretycznej przyszłości. Prezentowane technologie przechodzą dziś najtrudniejszy test w warunkach bojowych, m.in. na froncie w Ukrainie. Nasza obecność była czymś więcej niż tylko ekspozycją sprzętu. Towarzyszyła jej przede wszystkim misja edukacyjna – dzielenie się doświadczeniem i wiedzą o technologiach, które pomagają przygotować się na zagrożenia, zanim nadejdą.

Przedstawiciele LINC Polska byli obecni na stoiskach – wspólnie z TEKSAM COMPANY NV oraz na stoisku Echodyne. W przestrzeni Teledyne FLIR można było zapoznać się z oferowanymi przez nas zaawansowanymi kamerami termowizyjnymi. Prezentowaliśmy rozwiązania wspierające ochronę obiektów i infrastruktury, wykrywanie zagrożeń oraz bezpieczeństwo ludzi – w zastosowaniach zarówno cywilnych, jak i wojskowych.

Jednym z głównych tematów tegorocznej obecności były systemy C-UAS. Drony zmieniły sposób myślenia o ochronie baz wojskowych. Skuteczna odpowiedź wymaga współdziałania wielu warstw technologii: od sensorów RF, przez radary dopplerowskie, po głowice EO/IR – technologie umożliwiające precyzyjne śledzenie i identyfikację celu – aż po decyzję i neutralizację zagrożenia.

Właśnie temu poświęciliśmy konferencję „Wykrywanie i zwalczanie dronów – w bazie i na froncie", zorganizowaną wspólnie z Wojskowym Instytutem Techniki Pancernej i Samochodowej. Cztery wystąpienia pokazały problem z różnych perspektyw – radarów, platform bezzałogowych, efektorów oraz wielowarstwowej ochrony baz.

Na MSPO pokazaliśmy również nowe wydanie „Wizji Expert" – magazynu eksperckiego LINC Polska poświęconego technologiom bezpieczeństwa i obrony. Tym razem skupiliśmy się m.in. na tematyce C-UAS, balistyce i wielowarstwowej ochronie.

Nasza obecność wykraczała daleko poza samo stoisko. Dostarczyliśmy radary Echodyne, które można było zobaczyć na stoiskach wielu partnerów oraz w prezentowanych przez nich rozwiązaniach na terenie całych targów.

MSPO było przede wszystkim czasem spotkań – z przedstawicielami wojska, przemysłu obronnego, integratorami i partnerami technologicznymi. Na targach pojawiła się niemal cała załoga LINC Polska. Były rozmowy o konkretnych zagrożeniach, potrzebach i rozwiązaniach.

Dzisiejsza ochrona nie zaczyna się od pojedynczego urządzenia. Zaczyna się od zrozumienia zagrożenia, a następnie połączenia technologii, danych, doświadczenia i ludzi w jeden skuteczny system. •

Roger

Kontrolowany dostęp firm zewnętrznych. Istotny element bezpieczeństwa zakładów produkcyjnych



Regularne przeglądy, konserwacje i remonty wymagają obecności na terenie zakładu pracowników firm zewnętrznych. Jest to stały element funkcjonowania większości fabryk i magazynów, ale jednocześnie jeden z najczęściej pomijanych obszarów bezpieczeństwa.

W praktyce kluczowe jest nie tylko ustalenie, kto pojawia się w obiekcie, lecz także określenie, kiedy, gdzie i przez jaki czas może w nim przebywać. Tymczasowe identyfikatory, klucze czy ręcznie prowadzone rejestry często nie zapewniają wystarczającej kontroli nad ruchem podwykonawców.

Nowoczesne systemy kontroli dostępu pozwalają nadawać uprawnienia wyłącznie na czas realizacji zlecenia, ograniczać dostęp do wskazanych pomieszczeń oraz automatycznie rejestrować wszystkie zdarzenia. Dzięki temu przedsiębiorstwo zyskuje pełną wiedzę o obecności firm zewnętrznych, a jednocześnie usprawnia procesy związane z audytami i zgodnością z procedurami bezpieczeństwa.

Takie możliwości oferuje system kontroli dostępu RACS 5 firmy Roger, który pozwala elastycznie zarządzać uprawnieniami użytkowników oraz integrować kontrolę dostępu z innymi systemami bezpieczeństwa obiektu.

W dobie rosnących wymagań dotyczących ochrony infrastruktury krytycznej i ciągłości działania skuteczna kontrola dostępu staje się nie tylko narzędziem ochrony fizycznej, ale również ważnym elementem zarządzania ryzykiem operacyjnym. •


check. create. manage.
Checly
Zakład produkcyjny
wszystkie lokalizacje
Zadania do wykonania
dla mnie
wszystkie
2 gru
Kontrola ochrony fizycznej
Krzysztof Pacel
3 gru
Inspekcja obiektu Południe
Zbigniew Koczwara
4 gru
Kontrola bramy głównej
Łukasz Bleniek
5 gru
Sprawdzenie czujek na wejściu
Jarosław Reguła
6 gru
Kontrola pracownika w recepcji
Franciszek Gola
Checly
the best startup 2023
checly.app

BCS®

dla profesjonalistów





Bezpieczeństwo zaczyna się od właściwego **dostępu**



Więcej przeczytasz na stronie » 10

BCS LINE

POLSKA MARKA BCS

www.bcs.pl
www.facebook.com/bcspl
www.instagram.com/bcskamery