Nr 01/03-2026 | www.wladcysieci.pl

Redaktor naczelny:
dr Mirosław Gumularz

Wydawca portalu:
Axence Sp. z o.o. Sp. j.
ul. Na Zjeździe 11,
30-527 Kraków
NIP: 675-139-95-89

WŁADCY SIECI

W tym wydaniu:

Krajowy system cyberbezpieczeństwa na gruncie NIS2 – posłuchaj rozmowy z Zastępcą Prezesa UODO.

Zapraszamy do posłuchania rozmowy naszego Redaktora Naczelnego dr Mirosława Gumularza z Konradem Komornickim – Zastępcą Prezesa Urzędu Ochrony Danych Osobowych na temat Krajowego systemu cyberbezpieczeństwa na gruncie NIS2.

Link do rozmowy: https://vimeo.com/1177601215/3041ce94ef?share=copy&fl=sv&fe=ci

dr Miroslaw Gumularz | 30 marca 2026

Odpowiedzialności za zasoby IT i zarządzanie dostępem w świetle nowej ustawy o krajowym systemie cyberbezpieczeństwa

Jak wykazałem w tekście dotyczącym inwentaryzacji zasobów IT (tekst dostępny tutaj) w świetle nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, prawidłowo przeprowadzona ewidencja zasobów, procesów i usług stanowi punkt wyjścia budowania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

Niemniej same zestawienia zasobów (m.in. aktywów IT) oraz usług i procesów, które są przez nie wspierane, stanowią zaledwie wstęp do budowy SZBI. Kolejnym (naturalnym) krokiem po inwentaryzacji powinno być przypisanie ról i odpowiedzialności za te zasoby. Proces ten należy realizować w powiązaniu z uznanymi standardami, takimi jak normy ISO. W praktyce chodzi o dwie płaszczyzny przypisania odpowiedzialności:

1. Właścicielstwa (biznesowego lub technicznego) i odpowiedzialności za dany zasób oraz
2. W ramach dostępu na poziomie użytkownika końcowego.

„Właścicielstwo" a odpowiedzialność za ryzyko

Z punktu widzenia zarządzania organizacją, funkcjonowanie SZBI wymusza wyznaczenie podmiotu odpowiedzialnego za weryfikację dostawcy, cykl życia, konfigurację oraz adekwatne zabezpieczenie systemów IT. Z reguły funkcję tę pełnią osoby odpowiedzialne biznesowo za daną

usługę lub proces, co implikuje również odpowiedzialność za zasób IT który ją wspiera. Często te obowiązki są dzielone pomiędzy funkcjami biznesowymi i technicznymi. Znowelizowana ustawa o KSC przesądza, że to kierownik podmiotu (kluczowego lub ważnego) przydziela zadania z zakresu cyberbezpieczeństwa w podmiocie i nadzoruje ich wykonanie.

Działanie to stanowi odzwierciedlenie wymagań normy ISO 27001, która w wskazuje, że najwyższe kierownictwo powinno zapewnić przydzielenie (oraz zakomunikowanie) w organizacji ról, odpowiedzialności i uprawnień. Ponadto, w ramach załącznika A do tej normy wymaga się, aby role i odpowiedzialność za bezpieczeństwo informacji zostały jednoznacznie określone i przypisane zgodnie z potrzebami organizacji.

Role techniczne i biznesowe

Należy zauważyć, że zmiana w KSC nie przesądza zasad podziału ról biznesowych i technicznych. Zgodnie z art. 8d pkt 3 znowelizowanej ustawy o KSC, to kierownik podmiotu kluczowego lub ważnego przydziela zadania z zakresu cyberbezpieczeństwa w tym podmiocie i nadzoruje ich wykonanie. Wskazany przepis nie przesądza czy chodzi o role biznesowe czy techniczne. Jest bardzo ogólny i nie wyklucza rozdzielenia lub połączenia tych ról. Punktem odniesienia będzie tu analiza ryzyka. Dodatkowo prawodawca potwierdza możliwość wyodrębnienia (a nawet outsourcingu) ról technicznych, wskazując w art. 14 na dopuszczalność zawarcia umowy z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa. Można z tego wnioskować, że przepisy dostrzegają konieczność włączenia w SZBI także osób z biznesu. Jest to zresztą zgodne z powszechną praktyką w zakresie wdrażania systemów bezpieczeństwa. Sama wiedza techniczna nie jest wystarczająca żeby zrozumieć wpływ incydentu dotyczącego systemu IT na działalność operacyjną – świadczenie usług.

W związku z tym należy przyjąć, że właściciel biznesowy – decydujący o celowości przetwarzania informacji oraz kształcie procesu realizowanego za pomocą danego zasobu – może, lecz nie musi, pełnić funkcji właściciela technicznego (np. administratora IT czy architekta bezpieczeństwa).

Właściciel biznesowy a właściciel ryzyka

W tym miejscu należy dokonać kolejnego rozróżnienia pojęciowego. Jak wskazano powyżej punktem wyjścia przypisywania odpowiedzialności w organizacji jest rola właściciela biznesowego, decydującego o celowości, finansowaniu i cyklu życia zasobu wspierającego dany proces / usług.

Z kolei odrębnym pojęciem jest właściciel ryzyka zdefiniowany w normie ISO 27005 jako osoba lub podmiot posiadający odpowiedzialność i uprawnienia do zarządzania danym ryzykiem. Wskazane role często kumulują się w rękach jednej osoby. Norma ISO 27005 wskazuje, że właścicielami ryzyka mogą być między innymi najwyższe kierownictwo, komitet ds. bezpieczeństwa, właściciele procesów, właściciele funkcji, menedżerowie działów oraz właściciele aktywów. Oznacza to, że właściciel biznesowy zasobu może być jednocześnie właścicielem ryzyka.

Właściciel biznesowy a osoba odpowiedzialna za SZBI

Należy zauważyć, że w toku operacjonalizacji obowiązków wynikających z nowelizacji wyłania się problem na styku prawa cyberbezpieczeństwa, prawa pracy oraz ochrony danych osobowych. Dotyczy on bezpośrednio zakresu podmiotowego obowiązku weryfikacji personelu.

Zgodnie z art. 8f ust. 1 (w nowej wersji KSC), przed rozpoczęciem realizacji zadań osoba, która ma te zadania realizować, przedstawia podmiotowi informację z Krajowego Rejestru Karnego stwierdzającą niekaralność za przestępstwa przeciwko ochronie informacji. Przepis ten odsyła do zamkniętego katalogu zadań, tj. do obowiązków, o których mowa w art. 8 (ustanowienie i wdrożenie systemu zarządzania bezpieczeństwem informacji) oraz art. 11 (obsługa i zgłaszanie incydentów). W tym kontekście pojawia się pytanie czy każdy właściciel biznesowy aktywu, definiujący cele biznesowe danego zasobu, podlega ustawowemu rygorowi weryfikacji w KRK?

Jak precyzuje uzasadnienie do projektu ustawy, po otrzymaniu przedmiotowego zaświadczenia kierownik dopuszcza osobę do realizacji zadań związanych z systemem zarządzania bezpieczeństwem informacji oraz zgłaszaniem incydentów. Cel tego rozwiązania opiera się na założeniu, iż osoby, które dopuściły się czynów zabronionych przeciwko ochronie informacji, nie dają należytej rękojmi prawidłowego wykonywania powierzonych im zadań z zakresu cyberbezpieczeństwa. Uzasadnienie projektu wprost dostrzega wagę tej ingerencji w prywatność, podnosząc, że jest to istotne w kontekście przetwarzania danych osobowych, jako że dotyczy to danych o karalności w rozumieniu art. 10 RODO. W tym miejscu należy zadań pytanie czy w takim razie należy weryfikować karalność każdej osoby, która ma jakiekolwiek obowiązki w ramach SZBI? W tym osoby nie-technicznej? Z pozoru wydaje się to nadmiarowe. Sprawa jest jednak nieoczywista i należy liczyć w tym przypadku na stanowisko UODO.

Do czasu zajęcia stanowiska przez organ nadzorczy, podmiotom objętym zmianą w KSC należy zalecać daleko posuniętą ostrożność. Należy badać faktyczną rolę tych podmiotów. Moim zdaniem krytyczne będzie tu przypisanie odpowiedzialności jakie wskazane osoby pełniące funkcje biznesowe ponoszą w toku analizy ryzyka. Argumentem przemawiającym za koniecznością pozyskania informacji z Krajowego Rejestru Karnego od właścicieli biznesowych (jeżeli będą mieć role w zakresie analizy ryzyka) jest literalne brzmienie art. 8 ust. 1 pkt 1 nowej KSC. Przepis ten wprost definiuje, że przeprowadzanie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem jest elementem funkcjonowania SZBI.

Kaskadowanie zadań i zarządzanie uprawnieniami użytkowników

Drugim elementem wdrażania siatki ról i odpowiedzialności jest określenie zasad korzystania z zasobów przez wszystkich użytkowników w organizacji.

Ustawodawca wyznaczył w tym zakresie rygorystyczne zasady. Przykładowo w załączniku nr 4 do ustawy o KSC, wymaga się dopuszczenia do informacji wyłącznie osób posiadających stosowne uprawnienia do systemów informacyjnych, co ma uniemożliwić nieautoryzowany dostęp. Chociaż załącznik nr 4 stanowi zbiór uproszczonych wymagań adresowanych ściśle do podmiotów ważnych będących podmiotami publicznymi, to z perspektywy systemowej należy przyjąć, że będzie miał szersze znaczenie.

Ponadto, cykl życia uprawnień musi mieć charakter dynamiczny, dlatego wymagana jest modyfikacja zakresu praw w przypadku zmiany charakteru wykonywanych zadań oraz bezzwłoczne cofanie uprawnień w sytuacji utraty podstawy dostępu, a także ich zawieszanie w przypadku nie wykonywania obowiązków przez co najmniej jeden miesiąc. Mechanizm ten odpowiada wytycznym normy ISO 27001, nałożonym w obszarze przydzielania, przeglądania, modyfikowania i odbierania praw dostępu.

W tym miejscu należy też podkreślić formalny aspekt dostępu do informacji, w tym w zakresie oświadczeń o zachowaniu poufności. W tym zakresie KSC nie jest tak precyzyjna jak RODO i głównie skupia się na ocenie ryzyka. Moim zdaniem jednak odebranie niezbędnych oświadczeń będzie standardem. Wagę tego formalnego problemu dobrze pokazuje ostatnia decyzja Prezesa UODO w odniesieniu do upoważnień do przetwarzania danych osobowych i kary dla DPD (zob. https://uodo.gov.pl/pl/138/4075). Choć rozstrzygnięcie to nie zapadło na gruncie dyrektywy NIS 2, ukazuje analogiczny problem zarządczy. Jak wskazał Prezes UODO: „administrator nie udzielał pracownikom skutecznie i prawidłowo upoważnień do przetwarzania danych [...]. W zamyśle spółki, nowym pracownikom upoważnienia były udzielane automatycznie przez system informatyczny po odbyciu przez nich szkolenia [...]. Zaliczenie testu powodowało automatyczne wygenerowanie pliku z treścią sugerującą, że jest to upoważnienie do przetwarzania danych, jednak niezawierające istotnych elementów takich jak imię i nazwisko pracownika oraz podpis osoby udzielającej upoważnienia. Wobec powyższego, PUODO uznał, że generowanego automatycznie z systemu pliku o niejasnej treści nie można zakwalifikować jako upoważnienia". Prowadzi to do konkluzji, że w architekturze cyberbezpieczeństwa automatyzacja procesów IT nie zwalnia organizacji z formalnej, personalnej odpowiedzialności za dostęp.

Podsumowanie

Reasumując, następstwem inwentaryzacji zasobów informatycznych musi być wdrożenie siatki ról i odpowiedzialności. Wyznaczenie właścicieli biznesowych, pełniących nierzadko funkcję właścicieli ryzyka, jest warunkiem koniecznym dla skutecznego kaskadowania zadań. Właściwe przypisanie odpowiedzialności w SZBI obejmuje szerokie spektrum działań operacyjnych, takich jak systematyczne monitorowanie podatności technicznych, proaktywne monitorowanie zagrożeń w sieciach, restrykcyjne zarządzanie uprawnieniami (w tym bezwzględne ograniczanie kont uprzywilejowanych), czy weryfikacja łańcucha dostawców.

dr Miroslaw Gumularz | 18 marca 2026

Cisco XDR

Przez lata działanie SOC-ów opierało się na dwóch filarach: SIEM i EDR. SIEM zbierał logi i generował alerty, EDR chronił urządzenia końcowe. Problem polegał na tym, że atakujący dawno przestali ograniczać się do endpointów. Dzisiejszy łańcuch ataku przebiega jednocześnie przez pocztę, tożsamość, sieć, chmurę i endpoint. Analityk SOC musiał żonglować między konsolami, ręcznie korelować dane i gubił się w tysiącach alertów bez kontekstu.

XDR, czyli Extended Detection and Response, miał odpowiedzieć na ten problem. Zamiast zbierać logi i zostawiać korelację człowiekowi. XDR natywnie integruje telemetrię z wielu źródeł, koreluje ją automatycznie i prezentuje już gotowy incydent z priorytetem i kontekstem.

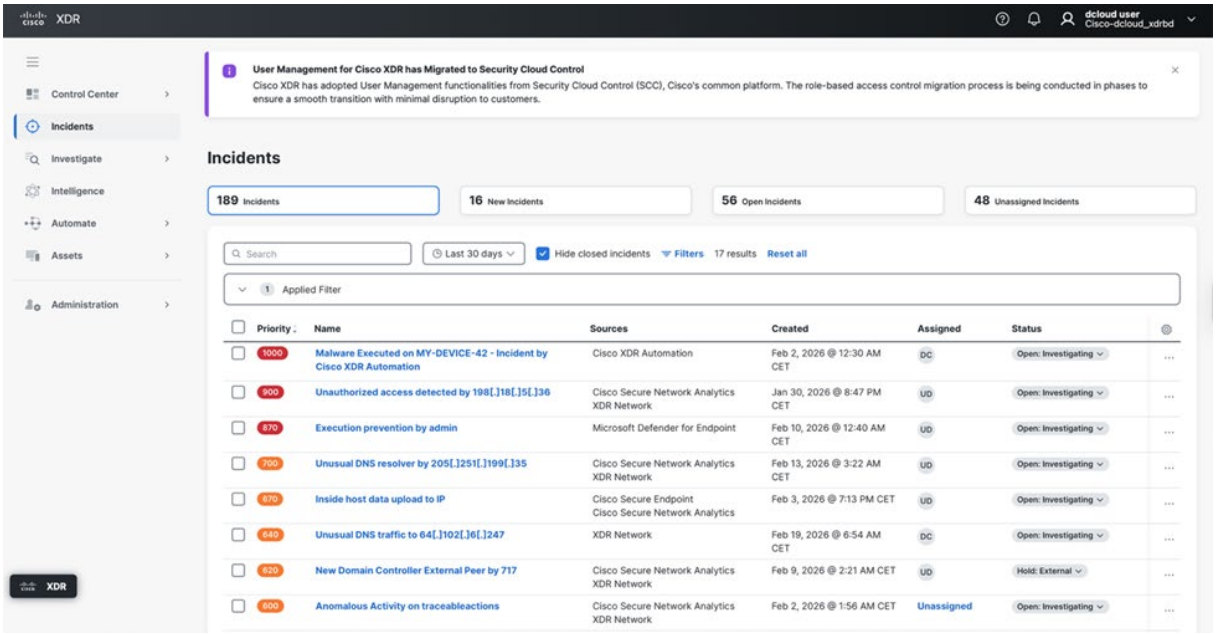
Cisco XDR to cloudowa platforma tej klasy, dostępna od 2023 roku, zbudowana na fundamencie wcześniejszego Cisco SecureX. Cisco wyróżnia się w tym segmencie jedną istotną cechą: zamiast skupiać się wyłącznie na endpointach, stawia sieć jako równorzędne źródło detekcji, a to duża różnica w środowiskach enterprise.

Co Cisco XDR konkretnie robi?

Cisco XDR analizuje i koreluje sześć źródeł telemetrii uznawanych przez operatorów SOC za krytyczne: endpoint, sieć, firewall, email, tożsamość i DNS. To nie jest tylko agregacja logów – platforma koreluje dane na poziomie semantycznym, łącząc zdarzenia w jeden wiarygodny incydent zamiast generować tysiące osobnych alertów.

Cisco XDR zawiera wbudowane natywne możliwości NDR (Network Detection and Response) prowadzące do szybkiej identyfikacji anomalii sieciowych zarówno w środowiskach on-premises,

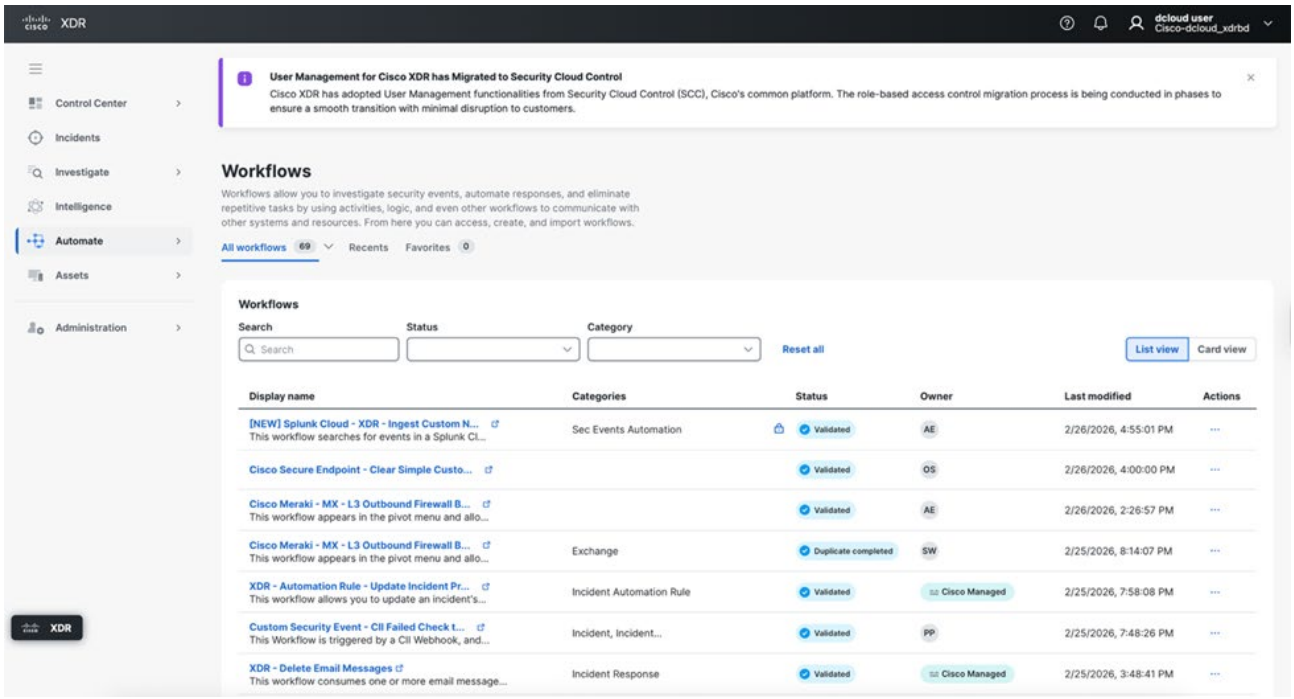
jak i cloud. Daje to widoczność na urządzenia niezarządzane, IoT i OT, które nie mogą uruchamiać tradycyjnych agentów endpointowych. W praktyce oznacza to, że nawet urządzenia bez agenta, takie jak sterowniki PLC, kamery IP czy kontrolery budynkowe, są widoczne w kontekście incydentu. No właśnie – incydentu. Cisco XDR nie wyrzuca alertów. Zamiast tego prezentuje gotowy incydent z oceną ryzyka i wyliczoną ścieżką ataku zmapowaną na framework MITRE ATT&CK. Analityk widzi od razu: co się dzieje, jak daleko się to posunęło, jakie zasoby są zagrożone.



Platforma zawiera bibliotekę gotowych playbooków reagowania na incydenty, które można uruchomić jednym kliknięciem lub w pełni zautomatyzować. Automatyzacja może natychmiastowo izolować endpoint, zablokować IP i poddać kwarantannie plik, wstrzymując takie zagrożenia jak ransomware w ciągu sekund. Orkiestracja synchronizuje działania między narzędziami bezpieczeństwa, na przykład rekonfigurując firewall do blokowania domeny, skanując endpoint i logując alert w SIEM jednocześnie. Cisco XDR wykrywa wczesne sygnały ataku ransomware i może automatycznie wywołać tworzenie snapshotu krytycznych zasobów przed zaszyfrowaniem. Potem umożliwia przywrócenie ostatniego dobrego stanu konfiguracji ze skróconą przerwą w działaniu systemu. Cisco XDR Forensics rozszerza rolę platformy o mechanizmy przyśpieszające zbieranie dowodów. Analityk może przeprowadzić dochodzenie bez fizycznego dostępu do maszyny.

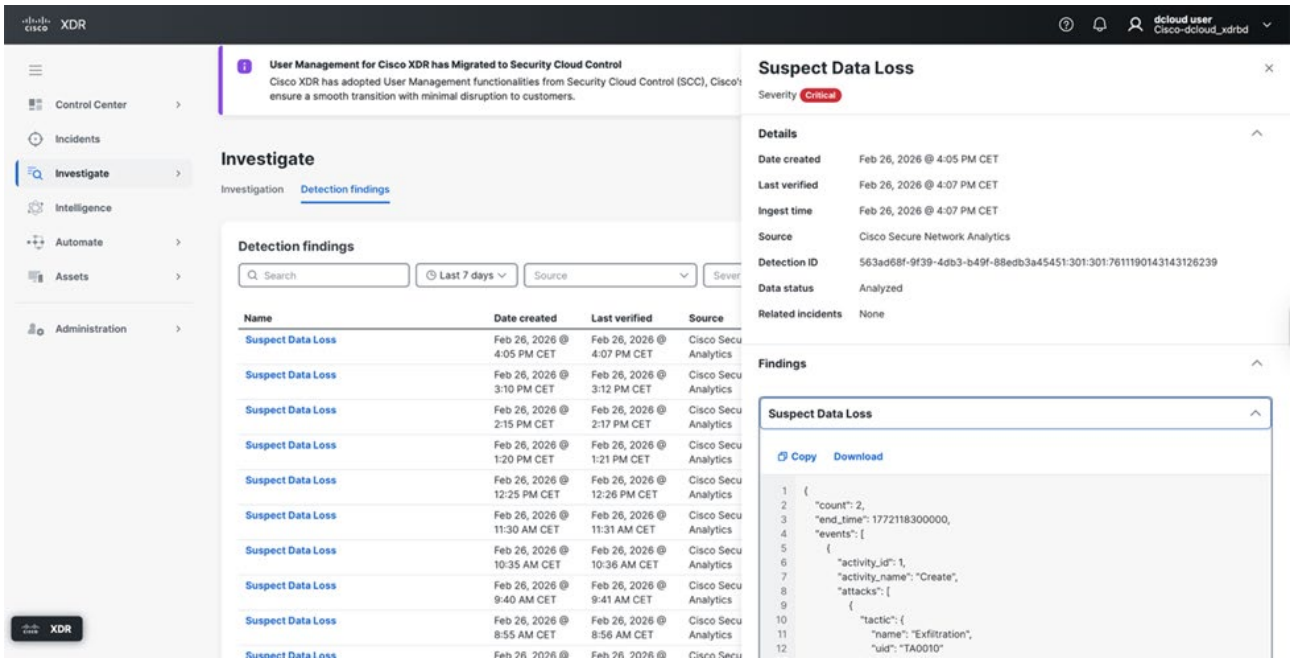
Cała detekcja jest wzbogacana o dane pochodzące z Cisco Talos, czyli jednego z największych komercyjnych zespołów threat research na świecie. Talos dostarcza kontekst i informacje o nowych kampaniach w czasie rzeczywistym. AI Assistant w XDR dostarcza opartych na danych wskazówek, kolejnych kroków i taktyk remediacji, prowadząc analityka przez odpowiedź na incydenty. Jest to szczególnie przydatne dla mniej doświadczonych analityków SOC, bo w praktyce „wyrównuje poziom" zespołu.

Cisco XDR oferuje dwa poziomy integracji. Natywnie integruje się z całym portfelem Cisco Security: Secure Endpoint, Umbrella, Secure Email, Meraki MX, Duo, Firepower/FTD. Na poziomie Advantage i wyżej dostępne są komercyjnie wspierane integracje third-party z narzędziami innych vendorów, takich jak Microsoft, CrowdStrike, Splunk, ServiceNow i wieloma innymi.



Kiedy stosować Cisco XDR, a kiedy nie?

Środowisko oparte na ekosystemie Cisco to najoczywistszy przypadek, w którym Cisco XDR się sprawdzi. Jeśli w organizacji działają Cisco Secure Endpoint, Cisco Umbrella, Cisco Email Security, Meraki lub Firepower/FTD, Cisco XDR jest naturalnym wyborem. Integracja jest natywna, bez dodatkowych konektorów i licencji. Użyteczność platformy pojawia się niemal od razu po włączeniu, bez tygodni konfiguracji. Organizacje proedukcyjne, energetyczne, infrastruktura krytyczna – wszędzie tam, gdzie sieć pełna jest urządzeń, na których nie można uruchomić agenta, to kolejny obszar. Cisco XDR dzięki natywnym możliwościom NDR widzi anomalie sieciowe tych urządzeń i włącza je w kontekst incydentu. Produkt przyda się także, jeśli SOC tonie w alertach z pięciu różnych konsoli i chce skonsolidować widok, Cisco XDR jako centrum korelacji i response jest sensownym krokiem. Funkcja automatycznego snapshotu i odtworzenia po ataku ransomware to konkretna wartość w sektorach, gdzie downtime jest kosztowny: w szczególności produkcja, healthcare, logistyka. Jeśli organizacja żyje w Microsoft 365 i Azure, ma CrowdStrike na endpointach i Palo Alto na firewallu, koszty integracji i licencji third-party w Cisco XDR mogą przewyższyć wartość. W takiej sytuacji Microsoft Defender XDR albo Cortex XDR będzie miał naturalną przewagę wynikającą z głębszej integracji z istniejącym stosem. Kupowanie Cisco XDR bez żadnych innych produktów Cisco to kupowanie drogiej platformy bez natywnych źródeł telemetrii. Technicznie możliwe przez integrację third-party, ale kosztowne i trudniejsze do uzasadnienia. Jeśli główny problem to detekcja na endpointach i analiza malware'u, a nie korelacja między domenami, CrowdStrike Falcon lub SentinelOne dadzą głębszą ochronę endpointową za podobne pieniądze. Cisco XDR nie jest najsilniejszy jako standalone EDR. W środowiskach serverless i cloud-native, gdzie sieć korporacyjna de facto nie istnieje, przewaga Cisco w NDR zanika. Palo Alto Cortex XDR lub Microsoft Defender XDR mogą być lepiej dopasowane do integracji z usługami chmurowymi.



Produkty alternatywne

CrowdStrike to aktualny lider rynku EDR/XDR pod względem udziałów i liczby recenzji. Platforma Falcon jest cloud-native, nie wymaga infrastruktury on-premises, lekkiego agenta można szybko wdrożyć na endpointach, a interfejs jest uważany za przyjazny. Mocne strony CrowdStrike to przede wszystkim głębokość detekcji endpointowej, Falcon OverWatch oferuje całodobowy threat hunting jako usługę. CrowdStrike odpada, jest skupiony na urządzeniach końcowych, więc nie wszędzie się sprawdzi. Na przykład jego integracja z siecią i OT jest słabsza niż w Cisco XDR. Incydent z lipca 2024, w którym aktualizacja sensora wywołała BSOD na milionach maszyn z Windows, nadal ciąży na reputacji vendora. Cisco XDR ma wyraźną przewagę tam, gdzie krytyczne są urządzenia sieciowe i bez agenta. Dla kogo CrowdStrike zamiast Cisco XDR? Dla organizacji z minimalną infrastrukturą Cisco, które chcą najlepszej ochrony endpointów i mają heterogeniczny stack. Szczególnie polecany w środowiskach, gdzie sieć to głównie chmura, a fizycznych urządzeń sieciowych jest mało.

Inną alternatywą jest Microsoft Defender XDR (dawniej Microsoft 365 Defender). To platforma zintegrowana z ekosystemem Microsoft: Defender for Endpoint, Defender for Identity, Defender for Office 365, Defender for Cloud Apps. W przypadku organizacji już posiadających licencje M365 E3/E5, koszt użycia Microsoft Defender jest nieporównywalnie niższy i przeliczany na użytkownika miesięcznie lub wliczony w posiadaną licencję.

Mocna strona Microsoft Defender XDR to integracja z Azure AD/Entra ID i Microsoft 365, która jest niezrównana. Jeśli środowisko to w 90% Microsoft, Defender XDR jest naturalnym centrum korelacji. Koszty są niskie, wdrożenie jest stosunkowo proste dla organizacji z istniejącym M365. Niestety, poza ekosystemem Microsoftu widoczność drastycznie spada. Detekcja sieciowa jest słaba, brak natywnego NDR porównywalnego z Cisco XDR. W środowiskach hybrydowych z dużą infrastrukturą sieciową Cisco XDR wyraźnie wygrywa. Dlatego Microsoft Defender XDR dedykowany jest dla organizacji opartych na Microsoft 365, Azure i Windows. Szczególnie tam, gdzie budżet jest ograniczony i sensowne jest wykorzystanie już posiadanych licencji.

A może Wazuh?

Wazuh unifikuje funkcje SIEM i XDR w jednym agencie i architekturze platformy. Ochrona obejmuje chmury publiczne, prywatne i środowiska on-premises. Architektura opiera się na czterech komponentach: agent na endpoincie, serwer zarządzający (manager), indekser oparty na OpenSearch, i dashboard. Każdy z nich można skalować horyzontalnie. Agent obsługuje Windows, Linux, macOS, kontenery Docker, VMware. Dla urządzeń bez agenta (routerów, przełączników, firewalli) Wazuh odbiera dane przez syslog lub SNMP. Agenty Wazuh skanują monitorowane systemy w poszukiwaniu malware, rootkitów i podejrzanych anomalii. Wykrywają ukryte pliki, zamaskowane procesy, niezarejestrowane nasłuchujące porty sieciowe oraz niespójności w odpowiedziach wywołań systemowych.

Natywnie Wazuh dostarcza kilka funkcjonalności. Jedną z nich jest monitorowanie zmian w plikach krytycznych (zawartość, uprawnienia, właściciel, atrybuty) oraz mapowanie do frameworka MITRE ATT&CK. Użytkownik i aplikacja modyfikująca plik są identyfikowane natywnie. Dodatkowo agent zbiera informacje o oprogramowaniu na urządzeniu końcowym i koreluje informacje z bazą CVE. Administrator otrzymuje dzięki temu automatyczną ocenę podatności bez dodatkowych narzędzi. Wazuh pozwala też na automatyczne skanowanie konfiguracji systemu pod kątem CIS Benchmarks, NIST, PCI DSS, HIPAA. Alert zawiera rekomendację, jak poprawić konfigurację. IDS zaś konstruujemy na regułach opartych na logach i anomaliach. Biblioteka ponad 3000 gotowych reguł, łatwa do rozszerzania. Reguły Sigma można konwertować do formatu Wazuh.

Nie jest to jednak bezpośredni odpowiednik ani konkurencja dla Cisco XDR. Właściwi rywale komercyjni w XDR (jak CrowdStrike Falcon) osiągają wyższą skuteczność detekcji zagrożeń, szczególnie w czasie rzeczywistym. Wazuh opiera detekcję na konfigurowalnej analizie reguł i logów, co fundamentalnie różni go od metod stosowanych przez wyspecjalizowanych producentów komercyjnych. Brak natywnej AI do korelacji incydentów. Cisco XDR przychodzi z gotowym ML, który automatycznie łączy zdarzenia w incydenty z priorytetem. W Wazuh musisz napisać reguły korelacji samodzielnie albo podpiąć zewnętrzne narzędzie. Produktowi brak też automatycznego playbooka typu response jak w Cisco. Active Response w Wazuh to proste skrypty uruchamiane lokalnie. Zaawansowane playbooki wymagają integracji z zewnętrznym SOAR (TheHive, Shuffle, n8n). Brak analogicznego threat intelligence do Talos to kolejna jego słaba strona. Wazuh integruje się z zewnętrznymi feedami (MISP, VirusTotal), ale nie ma własnego team researchowego. Sam NDR jest też słabszy. Wazuh widzi sieć przez logi i syslog z urządzeń sieciowych, nie ma natywnych możliwości analizy behawioralnej ruchu sieciowego porównywalnych z Cisco NDR.

Największym błędem finansowym przy ocenie Wazuh jest utożsamianie braku kosztów licencji z brakiem kosztów operacyjnych. Dla własnego wdrożenia brak opłat licencyjnych przekształca CapEx w istotny OpEx zdominowany przez koszty specjalistycznej pracy. Do tego trzeba dodać: infrastrukturę serwerową (indekser OpenSearch na dużych środowiskach potrzebuje niemałych zasobów RAM i dysku), czas na konfigurację, tuning reguł i utrzymanie. Dla dużego enterprise z setkami tysięcy eventów dziennie Wazuh może wymagać klastra z wieloma węzłami. To przestaje być darmowe.

Zamiast kupować monolityczny XDR możesz zbudować stos z narzędzi open source pokrywających każdą warstwę. Tylko to już zupełnie inny typ projektu i skala zagrożeń.

Piotr Wojciechowski | 26 marca 2026

Wnioski z raportu IBM X-Force Threat Intelligence Index 2026

Raport IBM X-Force Threat Intelligence Index 2026 wskazuje, że pomimo rosnącego wykorzystania sztucznej inteligencji przez cyberprzestępców, główną przyczyną skutecznych ataków pozostają elementarne braki w higienie bezpieczeństwa informatycznego. Z analizy wynika, że zautomatyzowane narzędzia ofensywne przyspieszają działania sprawców, jednak fundamentem ich sukcesu jest nadal wykorzystywanie luk w systemach o ekspozycji publicznej, słabych mechanizmów uwierzytelniania oraz zależności w łańcuchach dostaw.

Główne wektory ataków i statystyki

Zgromadzone dane ujawniają wzrost o 44 procent w zakresie wykorzystywania podatności aplikacji publicznych jako wektora początkowego dostępu. Problem ten potęguje fakt, że spośród

niemal 40 tysięcy luk w zabezpieczeniach zidentyfikowanych w 2025 roku, aż 56 procent nie wymagało od atakującego żadnego uwierzytelnienia do skutecznego wykorzystania. Należy przy tym zaznaczyć, że przestępcy nie zrezygnowali z tradycyjnych metod kompromitacji. Jak podaje IBM wykorzystanie legalnych, lecz skradzionych wcześniej danych logowania nadal odpowiadało za 32 procent wszystkich incydentów, pozwalając atakującym na niezauważalne wtopienie się w normalny ruch sieciowy bez konieczności przełamywania zabezpieczeń. W kontekście tożsamości cyfrowej zaobserwowano wyciek ponad 300 tysięcy poświadczeń do usługi ChatGPT, pozyskanych głównie za pomocą oprogramowania typu *infostealer*. Zdaniem IBM zjawisko to potwierdza, że platformy oparte na sztucznej inteligencji niosą obecnie ryzyko porównywalne z kluczowymi systemami korporacyjnymi. Ponadto IBM zwraca uwagę, że na przestrzeni ostatnich pięciu lat odnotowano blisko czterokrotny wzrost liczby poważnych naruszeń obejmujących łańcuch dostaw i podmioty trzecie.

Trendy rynkowe i profil ofiar

IBM podkreśla, że ekosystem oprogramowania ransomware uległ rozdrobnieniu, co świadczy o obniżeniu progu wejścia dla cyberprzestępców. Liczba aktywnych grup wzrosła o 49 procent w porównaniu z rokiem 2024, osiągając pułap 109 zidentyfikowanych podmiotów. Pod względem sektorowym głównym celem ataków pozostaje niezmiennie przemysł wytwórczy, obejmujący 27,7 procent wszystkich incydentów, wyprzedzając jedynie o ułamek procenta sektor finansowy i ubezpieczeniowy (27 procent). Zmianie uległa również geografia zagrożeń. Ameryka Północna stała się najczęściej atakowanym regionem, odpowiadając za 29 procent spraw i tym samym wyprzedzając region Azji i Pacyfiku. Zdaniem IBM prowadzi to do konkluzji, że wobec łatwego dostępu do narzędzi przestępczych, najskuteczniejszą obroną pozostaje rygorystyczna konfiguracja dostępu oraz kompleksowa ochrona tożsamości w sieci.

Źródło: https://www.ibm.com/reports/threat-intelligence.

dr Mirosław Gumularz | 5 marca 2026

Bezpieczeństwo IoT – dlaczego warto na nie zwrócić uwagę?

Wszyscy dobrze wiemy, że zapalona świeca w nieodpowiednim miejscu może doprowadzić do pożaru. Podobnie jako władca sieci, nie zostawiaj urządzeń podłączonych do sieci bez nadzoru. W Internecie rzeczy (IoT / Internet of Things), wiele urządzeń posiada możliwość komunikacji ze światem zewnętrznym, na przykład w celu zdalnej kontroli. Ciekawym przykładem tego jak urządzenie podłączone do sieci bez nadzoru potrafi narobić dużo zamieszania jest mały termometr do akwarium. Niepozorny, ale połączony z infrastrukturą kasyna, doprowadzi do kosztownych strat.

Dla zainteresowanych niniejszy link opisuje dokładniej wspomniany incydent. Przed rekomendacjami i poradami, jakie rozwiązania można wdrożyć, warto najpierw poznać rodzaje ataków i zagrożeń.

Ataki na sieci Wi-Fi (w tym IoT)

- **Ataki dysocjacyjne** polegają na wysyłaniu fałszywych ramek danych w celu rozłączenia klienta z punktem dostępu. Umożliwia przerywanie komunikacji lub przygotowanie gruntu pod kolejne ataki.
- **Ataki blokujące usługę (DoS)** w Wi-Fi, które mają na celu uniemożliwienie działania sieci, na przykład przez zalewanie punktu dostępu ramkami asocjacyjnymi lub zakłócanie kanału radiowego.
  Zakłócanie sygnału radiowego czyli w praktyce atakujący generuje silne sygnały radiowe

na przykład przy użyciu SDR, które uniemożliwiają innym urządzeniom korzystanie z danego kanału.

Ataki asocjacyjne (Man-in-the-Middle)

- **Evil Twin** to atak polegający na utworzeniu fałszywego punktu dostępu o tej samej nazwie (ESSID), adresie BSSID i metodzie szyfrowania co legalny AP, ale z silniejszym sygnałem. Klient łączy się z nim, myśląc, że to zaufana sieć.
- **Atak KARMA** wykorzystuje automatyczne wyszukiwanie sieci przez klienta. Atakujący odpowiada na żądania sondujące i zmusza klienta do połączenia z fałszywym, otwartym punktem dostępu.
  Known Beacons jest atakiem polegający na podszywaniu się pod popularne lub wcześniej używane przez klienta sieci (na przykład „Guest", „FREE Wi-Fi"), co powoduje automatyczne połączenie klienta z fałszywym AP.

Ataki na szyfrowanie Wi-Fi

- **Łamanie WPA/WPA2 (PSK)** czyli przechwycenie czteroetapowego uwierzytelnienia (handshake), a następnie próba odgadnięcia klucza metodą brute force.
  Atak na PMKID atak na sieci WPA/WPA2 wykorzystujące identyfikator PMKID, który umożliwia łamanie hasła bez przechwytywania pełnego handshake.
- **Inne rodzaje ataków**
- **Ataki na sieci LoRaWAN to atak odtworzeniowy (Replay)** charakteryzuje się ponownym wysłaniem wcześniej przechwyconych poprawnych komunikatów. Może być skuteczny w określonych scenariuszach (na przykład reset liczników ramek w ABP).
- **Bit-flipping** polega na modyfikacji pojedynczych bitów zaszyfrowanych danych aplikacyjnych bez ich deszyfrowania, co może prowadzić do zmiany znaczenia przesyłanych informacji.
- **Fałszowanie potwierdzeń (ACK spoofing)** jest atakiem przy pomocy wysyłania sfałszowanych potwierdzeń w celu zablokowania usługi lub zakłócenia poprawnej komunikacji między węzłem a serwerem.
- **Denial of Service (DoS) w LPWAN** to przeciążenie sieci lub urządzeń (np. LoRaWAN, Sigfox, NB-IoT), aby uniemożliwić obsługę poprawnych komunikatów.
- **Zagłuszanie (Jamming)** to zakłócanie transmisji radiowej poprzez emisję sygnałów na tej samej częstotliwości, co skutecznie blokuje komunikację urządzeń.
- **Ponowna transmisja zmodyfikowanej ramki (Replay – zaawansowany)** skupia się na ponownym nadawaniu przechwyconych i zmodyfikowanych ramek. Ten atak jest trudny do realizacji ze względu na mechanizmy szyfrowania i kontroli integralności.
- **Podsłuch (Eavesdropping)** to atak związany z przechwytywaniem ruchu sieciowego w celu analizy komunikacji, pozyskania metadanych lub przygotowania kolejnych ataków.

Krótko poniżej zostały wspomniane regulacje wprowadzone przez Unie Europejską, które również mogą być podpowiedziami na co zwrócić uwagę w temacie bezpieczeństwa IoT.

EU Data Act to regulacja między innymi dotycząca urządzeń połączonych z Internetem czyli IoT, których dane są generowane w ogromnych ilościach. Użytkownikom tych urządzeń przysługuje prawo dostępu, przenoszenia i udostępniania danych, co wpływa na sposób projektowania i sprzedaży urządzeń IoT oraz platform analizujących te dane.

Dyrektywa NIS2 choć nie dotyczy konkretnie urządzeń IoT, obejmuje systemy i sieci krytyczne, które coraz częściej integrują urządzenia IoT (np. w energetyce, logistyce czy służbie zdrowia). Firmy, które operują takimi systemami, muszą uwzględniać bezpieczeństwo IoT w swoich procesach zarządzania ryzykiem cybernetycznym.

EU-RED (Radio Equipment Directive) dyrektywa wprowadza ustalenie aby urządzenia IoT komunikujące się bezprzewodowo (smart home, wearable, sensory) muszą od 1 sierpnia 2025 spełniać obowiązkowe wymagania bezpieczeństwa takie jak na przykład ochrona sieci, danych osobowych, prywatności i przeciwdziałanie nadużyciom przed wprowadzeniem na rynek UE.

EU-CRA (Cyber Resilience Act) regulacja ta z kolei obejmuje większość urządzeń IoT ale najbardziej producentów, którzy muszą analizować ryzyka, projektować bezpiecznie, udzielać aktualizacji i zgłaszać incydenty.

Ochrona IoT to proces ciągły, obejmujący sieć, użytkowników, urządzenia końcowe, chmurę oraz sposób zarządzania całością. Podstawą jest pełna widoczność i scentralizowane zarządzanie siecią. Bez wiedzy, jakie urządzenia są podłączone, gdzie się znajdują i w jaki sposób komunikują się z innymi zasobami, nie da się mówić o realnym bezpieczeństwie. W tym kontekście bardzo ważne jest zautomatyzowane rejestrowanie zasobów sprzętowych i programowych, które znacząco poprawia przejrzystość środowiska. **Warto zapamiętać, że urządzenia IoT powinny działać w wydzielonym segmencie, całkowicie odseparowanym od krytycznych systemów oraz danych organizacji. Dotyczy to również oddzielenia IoT od laptopów, komputerów stacjonarnych, tabletów i smartfonów, na których przechowywane są dane firmowe.** Dzięki temu ewentualne naruszenie bezpieczeństwa jednego obszaru nie rozprzestrzeni się na całą infrastrukturę.

Niezwykle istotne jest także zabezpieczenie komunikacji. W praktyce oznacza to stosowanie takich mechanizmów jak prywatne APN (Access Point Name), VPN (wirtualna sieć prywatna), szyfrowanie transmisji oraz uwierzytelnianie urządzeń. W sieciach bezprzewodowych należy korzystać wyłącznie z szyfrowania WPA2 lub WPA3. Równocześnie trzeba pamiętać, że nawet najlepiej zabezpieczona sieć nie będzie bezpieczna, jeśli urządzenia końcowe użytkowników, takie jak smartfony, są podatne na infekcje malware. Z reminderem zainfekowany smartfon może stać się bramą do przejęcia kontroli nad podłączonymi do niego urządzeniami IoT.

Dlatego ogromną rolę odgrywa edukacja użytkowników. **Świadomość zagrożeń i odpowiedzialne korzystanie z urządzeń są jednym z filarów bezpieczeństwa IoT.**

W praktyce oznacza to również wdrażanie podstawowych zasad higieny bezpieczeństwa: wyłączanie nieużywanych funkcji dostępu, zmianę domyślnych haseł, stosowanie silnych haseł oraz, tam gdzie to możliwe, uwierzytelniania dwuskładnikowego. Nie można pominąć monitorowania i ochrony urządzeń IoT. Sprzęt powinien być stale obserwowany, a ruch sieciowy filtrowany przez systemy zabezpieczające, takie jak firewalle. Zabezpieczenia muszą być regularnie weryfikowane i testowane, najlepiej przez specjalistów. Równie ważne są aktualizacje oprogramowania producenci, po wykryciu luk, powinni dostarczać poprawki, a organizacja musi je konsekwentnie wdrażać.

Bezpieczeństwo zaczyna się jeszcze przed zakupem urządzenia. Przed wdrożeniem IoT należy przeanalizować ryzyko, sprawdzić dostępne mechanizmy zabezpieczeń i odpowiedzieć sobie na pytanie, czy dane urządzenie jest rzeczywiście potrzebne. Konieczna jest także weryfikacja producenta jego reputacji, podejścia do bezpieczeństwa oraz tego, jakie dane urządzenie gromadzi i w jaki sposób są one przechowywane, wykorzystywane i udostępniane.

Całość powinna być uzupełniona o regularne audyty bezpieczeństwa, najlepiej prowadzone przez zewnętrznych ekspertów, którzy obiektywnie ocenią poziom ochrony i wskażą obszary do poprawy. Dopełnieniem tego podejścia są fizyczne zabezpieczenia urządzeń, właściwa autoryzacja i identyfikacja, ochrona komunikacji między urządzeniami, bezpieczeństwo chmury oraz spójny, komplementarny system zarządzania bezpieczeństwem IoT.

1. Widoczność i zarządzanie

- Zapewnienie pełnej widoczności wszystkich urządzeń IoT w sieci
- Centralne zarządzanie całą infrastruktur
- Zautomatyzowane rejestrowanie zasobów sprzętowych i programowych

2. Segmentacja sieci

- Wydzielenie osobnego segmentu sieci dla urządzeń IoT
- Odseparowanie IoT od systemów krytycznych i danych wrażliwych
- Odseparowanie IoT od laptopów, komputerów, tabletów i smartfonów firmowych

3. Zabezpieczenie komunikacji

- Stosowanie szyfrowania komunikacji
- Wykorzystanie VPN lub prywatnych APN (jeśli dotyczy)
- Uwierzytelnianie urządzeń IoT
- Zastosowanie WPA2 lub WPA3 w sieciach bezprzewodowych

4. Konfiguracja urządzeń

- Zmiana domyślnych haseł na silne
- Wyłączenie nieużywanych funkcji i interfejsów dostępu
- Włączenie uwierzytelniania dwuskładnikowego (jeśli dostępne)

5. Aktualizacje i utrzymanie

- Regularne aktualizowanie firmware i oprogramowania urządzeń
- Monitorowanie informacji o lukach bezpieczeństwa od producentów

6. Monitorowanie i ochrona

- Stałe monitorowanie pracy urządzeń IoT
- Zastosowanie firewalli i systemów zabezpieczających
- Regularne testowanie i weryfikacja zabezpieczeń

7. Urządzenia użytkowników

- Zabezpieczenie smartfonów i innych urządzeń końcowych użytkowników
- Ograniczenie dostępu IoT z niezabezpieczonych urządzeń
- Edukacja użytkowników w zakresie zagrożeń IoT

8. Etap zakupu i wyboru sprzętu

- Analiza ryzyka przed zakupem urządzenia IoT
- Weryfikacja producenta i jego reputacji w zakresie bezpieczeństwa
- Sprawdzenie, jakie dane są zbierane i jak są przetwarzane

9. Audyty i kontrola

- Regularne audyty bezpieczeństwa
- Współpraca z zewnętrznymi ekspertami ds. cyberbezpieczeństwa

10. Bezpieczeństwo systemowe

- Fizyczne zabezpieczenie urządzeń IoT
- Właściwa autoryzacja i identyfikacja
- Zabezpieczenie komunikacji między urządzeniami
- Zabezpieczenie środowiska chmurowego
- Spójny system zarządzania bezpieczeństwem IoT

Na sam koniec warto wspomnieć o OWASP IoT Top 10, czyli liście dziesięciu najważniejszych aspektów na jakie warto zwrócić uwagę w trakcie budowania, wdrażania i zarządzania systemami IoT.

Warto bowiem pamiętać, że „inteligentne" przedmioty, pozostawione bez właściwej kontroli, mogą stać się niepostrzeżenie wektorem ataku. Nie zawsze zagrożenie przychodzi przez główne bramy i dobrze strzeżone skarbce czasem zaczyna się od drobnych, pozornie nieistotnych elementów. Tak jak mądry władca pilnuje nie tylko murów i bogactw, ale również małych świec tlących się w kątach zamku, tak odpowiedzialne podejście do IoT wymaga dostrzegania potencjalnych zagrożeń tam, gdzie na pierwszy rzut oka wydają się one niegroźne. To właśnie te niewielkie iskry, pozostawione bez nadzoru, najczęściej stają się początkiem pożaru.

Alina Kobyłecka | 12 marca 2026

Sieciówka – luty: Admin Days 2026, NIS2, Wyciek danych, Nowości w Axence SecureTeam®

Dzień dobry, cześć, witajcie! Przed nami kolejny artykuł z cyklu Sieciówki! O czym dziś?

- Admin Days 2026 – zbliżają się wielkimi krokami!
- NIS2 – Prezydent podpisał ustawę KSC/NIS2 i wysłał ją do Trybunału.
- Nowości w Axence SecureTeam®.
- Zarzuty dla 29-latka w sprawie wycieku z Morele.net.
- Webinar Axence SecureTeam®: Jak nasza platforma szkoleniowa wspiera konkurs cyberbezpiecznych wodociągów.

Admin Days – zbliżają się wielkimi krokami!

Wiemy, że dobrze znacie Admin Daysy ale czy w tym roku już się na nie zapisaliście?

To cykl prelekcji i rozmów dla adminów i specjalistów IT, który od 2019 roku pozwala pogadać o tym, co w codziennej pracy naprawdę ważne – od zarządzania infrastrukturą po kwestie bezpieczeństwa i cyberzagrożeń.

W tym roku wracamy online i spotykamy się 21–23 kwietnia! Na scenie pojawią się m.in.: **Marcel Guzenda, Artur Markiewicz, Paula Januszkiewicz, dr Mirosław Gumularz, Agata**

Ślusarek, Adam Lange i wiele innych osób! Możecie liczyć na praktyczne wskazówki, historie z życia wzięte i konkretne rozwiązania dla codziennych problemów IT.

Admin Days są darmowe, ale pamiętajcie – obowiązuje zapis na stronie. Nie przegapcie!

NIS2 – Prezydent podpisał ustawę KSC/NIS2 i wysłał ją do Trybunału

Prezydent Karol Nawrocki podpisał ustawę o **Krajowym Systemie Cyberbezpieczeństwa (KSC)**, która wdraża do polskiego prawa unijną dyrektywę **NIS2**, a następnie skierował ją do Trybunału Konstytucyjnego w ramach kontroli następczej, co oznacza, że część przepisów może ostatecznie zostać uchylona.

Ustawa ma **strategiczne znaczenie dla cyberbezpieczeństwa w Polsce**, rozszerza katalog podmiotów kluczowych i ważnych oraz **wprowadza nowe obowiązki i mechanizmy reagowania na incydenty**, które mają **podnieść odporność sieci i usług krytycznych.**

Pomimo wysłania ustawy do Trybunału, regulacje wejdą w życie po upływie miesiąca od ogłoszenia i już teraz trzeba się szykować na ich wdrażanie; mniej rygorystyczne w skutkach mają być kary za naruszenia, które zaczną obowiązywać dopiero po 2 latach od wejścia w życie.

Z punktu widzenia IT i bezpieczeństwa sieci, nowelizacja KSC jest jedną z najważniejszych zmian prawnych tego roku i warto śledzić jej dalszy bieg w Trybunale Konstytucyjnym.

Przeczytaj więcej w artykułach na naszej stronie:

- Sejm uchwalił nowelizację ustawy o KSC – wdrożenie dyrektywy NIS2 i nowe ramy cyberbezpieczeństwa
- Jakie są najważniejsze zmiany do krajowego systemu cyberbezpieczeństwa?
- Inwentaryzacja zasobów IT w świetle nowelizacji ustawy o KSC.

Nowości w Axence SecureTeam®

Axence SecureTeam® wprowadził właśnie nowości ułatwiające zarządzanie szkoleniami z cyberbezpieczeństwa. Pojawiły się m.in. **nowe opcje filtrowania statystyk, eksport danych do CSV/Excel oraz dedykowane widoki postępów uczestników**, dzięki czemu administratorzy i menedżerowie mogą szybciej oceniać efektywność szkoleń i identyfikować ewentualne luki w wiedzy zespołu.

Przeczytaj więcej.

Zarzuty dla 29-latka w sprawie wycieku z Morele.net

Po kilku latach od głośnego wycieku danych użytkowników sklepu internetowego Morele.net śledczy z Centralnego Biura Zwalczania Cyberprzestępczości **ustalili, kto był odpowiedzialny za włamanie z 2018 roku i przedstawili zarzuty 29-letniemu mężczyźnie.**

Podejrzany usłyszał zarzuty bezprawnego uzyskania i ujawnienia informacji, **przyznał się do winy i złożył obszerne wyjaśnienia** – śledztwo nadzoruje Prokuratura Okręgowa w Krakowie. W tamtym incydencie dane ponad dwóch milionów klientów mogły zostać naruszone, co przez lata

było jednym z największych wycieków w polskim e-commerce. **Ujawnienie sprawcy to ważny sygnał, że nawet dawne cyberataki mogą zostać wyjaśnione dzięki uporczywej pracy służb.**

Przeczytaj więcej.

Webinar Axence SecureTeam®: Jak nasza platforma szkoleniowa wspiera konkurs cyberbezpiecznych wodociągów

Już 5 marca o godzinie 11:00 odbędzie się webinar poświęcony platformie Axence SecureTeam! To platforma, które pozwoli szybko, skutecznie i komfortowo przeszkolić osoby w Twojej firmie. Cyberprzestępcy nie czekają – nie warto więc tracić czasu. Dodatkowo podczas webinaru **wspomnimy także o rozstrzygniętym konkursie grantowym na cyberbezpieczne wodociągi i o tym, jak pozyskane środki można przeznaczyć na skuteczne szkolenia z Axence SecureTeam®.**

Rejestruje się!

Angelika Jastrząb | 2 marca 2026

Redakcja czasopisma:

Redaktor naczelny
dr Mirosław Gumularz

Prowadzący portal
Angelika Jastrząb

Przedstawiciel wydawcy
Robert Posłajko

Kontakt z redakcją:
info@wladcysieci.pl

Wydawca miesięcznika Władcy Sieci

Axence Sp. z o.o. Sp. j.
ul. Na Zjeździe 11,
30-527 Kraków
NIP: 675-139-95-89

Czasopismo wpisane do rejestru dzienników i czasopism prowadzonego przez Sąd Okręgowy w Krakowie pod numerem 1 z dnia 2026-02-10