EUROSOC

CYBERSECURITY MAGAZINE

POWERED BY IBM

KWARTALNIK
OGÓLNOPOLSKI

WYDANIE NR 1

RYZYKO, DOSTAWCY I MONITOROWANIE

PUBLIC PRZEPŁACA ZA MONITOROWANIE
DLA MENEDŻERA

DOBRE PRAKTYKI W KONFIGURACJI AD
DLA INFORMATYKA

ZABEZPIECZENIA A RYZYKO W SZBI
DLA BEZPIECZNIKA

IBM **Security** QRadar

QRadar SIEM

Wiodący na rynku system QRadar SIEM wykorzystuje analitykę sieci oraz zachowań użytkowników, a także rzeczywiste informacje o zagrożeniach, aby dostarczać analitykom bezpieczeństwa dokładniejsze, kontekstowe i priorytetyzowane alerty. Lider rozwiązań SIEM wg analiz Gartnera w 2024 roku.

QRadar SOAR

Niedawno nagrodzony w Red Dot Design Award za interfejs i doświadczenia użytkownika, pomaga organizacjom automatyzować i orkiestracyjnie zarządzać procesami reagowania na incydenty. Zapewnia również, że określone procedury są realizowane w sposób spójny, zoptymalizowany i mierzalny.

IBM Watson AI

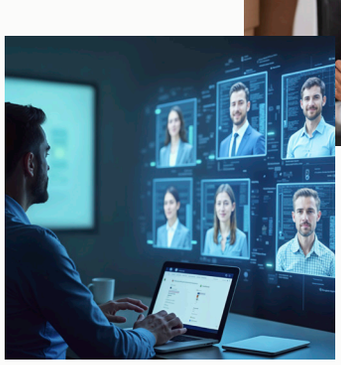
Wspiera analityków bezpieczeństwa poprzez wykorzystanie AI do szybszego wykrywania zagrożeń oraz redukcji liczby fałszywych alarmów. Pozwala analizować ogromne ilości danych w czasie rzeczywistym, łączyć je z globalną wiedzą o zagrożeniach i dostarczać bardziej trafne, kontekstowe rekomendacje.

Oddajemy w Państwa ręce numer naszego magazynu o cyberbezpieczeństwie. Temat bywa poważny, ale podejdziemy do niego po ludzku: konkretnie, bez żargonu i z myślą o tym, by decyzje techniczne realnie pomagały planować budżet, porządkować procesy i zmniejszać ryzyko – nie tylko technologiczne, ale też to, które wynika z codziennej pracy ludzi.

Funkcjonujemy dziś w środowisku, w którym wymagania rosną szybciej niż zasoby. Zmieniane regulacje, presja na ciągłość działania oraz ograniczone budżety sprawiają, że w cyberbezpieczeństwie liczą się przede wszystkim rozsądne priorytety i dobrze uzasadnione inwestycje. Ten numer ma w tym pomóc: pokazujemy, gdzie instytucje i firmy realnie przepłacają, co można uprościć, a co koniecznie trzeba zrobić, by spać spokojniej.

MARCIN MIELZIUK
REDAKTOR PROWADZĄCY

W magazynie



Wydanie nr 1

Wydawca:
EUROSOC Sp. z o.o.

Polska 20
81-533 Gdynia

NIP: 8471607042

Tel.: +48 774 62 89
Mail: hello@eurosoc.eu

Web: eurosoc.eu

Znajdź nas w social media

Kontakt handlowy:

Dominika Smolarczyk
Kierownik Departamentu Sprzedaży
Tel.: +48 530 342 577
Mail: hello@eurosoc.eu

Autorzy:
Grzegorz Bratuś
CEO

Tomasz Browarczyk
DevOps

Łukasz Mitera
Auditor Wiodący

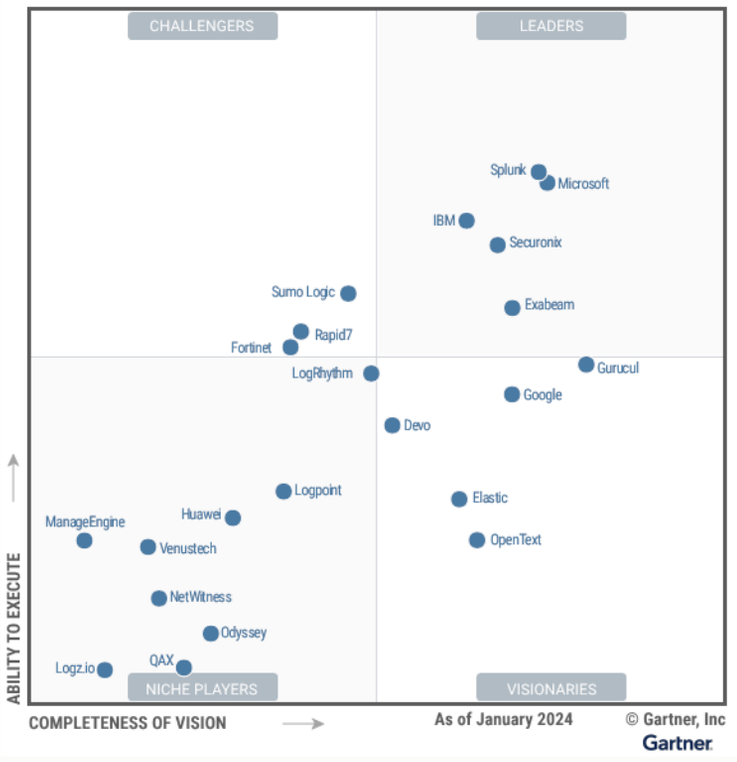
Marcin Mielziuk
Redaktor

Czy **podmioty publiczne przepłacają** za systemy klasy SIEM / SOAR?

W dzisiejszym świecie, gdzie cyberataki stają się coraz częstsze i bardziej wyrafinowane, instytucje publiczne muszą inwestować w zaawansowane narzędzia do ochrony danych. Jednak wiele z nich kończy z wysokimi rachunkami, które nie zawsze przekładają się na realne korzyści. Dlaczego tak się dzieje?

Klucz leży w modelach rozliczeń za systemy SIEM (Security Information and Event Management – zarządzanie informacjami i zdarzeniami bezpieczeństwa) oraz SOAR (Security Orchestration, Automation and Response – orkiestracja, automatyzacja i reakcja na zagrożenia). W tym artykule, opartym na najnowszych analizach rynkowych, wyjaśnimy, jak mądrze wybrać rozwiązanie, unikając pułapek finansowych.

Bazujemy na raporcie Gartner Magic Quadrant for SIEM z 2024 roku (najnowszym dostępnym, gdyż edycja 2025 nie została jeszcze opublikowana), który jest uznanym przewodnikiem po rynku technologii bezpieczeństwa. Gartner, globalna firma analityczna założona w 1979 roku, ocenia dostawców na podstawie ich wizji i zdolności do realizacji projektów, dzieląc ich na kategorie takie jak Liderzy czy Wizjonerzy. To narzędzie pomaga menedżerom podejmować decyzje oparte na faktach, choć pamiętajmy – nie uwzględnia ono bezpośrednio kosztów długoterminowych.

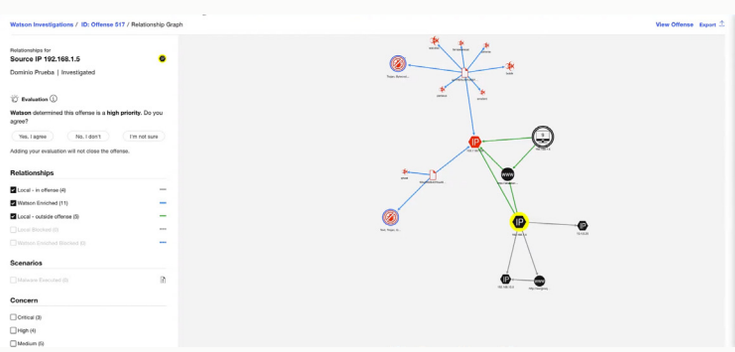


Czym są SIEM i SOAR – i dlaczego warto je łączyć

SIEM to system, który działa jak centralny „mózg" bezpieczeństwa IT. Zbiera on dane (tzw. logi) z różnych urządzeń w organizacji – serwerów, komputerów, sieci - analizuje je w poszukiwaniu podejrzanych wzorców i generuje alerty o potencjalnych zagrożeniach. Wyobraź sobie, że to jak system monitoringu wideo, który nie tylko nagrywa, ale też automatycznie wykrywa intruzów. SOAR to z kolei narzędzie, które automatyzuje reakcję na te alerty. Na przykład, jeśli SIEM zauważy próbę włamania, SOAR może samodzielnie zablokować dostęp, izolować zainfekowany komputer lub powiadomić zespół. Łączenie SIEM z SOAR jest kluczowe, bo samo wykrycie zagrożenia to za mało – szybka reakcja skraca czas neutralizacji ataku z godzin do minut, co jest szczególnie ważne w sektorze publicznym, gdzie opóźnienia mogą zagrozić danym obywateli.

Innowacje w sztucznej inteligencji – jak AI zmienia grę w cyberbezpieczeństwie

Sztuczna inteligencja (AI) przestała być gadżetem - stała się nieodłączną częścią nowoczesnych systemów SIEM i SOAR. AI analizuje ogromne ilości danych szybciej niż człowiek, przewidując ataki na podstawie wzorców zachowań. Na przykład, uczy się „normalnych" działań użytkowników i alarmuje o anomaliach, jak logowanie o nietypowej porze. Liderzy rynku integrują AI, by wspierać operatorów: Microsoft oferuje Security Copilot, który podpowiada zapytania i podsumowuje incydenty; Splunk ma AI Assistant do budowania zapytań; Securonix EON upraszcza triage (sortowanie alertów); Exabeam Copilot pomaga w dochodzeniach. Szczególnie wyróżnia się IBM z Watsonx - to AI oparte na dekadach badań, które zaczęły się od systemów pokonujących mistrzów szachów czy teleturniejów. Watsonx analizuje nie tylko logi, ale też globalne trendy zagrożeń, redukując ręczną pracę o nawet 60 proc. i umożliwiając szybsze decyzje. Dla menedżerów to oznacza mniej błędów ludzkich i efektywniejsze zespoły.



Modele licencjonowania – pułapki kosztowe

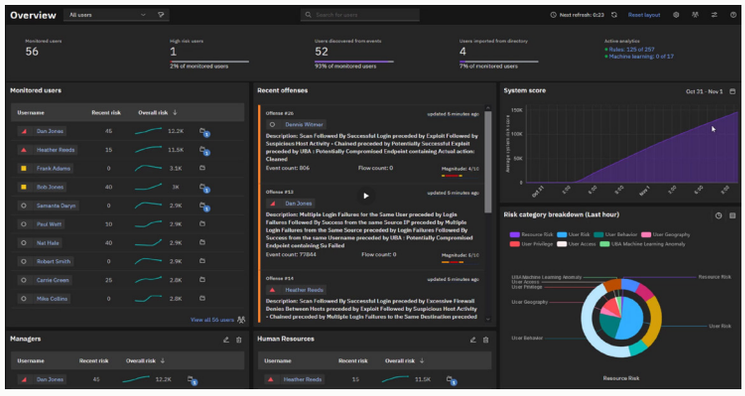
Koszt systemów SIEM/SOAR zależy od modelu rozliczeń, a wybór niewłaściwego może spowodować niekontrolowany wzrost wydatków. Najpopularniejszy to EPS (Events Per Second - zdarzenia na sekundę), gdzie płacisz za tempo przetwarzanych danych - idealny dla stabilnych środowisk, ale ryzykowny, gdyż atak DDoS (masowe zalewanie systemu fałszywymi żądaniami) może zwiększyć rachunek. Podobnie działa model GB/dzień (gigabajty na dzień), dominujący w chmurze. Inne opcje to per-użytkownik lub per-zasób (np. per-serwer), które są bardziej przewidywalne, gdyż zależą od liczby monitorowanych elementów. Subskrypcje (miesięczne lub roczne) zapewniają aktualizacje, ale ich koszt z czasem rośnie. Licencje wieczyste to jednorazowy zakup z opcjonalną opłatą za wsparcie - tańsze długoterminowo. Open source, jak Wazuh, jest bezpłatny licencyjnie, ale wymaga inwestycji w utrzymanie. Wybór zależy od potrzeb: dla sektora publicznego przewidywalność jest kluczowa, by unikać budżetowych niespodzianek.

Liderzy rynku według Gartnera – jak się rozliczają?

Raport Gartnera z 2024 roku wskazuje pięciu Liderów: Microsoft Sentinel, Splunk, IBM QRadar, Securonix i Exabeam. Sentinel (chmurowy) integruje się z ekosystemem Microsoft, używa modelu subskrypcyjnego opartego na wolumenie danych (Commitment Tiers) - szybki we wdrożeniu, ale koszty rosną z danymi. Splunk, oferuje elastyczne modele (GB/dzień lub workload-based) – bogaty w funkcje, ale skomplikowany i relatywnie drogi. Securonix (SaaS) skupia się na AI, rozlicza per-wolumen lub per-użytkownik - nowoczesny, ale zależny od chmury. Exabeam podkreśla analitykę behawioralną, z modelem per-użytkownik niezależnym od danych - przewidywalny dla zmiennych środowisk. IBM QRadar wyróżnia się elastycznością: oferuje subskrypcje, ale też licencje wieczyste (on-premise), w tym model MVS (per-serwer, bez limitu danych). To obniża koszty utrzymania, gdyż pozwala uniknąć rosnących opłat – idealne dla budżetów publicznych.

Źródła wiedzy o zagrożeniach – dlaczego MITRE ATT&CK jest standardem

Systemy SIEM „wiedzą” o atakach dzięki bazom threat intelligence (wywiadu o zagrożeniach) – zbiorom danych o taktykach hakerów. Microsoft czerpie z własnej globalnej sieci; Splunk z Intelligence Management; Securonix z Threat Labs; Exabeam agreguje dane komercyjne i otwarte. IBM X-Force to największa baza – monitoruje miliardy zdarzeń dziennie w 130 krajach, dostarczając kontekstowych informacji. Kluczowy jest framework MITRE ATT&CK, otwarty katalog taktyk ataków, np. „brute force” (próby zgadywania haseł). Wszyscy Liderzy integrują MITRE: mapując alerty do konkretnych technik, ułatwiając analizę i raportowanie. To jak wspólny język dla zespołów – bez niego alerty są chaotyczne, a z nim menedżerowie lepiej rozumieją ryzyka i planują obronę.



Polskie rozwiązania i open source – szanse i ograniczenia

Na polskim rynku działają systemy jak Energy Logserver czy SecureVisio, często oparte na silniku Elasticsearch (lub jego forku OpenSearch) – darmowej technologii do przetwarzania danych. To nakładki na open source, rozszerzające jego funkcje. Porównując do bezpłatnego Wazuh (wykorzystujący obecnie OpenSearch), polskie rozwiązania oferują wsparcie lokalne, ale mogą być droższe bez unikalnych zalet. Open source nie generuje kosztów licencyjnych, ale wymaga głębokiej wiedzy technicznej - np. czytania logów w surowej formie. Są mniej skuteczne niż komercyjne, gdyż brakuje im własnych baz threat intelligence (polegają na publicznych, „hałaśliwych” źródłach, generujących fałszywe alarmy). IBM X-Force przewyższa je skalą. Dodatkowo, open source angażuje finanse inaczej: więcej czasu na obsługę, audyty kodu (traktowane jak systemy na zamówienie w testach penetracyjnych). Mimo to Wazuh jest świetnym agregatorem logów – zbiera dane tanio, spełniając polskie wymogi KRI (Krajowe Ramy Interoperacyjności – przechowywanie logów przez co najmniej 2 lata). Może przesyłać kluczowe alerty do SIEM jak QRadar, tworząc hybrydowy system.

Konkluzja – jak uniknąć przepłacania i zbudować solidną obronę

Podmioty publiczne bardzo często przepłacają, gdyż wiele systemów SIEM opiera się na modelu EPS, gdzie atak DDoS czy wzrost danych potrafi nagle zwiększyć koszty utrzymania, zmuszając czasem do kupna licencji „na zapas”. Subskrypcje dodają dodatkowych presji rosnących opłat operacyjnych.

Wydaje się, że jest jednak efektywne rozwiązanie tego problemu na polskim rynku: IBM, jako jedyny Lider Gartnera, oferuje w QRadar (zarówno SIEM, jak i SOAR), w licencji wieczystej – bez subskrypcji, z niskimi kosztami utrzymania. To jak dobry open source, ale z aktualizacjami producenta i bez konieczności wykonywania dodatkowych audytów aplikacji i jej aktualizacji. Połączenie z Wazuh jako agregatorem, to przewidywalny budżet, zgodność z regulacjami i bezpieczeństwo światowej klasy, w najwyższym standardzie, co potwierdzają rekomendacje firmy Gartner.

EUROSOC

SECURITY AWARENESS

SECURITY OPERATIONS CENTER

BEZPIECZEŃSTWO WSPOMAGANE PRZEZ SYSTEMY AI,
MDR, DLP, OCHRONĘ POCZTY I BUDOWANIE
ŚWIADOMOŚCI UŻYTKOWNIKÓW

Co składa się na cenę usługi typu **Security Operations Center** (SOC)?

W dzisiejszym świecie, gdzie cyberataki mogą sparaliżować działalność firmy w ciągu minut, Security Operations Center (SOC) - czyli centrum operacji bezpieczeństwa - staje się niezbędnym elementem strategii obronnej. Jako menedżer z wieloletnim doświadczeniem, widzę, jak kierownicy często pytają: „Za co właściwie płacimy?".

Ten artykuł rozkłada na czynniki pierwsze koszty usługi SOC, wyjaśniając je w sposób zrozumiały, bez zagłębiania się w techniczne detale. Pamiętajmy: inwestycja w SOC to nie wydatek, lecz ubezpieczenie przed stratami, które mogą sięgać milionów złotych.

Praca w SOC przypomina dyżur w centrum kryzysowym: zespół monitoruje systemy IT organizacji 24 godziny na dobę, 7 dni w tygodniu. Codziennie analitycy przeglądają tysiące sygnałów o potencjalnych zagrożeniach - od podejrzanych logowań po nietypowy ruch w sieci. Ich celem jest szybkie wykrycie ataku, zanim wyrządzi szkodę. Na przykład, jeśli ktoś próbuje wielokrotnie zgadnąć hasło do konta, SOC to zauważy, zbada i zareaguje. To nie jest pasywna obserwacja - to aktywne polowanie na ryzyka, z regularnymi raportami dla zarządu, by menedżerowie wiedzieli, co dzieje się w sieci.

Trzy linie wsparcia – kto i co robi w zespole SOC

SOC działa na trzech poziomach, jak dobrze zorganizowana fabryka: każdy poziom ma swoją rolę, co optymalizuje koszty i efektywność. **Pierwsza linia** (L1) to „strażnicy": młodsi analitycy, którzy filtrują alerty, odrzucając te nieszkodliwe (np. zwykłe aktualizacje systemu). Ich praca to wstępna ocena – eskalują tylko to, co naprawdę podejrzane. To w tym miejscu najlepiej sprawdzają się systemy AI, które zmniejszają ilość pracy ludzkiej, dzięki wytrenowanym modelom AI, które wspomagają pracę specjalistów. **Druga linia** (L2) to „detektywi": doświadczeni specjaliści, którzy głębiej analizują incydenty, łącząc fakty z różnych źródeł i proponują działania, jak zablokowanie dostępu. **Trzecia linia** (L3) to „eksperci": najstarsi w zespole, którzy polują na ukryte zagrożenia, tworzą nowe procedury i prowadzą skomplikowane dochodzenia po atakach. Taka struktura zapewnia najlepszą efektywność kosztową.

Obsługa całodobowa – dlaczego to generuje koszty

Cyberprzestępcy, nie biorą wolnego, często atakują nocą lub w święta, dlatego SOC musi działać non-stop. Aby obsadzić jedno stanowisko 24/7, potrzeba co najmniej 5 osób (full-time equivalents – etatów), biorąc pod uwagę zmiany, urlopy i choroby. To oznacza wyższe pensje za pracę w nocy i święta plus koszty zarządzania zespołem. W praktyce, dla pełnego SOC, mówimy o 10-15 osobach, co stanowi lwią część budżetu – nawet 60-90% ceny usługi.

SIEM i SOAR z AI jako odpowiedź na NIS2

Dużą część kosztów pochłania technologia, zwłaszcza systemy SIEM) oraz SOAR. Licencjonowanie często opiera się na EPS (Events Per Second – liczba zdarzeń na sekundę), co oznacza, że im więcej danych analizujesz, tym drożej. Unijna dyrektywa NIS2 wymaga ciągłego monitorowania IT i szybkiego raportowania incydentów: wstępne ostrzeżenie w 24 godziny, pełny raport w 72 godziny, finałowy w miesiąc. SOC pomaga w tym, analizując incydenty – w tym false positives (fałszywe alarmy, które mogą stanowić 80% alertów). Procedury SOC muszą być częścią firmowej dokumentacji bezpieczeństwa, ale organizacja nadal odpowiada za decyzje biznesowe (np. komunikację z klientami), klasyfikację incydentów, zgłoszenia regulacyjne i wdrożenia napraw (np. łatki w systemach). SOC wykrywa i doradza, ale nie przejmuje wszystkiego.

MDR – rozszerzenie SOC dla pełnej ochrony

Managed Detection and Response (MDR) to ewolucja SOC: nie tylko monitoruje, ale aktywnie poluje na zagrożenia i reaguje (np. izoluje zainfekowane urządzenia). SOC + MDR daje kompleksową obsługę incydentów od A do Z. Najlepsze usługi idą dalej: dodają DLP (ochronę przed wyciekami danych, np. blokując wysyłkę poufnych plików) czy dedykowanego pełnomocnika SZBI (Systemu Zarządzania Bezpieczeństwem Informacji), który nadzoruje procedury, szkolenia i audyty, zapewniając zgodność z normami jak ISO 27001.

Porównanie kosztów – outsourcing vs. własny SOC

W Polsce usługa SOC kosztuje od 8 tys. zł netto miesięcznie do kilkudziesięciu tysięcy, plus jednorazowy onboarding (1-2x miesięczna opłata). **Budowa własnego SOC:** Średnie wynagrodzenia brutto to L1: 10-15 tys. zł/mies., L2: 15-20 tys. zł/mies., L3: 20-30 tys. zł/mies.. Na 24/7 potrzeba min. 5 osób (np. 3x L1, 1x L2, 1x L3) – to ok. 120 tys. zł/mies. na same pensje. Dodając szkolenia (10 tys. zł/os./rok) i technologie (SIEM/SOAR/AI) – rocznie ponad 2 mln zł. **Outsourcing:** 240-600 tys. zł/rok. Różnica? 4-8 razy taniej, bez ryzyka rotacji.

Konkluzja – jak wybrać mądrze

Na cenę SOC składają się ludzie (obsada 24/7), technologia (SIEM/SOAR z EPS) i procesy (zgodność z NIS2). Szukaj usług z SOAR i AI (sztuczną inteligencją, która automatyzuje analizy – cyberprzestępcy też jej używają). Polecam systemy jak IBM QRadar z licencją wieczystą: jednorazowy zakup zapewnia niskie koszty długoterminowe i wysoką jakość. To inwestycja w spokój – tańsza niż skutki ataku.

Analiza ryzyka jako metoda dobierania zabezpieczeń

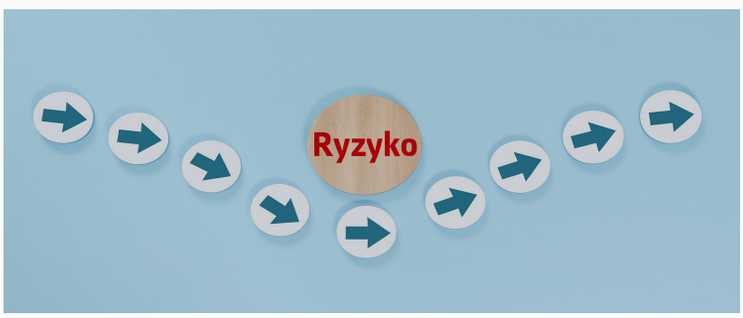
Zarządzanie ryzykiem w bezpieczeństwie informacji stanowi fundament Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), umożliwiając racjonalne decyzje dotyczące zabezpieczeń, alokacji zasobów i priorytetów. Norma ISO/IEC 27001:2022 definiuje wymagania dla SZBI, podkreślając konieczność oceny ryzyka jako kluczowego elementu, podczas gdy ISO/IEC 27005:2022 dostarcza szczegółowych wytycznych do zarządzania ryzykiem, w tym identyfikacji, analizy i traktowania. Uzupełniają to metodyki takie jak NIST SP 800-30 Rev. 1, oferująca przewodnik po ocenach ryzyka z naciskiem na federalne systemy oraz OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), skupiająca się na aktywach krytycznych

Zarządzanie ryzykiem w bezpieczeństwie informacji – wyzwania w praktyce

Budowa bezpieczeństwa informacji w organizacji - zarówno w administracji publicznej, jak i w sektorze prywatnym - zaczyna się od zrozumienia procesów w niej zachodzących oraz elementów, które je tworzą. Nie można chronić tego, czego się nie zna. Dopiero taka wiedza pozwala przejść do kluczowego etapu, jakim jest ocena ryzyka - fundament skutecznego zarządzania bezpieczeństwem, a jednocześnie największe wyzwanie dla wielu instytucji.
Ocena zagrożeń i ich wpływu na funkcjonowanie jednostki stanowi podstawę do podejmowania racjonalnych decyzji dotyczących inwestycji w zabezpieczenia, procedury i rozwiązania techniczne. System Zarządzania Bezpieczeństwem Informacji (SZBI), określony w normie ISO/IEC 27001:2022 i wspierany m.in. przez ISO/IEC 27005 oraz NIST SP 800-30, nakłada obowiązek prowadzenia analizy ryzyka w sposób systematyczny, spójny i udokumentowany. W teorii proces wydaje się prosty, lecz praktyka pokazuje, że wiele podmiotów publicznych napotyka powtarzające się trudności – w efekcie przeprowadzona ocena ryzyka często nie przynosi oczekiwanej wartości i nie wspiera realnie procesu zarządzania bezpieczeństwem.

Błędy w identyfikacji ryzyk

Jednym z najtrudniejszych etapów jest właściwe zidentyfikowanie ryzyk. W wielu jednostkach administracyjnych proces ten prowadzony jest w oderwaniu od faktycznie realizowanych działań i rzeczywistej wartości przetwarzanych informacji. Powstają wówczas listy hipotetycznych zagrożeń, które formalnie wyglądają poprawnie, ale nie odzwierciedlają faktycznych problemów mogących zakłócić działalność organizacji.



Częstym błędem jest również pomijanie ryzyk w obszarach, gdzie istnieją już zabezpieczenia. Takie podejście odbiera możliwość monitorowania skuteczności wdrożonych środków. Równie problematyczne jest niewłaściwe określenie krytyczności procesów – brak priorytetyzacji prowadzi do sytuacji, w której zasoby ochronne kierowane są na mniej istotne obszary, a kluczowe usługi publiczne pozostają narażone.

Braki organizacyjne

Poważnym źródłem ryzyka jest brak jasno określonych i udokumentowanych procedur, szczególnie w obszarach takich jak reagowanie na incydenty, wykonywanie i testowanie kopii zapasowych, zarządzanie zmianami czy realizacja projektów wymagających wiedzy z zakresu cyberbezpieczeństwa. Brak uporządkowanych zasad skutkuje chaosem decyzyjnym w sytuacjach kryzysowych i wydłuża czas reakcji, co bezpośrednio zwiększa skalę strat. W wielu jednostkach dodatkowym problemem jest brak spójności w działaniu zespołów IT - różne praktyki i przyzwyczajenia prowadzą do niespójnych konfiguracji, rozproszenia zasad bezpieczeństwa i trudności w centralnym zarządzaniu infrastrukturą. W konsekwencji rośnie ryzyko podatności oraz maleje efektywność ochrony środowiska IT.

Ryzyka techniczne i dług technologiczny

Jednym z najczęściej ignorowanych obszarów jest tzw. dług technologiczny - odkładanie modernizacji systemów i urządzeń. Przestarzałe rozwiązania częściej zawierają znane podatności, a systemy pozbawione wsparcia producenta (End of Life) stanowią szczególnie poważne zagrożenie. Równie niebezpieczna jest niespójność środowiska – różne wersje i konfiguracje systemów utrudniają monitoring oraz szybkie reagowanie na incydenty. Kolejnym problemem jest prowadzenie oceny ryzyka bez odniesienia do nowoczesnych standardów i rzeczywistych scenariuszy ataków. Brak powiązania z frameworkami, takimi jak MITRE ATT&CK, sprawia, że instytucje koncentrują się na mało realistycznych zagrożeniach, pomijając faktyczne techniki stosowane przez cyberprzestępców. Podobne zaniedbania dotyczą hardeningu – jeśli nie analizuje się podatności możliwych do wyeliminowania prostymi zmianami konfiguracyjnymi, organizacja traci szansę na znaczące wzmocnienie bezpieczeństwa przy minimalnych nakładach.

W rezultacie analiza ryzyka pozostaje ćwiczeniem teoretycznym, bez przełożenia na praktykę.

Ryzyko inherentne i rezydualne

Nieporozumienia budzi często rozróżnienie ryzyka inherentnego i rezydualnego. Ryzyko inherentne pokazuje, jak duże byłoby zagrożenie bez jakichkolwiek zabezpieczeń. Na tym tle można dopiero ocenić sens i skuteczność wprowadzonych środków. Ryzyko rezydualne wskazuje, jakie zagrożenia pozostają mimo istniejących zabezpieczeń. Pomijanie go prowadzi do fałszywego przekonania, że problem został wyeliminowany całkowicie, co w praktyce hamuje dalszy rozwój systemu bezpieczeństwa.

Ryzyka związane z dostawcami

Nie wolno pomijać ryzyk związanych z podmiotami zewnętrznymi. Outsourcing IT, usługi chmurowe czy współpraca z dostawcami są powszechne, jednak często brak oceny konsekwencji ich niedostępności, opóźnień w świadczeniu usług czy incydentów w ich infrastrukturze. Bez takiej analizy nie da się skutecznie planować ciągłości działania, a w kryzysie może się okazać, że krytyczne procesy zależą od podmiotu, którego poziom bezpieczeństwa nigdy nie został zweryfikowany.

Słabości pierwszych analiz ryzyka

W początkowych ocenach ryzyka często popełnia się ten sam błąd – skupienie wyłącznie na zagrożeniach technologicznych, z pominięciem czynników ludzkich i organizacyjnych. Tak jednostronne podejście prowadzi do niepełnej oceny i zaniżenia faktycznego poziomu ryzyka, a w konsekwencji do zniekształconego obrazu bezpieczeństwa organizacji.

Brak szczegółowości i odpowiedzialności

Kolejnym problemem jest nadmierna ogólność opisów zagrożeń. Określenie incydentu jako „atak hakerski" nie wnosi żadnych praktycznych wskazówek dotyczących sposobów ochrony czy minimalizacji skutków. Równie istotnym brakiem jest nieprzypisywanie właścicieli ryzyk do osób odpowiedzialnych za poszczególne procesy biznesowe. Bez jasno określonej odpowiedzialności ocena ryzyka bywa traktowana jako jednorazowa formalność, zamiast jako element ciągłego zarządzania bezpieczeństwem.

Dodatkowo, analizy często prowadzone są wyłącznie przez działy IT, bez zaangażowania pracowników merytorycznych, którzy najlepiej znają znaczenie danych i procesów dla działania urzędu. Brak ich udziału obniża jakość analizy i sprawia, że nie odzwierciedla ona rzeczywistych priorytetów organizacji.

Wnioski

Rzetelna ocena ryzyka nie jest ćwiczeniem formalnym, lecz praktycznym narzędziem, które umożliwia instytucji bezpieczne i przewidywalne działanie. Wymaga powiązania ryzyk z faktycznymi procesami, uwzględnienia zagrożeń technicznych i organizacyjnych oraz regularnej aktualizacji wyników w oparciu o zmieniające się otoczenie. Wykorzystanie sprawdzonych frameworków (np. MITRE ATT&CK) oraz wdrażanie praktyk wzmacniających konfigurację systemów pozwala nadać analizie ryzyka realną wartość. Dzięki temu zarządzanie ryzykiem staje się nie biurokratycznym obowiązkiem, lecz kluczowym elementem zapewniającym ciągłość działania urzędu i bezpieczeństwo danych obywateli.

Terminologia pomocnicza:

Kontekst (context) – zewnętrzne i wewnętrzne uwarunkowania, w których zarządzasz ryzykiem (cele, interesariusze, kryteria, procesy). Bez definiowania kontekstu wyniki oceny ryzyka są zwykle niemiarodajne.

Kryteria ryzyka (risk criteria) – reguły oceny „akceptowalności" ryzyka (skale, progi, zasady ważenia). Oparte na celach, przepisach i apetycie/tolerancji.

Apetyt na ryzyko (risk appetite) – ile i jakiego rodzaju ryzyka organizacja chce podejmować w pogoni za celami; wyznacza ramy dla decyzji i progów.

Tolerancja ryzyka (risk tolerance) – dopuszczalny zakres odchyleń od apetytu/poziomu docelowego; „ile bólu" można znieść zanim trzeba działać.

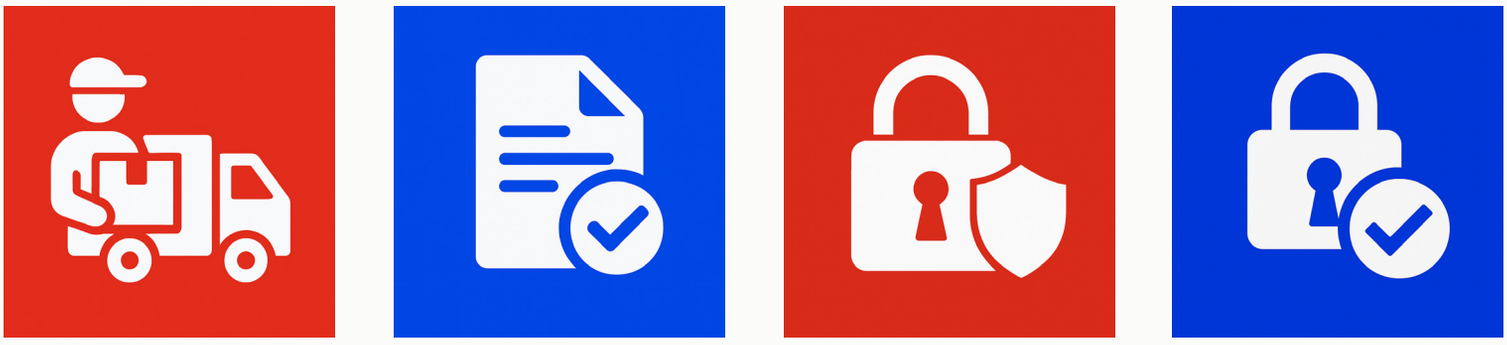
Akceptacja ryzyka – świadoma decyzja o przyjęciu ryzyka rezydualnego po traktowaniu. (ISO/IEC 27005).

Ewaluacja/ocena ryzyka – porównanie poziomów ryzyka do kryteriów w celu priorytetyzacji.

Właściciel ryzyka (risk owner) – osoba/podmiot z odpowiedzialnością i uprawnieniem do zarządzania ryzykiem.

Zasób informacyjny (asset) – to, co ma wartość (dane, systemy, ludzie, usługi) i wymaga ochrony.

Zagrożenie (threat) – potencjalna przyczyna niepożądanego zdarzenia; podatność (vulnerability) – słabość mogąca zostać wykorzystana; skutek/konsekwencja – efekt zdarzenia; prawdopodobieństwo/likelihood – szansa zajścia.



Bezpieczne zarządzanie dostawcami w ramach SZBI

Coraz większa część działalności jednostek publicznych opiera się na technologiach informatycznych dostarczanych z zewnątrz. Oprogramowanie, infrastruktura teleinformatyczna czy systemy wspierające obsługę mieszkańców są dziś najczęściej elementem usług świadczonych przez firmy IT.
Taka współpraca niesie wiele korzyści, ale jednocześnie powoduje, że stabilność i bezpieczeństwo podmiotu publicznego zależą nie tylko od jego własnych działań, lecz także od jakości i rzetelności dostawców.

Aktualne regulacje, m.in. NIS2, RODO oraz ISO 27001, jasno wskazują, że zarządzanie dostawcami musi być procesem uporządkowanym i kontrolowanym. Sama optymalizacja kosztów czy umowy SLA nie wystarczą - kluczowe znaczenie mają wymogi bezpieczeństwa, ciągły nadzór oraz ocena ryzyka. Doświadczenie pokazuje, że brak takiego podejścia staje się jednym z głównych czynników zagrażających zarówno ciągłości funkcjonowania administracji, jak i bezpieczeństwu danych.

Obserwacja funkcjonowania jednostek publicznych pokazuje, że w obszarze zarządzania dostawcami usług IT i ICT pojawia się szereg powtarzających się trudności. Problemy te występują niezależnie od charakteru czy wielkości urzędu – zmienia się jedynie ich natężenie oraz skala. Niezmiennym czynnikiem pozostaje brak jednolitego, systemowego podejścia do współpracy z podmiotami zewnętrznymi, a także niewystarczający nadzór i kontrola nad wykonywaniem powierzonych im obowiązków. W efekcie czego osłabia to bezpieczeństwo organizacji, utrudnia utrzymanie ciągłości działania oraz zwiększa poziom ryzyka w obszarze zarządzania informacją i infrastrukturą krytyczną.

Podstawowym problemem jest brak kompletnej i aktualnej ewidencji dostawców oraz świadczonych przez nich usług i dostarczanych systemów. W praktyce oznacza to, że w wielu jednostkach nie ma jasności, które podmioty odpowiadają za realizację kluczowych procesów, ani które usługi należy traktować jako krytyczne z punktu widzenia ciągłości działania. Taki stan rzeczy utrudnia nie tylko szybkie reagowanie na awarie i incydenty bezpieczeństwa, ale także skuteczne planowanie działań naprawczych, zarządzanie ryzykiem oraz tworzenie realnych planów ciągłości działania. Brak tej wiedzy uniemożliwia również właściwą ocenę, czy dany dostawca spełnia wymagania prawne i regulacyjne, co dodatkowo zwiększa ryzyko operacyjne i prawne.

Istotnym problemem jest niewystarczające uwzględnianie aspektów bezpieczeństwa w umowach zawieranych z dostawcami. Niejednokrotnie akcent kładzie się niemal wyłącznie na cenę, terminy realizacji i ogólne parametry jakości, marginalizując znaczenie bezpieczeństwa informacji oraz stabilności technologicznej. W wielu przypadkach brakuje w nich zapisów dotyczących obowiązku stosowania aktualizacji bezpieczeństwa, mechanizmów szybkiego reagowaniana incydenty, przeprowadzania regularnych testów odporności systemów czy zapewnienia cyklicznego wykonywania kopii zapasowych. W efekcie podmiot traci kontrolę nad poziomem bezpieczeństwa, zdając się całkowicie na dostawcę i nie mając możliwości egzekwowania bardziej rygorystycznych wymagań. W konsekwencji rośnie ryzyko niekontrolowanej przerwy w świadczeniu usług publicznych, utraty danych lub naruszenia obowiązków prawnych.

Kolejnym częstym błędem jest traktowanie umowy z dostawcą jako „zamkniętego tematu”. Podpisanie kontraktu zwykle oznacza ograniczenie relacji do rutynowej realizacji usług, bez prowadzenia systematycznej kontroli, przeglądów SLA czy niezależnych audytów bezpieczeństwa. W praktyce oznacza to, że dostawcy często nie raportują incydentów ani problemów technicznych, a urząd nie ma formalnych mechanizmów, by tego wymagać. Brak nadzoru sprawia, że ryzyka narastają w sposób niezauważalny, a problemy ujawniają się dopiero w momencie poważnej awarii, długotrwałej niedostępności systemu lub naruszenia ochrony danych osobowych. Taka sytuacja utrudnia szybkie podejmowanie działań naprawczych i znacząco obniża poziom kontroli nad środowiskiem informatycznym.

Szczególnie wymagającą kategorią są dostawcy oprogramowania i usług ICT, od których bezpośrednio zależy ciągłość działania systemów urzędu. Brak regularnych aktualizacji, opóźnienia w dostarczaniu poprawek bezpieczeństwa czy zbyt ograniczone wsparcie techniczne prowadzą do powstawania podatności, które mogą zostać wykorzystane przez cyberprzestępców. Problemem pozostaje także vendor lock-in - stan, w którym urząd staje się zależny od jednego dostawcy, a zmiana rozwiązania wymagałaby poniesienia dużych kosztów i wysiłku organizacyjnego. Brak jasnych informacji o podwykonawcach dodatkowo osłabia możliwość pełnej oceny ryzyk w łańcuchu dostaw. W efekcie rośnie nie tylko podatność na ataki, lecz także ryzyko strategiczne związane z utratą kontroli nad kluczowymi usługami i infrastrukturą organizacji.

Wrażliwą kategorię stanowią dostawcy krytyczni - podmioty, od których bezpośrednio zależy ciągłość funkcjonowania całego podmiotu i realizacja jego podstawowych zadań. Niedostępność usług IT może doprowadzić do zatrzymania kluczowych procesów organizacji, przerwania świadczenia usług dla mieszkańców, a nawet utraty danych o znaczeniu krytycznym. Problem pogłębia fakt, że niektórzy dostawcy nie posiadają wdrożonych dojrzałych procesów bezpieczeństwa, działają reaktywnie zamiast proaktywnie lub reagują zbyt wolno na zgłoszenia serwisowe. Zdarza się również, że jakość świadczonych usług utrzymuje się na granicy akceptowalności, a jednostka - z powodu uzależnienia od dostawcy - w rezultacie nie ma możliwości szybkiej zmiany. W rezultacie ryzyko operacyjne i strategiczne dla jednostki samorządowej rośnie w sposób nieproporcjonalny, a zdolność do skutecznego reagowania na incydenty jest poważnie ograniczona.

W obliczu opisanych powyżej problemów niezbędne jest wdrożenie zestawu rozwiązań i mechanizmów, które pozwolą podmiotom publicznym nie tylko uporządkować relacje z dostawcami IT, ale także realnie zwiększyć poziom bezpieczeństwa i odporności na zakłócenia. Dobre praktyki obejmują zarówno aspekty formalne (umowy, procedury), jak i operacyjne (monitoring, audyty, testy). Kluczowe jest też podejście systemowe, które traktuje współpracę z dostawcami jako integralny element systemu zarządzania bezpieczeństwem informacji i planów ciągłości działania.

Dlatego pierwszym krokiem powinno być stworzenie centralnego rejestru dostawców IT wraz z dokładnym opisem usług, systemów oraz procesów, za które odpowiadają. Pozwala to jednoznacznie zidentyfikować podmioty krytyczne dla funkcjonowania urzędu, a także odróżnić je od tych, których znaczenie operacyjne jest ograniczone. Najbardziej przejrzysta klasyfikacja opiera się na podziale dostawców na trzy kategorie:
• **krytycznych** – których niedostępność powoduje całkowity paraliż działania urzędu,
• **istotnych** – których czasowa awaria jest uciążliwa, ale nie blokuje całkowicie procesów,
• **pomocniczych** – których wpływ na działalność urzędu jest niski i łatwy do zastąpienia.

Taki podział umożliwia właściwą priorytetyzację działań, lepsze zarządzanie ryzykiem i racjonalne alokowanie zasobów. Ponadto stanowi fundament do wdrożenia dalszych mechanizmów kontroli, takich jak audyty, testy bezpieczeństwa czy wymagania dotyczące planów ciągłości działania po stronie dostawców.

Dalszym kluczowym elementem jest odpowiednie kształtowanie umów z dostawcami. Dokumenty regulujące współpracę nie mogą ograniczać się wyłącznie do aspektów finansowych czy ogólnych parametrów jakościowych. Powinny wprost zawierać zapisy dotyczące bezpieczeństwa informacji oraz ciągłości działania. W praktyce oznacza to określenie obowiązków dostawcy w zakresie stosowania szyfrowania danych, regularnych aktualizacji i łatek bezpieczeństwa, raportowania incydentów, utrzymywania planów ciągłości działania oraz wdrażania procedur odtwarzania środowiska po awarii. Dobrym rozwiązaniem jest także jednoznaczne wskazanie, że dostawca zobowiązany jest do przestrzegania aktualnych regulacji prawnych. Dzięki temu urząd zyskuje realne narzędzia do egzekwowania wymagań, a współpraca z dostawcą staje się bardziej przejrzysta i przewidywalna.

Podpisanie umowy stanowi jedynie początek współpracy - równie istotny jest stały nadzór nad jej realizacją. Dobrą praktyką jest cykliczne przeglądanie kluczowych parametrów SLA oraz mechanizmów bezpieczeństwa, a także żądanie od dostawców raportów, ankiet kontrolnych czy certyfikatów potwierdzających stosowanie określonych standardów ochrony. W przypadku dostawców krytycznych warto wprost zagwarantować sobie prawo do audytów – zarówno w formie zdalnej, jak i bezpośredniej wizyty w siedzibie dostawcy. Niezbędne jest również zdefiniowanie jasnych i skutecznych procedur eskalacji problemów, tak aby urząd miał możliwość szybkiej reakcji w przypadku powtarzających się uchybień lub poważnych nieprawidłowości.

W odniesieniu do dostawców krytycznych konieczne jest utrzymywanie bliskiej, transparentnej i regularnej współpracy. Powinna ona obejmować m.in. cykliczne spotkania robocze, wspólne testowanie planów awaryjnych, a także systematyczną analizę ryzyka związanego z każdą usługą o znaczeniu kluczowym. Dodatkowo warto wdrożyć mechanizmy redundancji - przykładowo poprzez utrzymywanie zapasowych kopii danych w chmurze, wykorzystywanie drugiego operatora Internetu czy alternatywnych systemów wspierających pracę urzędu. Takie podejście pozwala znacząco ograniczyć ryzyko paraliżu w sytuacji awarii lub niedostępności usług po stronie dostawcy oraz wzmacnia odporność całej organizacji.

W praktyce nie wszystkie relacje z dostawcami przebiegają bez zakłóceń - część współpracy może generować problemy wpływające na ciągłość działania i bezpieczeństwo organizacji. W takich sytuacjach kluczowe znaczenie ma systematyczne dokumentowanie nieprawidłowości oraz ocena ich wpływu na procesy administracyjne. Zebrane informacje stanowią podstawę do prowadzenia konstruktywnych negocjacji w zakresie działań naprawczych, a także do egzekwowania zapisów umownych. W skrajnych przypadkach konieczne może być przygotowanie planu wyjścia, obejmującego analizę rynku i poszukiwanie alternatywnych dostawców. Taka strategia minimalizuje ryzyko uzależnienia się od jednego podmiotu i pozwala uniknąć sytuacji, w której urząd staje się zakładnikiem nieefektywnej lub nierzetelnej współpracy.

Aby skutecznie ograniczać ryzyko związane z dostawcami IT i usług ICT, podmioty publiczne powinny wdrożyć

zestaw praktycznych mechanizmów organizacyjnych i technicznych. Nie są one skomplikowane ani nadmiernie kosztowne, ale wymagają konsekwentnego i systematycznego stosowania. Ich wprowadzenie pozwala uporządkować relacje z kontrahentami, zapewnić większą przejrzystość współpracy i zwiększyć odporność całej organizacji na zakłócenia w łańcuchu dostaw.

Podstawą efektywnego podejścia jest opracowanie polityki zarządzania dostawcami IT. Dokument ten powinien jasno definiować zasady współpracy, role i odpowiedzialności, a także procedury dotyczące wyboru, oceny i bieżącego nadzoru nad kontrahentami. Powinien również określać kryteria klasyfikacji dostawców (np. krytyczni, istotni, pomocniczy) oraz reguły dotyczące eskalacji problemów. Dzięki temu każdy etap współpracy - od momentu zawarcia umowy, poprzez monitorowanie jej realizacji, aż po zakończenie współpracy - przebiega według jednolitych, przejrzystych standardów. Takie podejście ułatwia kontrolę nad relacjami z dostawcami, pozwala ograniczać ryzyka prawne i operacyjne oraz wzmacnia pozycję negocjacyjną urzędu.

Jednym z fundamentalnych elementów skutecznego zarządzania relacjami z kontrahentami IT jest prowadzenie centralnego rejestru dostawców, w którym każdemu podmiotowi przypisana zostaje kategoria wpływu na funkcjonowanie urzędu. Takie uporządkowanie pozwala jasno odróżnić dostawców krytycznych, od których zależy ciągłość kluczowych procesów administracyjnych, od tych, których znaczenie operacyjne jest ograniczone. Dzięki temu można odpowiednio dobierać wymagania bezpieczeństwa, zakres monitorowania oraz mechanizmy nadzoru w zależności od rangi dostawcy. Rejestr staje się także narzędziem wspierającym planowanie ciągłości działania, zarządzanie ryzykiem i podejmowanie decyzji strategicznych w obszarze ICT.

Każda umowa zawierana z dostawcą powinna obligatoryjnie uwzględniać zestaw zapisów dotyczących bezpieczeństwa informacji i ciągłości działania. Do kluczowych wymogów należą m.in.: stosowanie szyfrowania danych, terminowe aktualizacje i instalowanie poprawek bezpieczeństwa, obowiązek raportowania incydentów, posiadanie i testowanie planu ciągłości działania oraz wdrożone procedury odtwarzania systemów po awarii. Umowy powinny także wprost wskazywać na konieczność zgodności działań dostawcy z obowiązującymi regulacjami prawnymi i normami branżowymi. Dzięki temu urząd uzyskuje formalną podstawę do egzekwowania oczekiwanych standardów bezpieczeństwa.

Równie istotnym elementem jest stworzenie systemu bieżącego monitorowania współpracy z dostawcami. Powinien on obejmować regularne przeglądy parametrów SLA, okresowe raporty z zakresu bezpieczeństwa, a w przypadku dostawców krytycznych – możliwość przeprowadzania audytów, zarówno zdalnych, jak i na miejscu. Takie podejście pozwala na weryfikację, czy deklarowane w umowach wymogi są faktycznie realizowane w praktyce, a także umożliwia szybkie wykrywanie nieprawidłowości. Dzięki temu urząd zyskuje realny wpływ na jakość i bezpieczeństwo świadczonych usług, a nie jedynie formalne zapisy na papierze.

Ostatnim, ale niezwykle ważnym elementem, jest przygotowanie planu awaryjnego na wypadek utraty kluczowego dostawcy lub poważnej awarii świadczonych przez niego usług. Powinien on obejmować zidentyfikowanie alternatywnych dostawców, wdrożenie rozwiązań redundantnych (np. dodatkowych kopii danych w chmurze, drugiego operatora telekomunikacyjnego) oraz procedury czasowego przejęcia obsługi przez inne jednostki lub wewnętrzny dział IT. Posiadanie takiego planu stanowi istotny element budowania odporności operacyjnej urzędu, pozwalając ograniczyć skutki sytuacji kryzysowych i zachować ciągłość świadczenia usług publicznych.

Dostawcy IT i usług ICT stali się nieodłącznym elementem funkcjonowania administracji publicznej - w wielu obszarach to właśnie oni zapewniają dostępność systemów, obsługę procesów administracyjnych czy utrzymanie infrastruktury krytycznej podmiotu. W praktyce oznacza to, że pełnią rolę „przedłużenia" urzędu, a więc wszystkie ich niedoskonałości, zaniedbania czy braki w dojrzałości procesów bezpieczeństwa mają bezpośrednie przełożenie na funkcjonowanie organizacji. Każdy błąd po stronie dostawcy – opóźniona reakcja na incydent, brak aktualizacji, niewłaściwa obsługa systemu - staje się realnym ryzykiem dla urzędu i jego mieszkańców.

Z tego względu skuteczne zarządzanie dostawcami IT nie może być traktowane wyłącznie jako kwestia organizacyjna czy formalna. Jest to jeden z kluczowych filarów bezpieczeństwa i ciągłości działania jednostki. Brak nadzoru nad dostawcami oznacza narażenie się nie tylko na cyber incydenty i awarie systemów, lecz także na poważne konsekwencje wizerunkowe. W przypadku administracji publicznej utrata zaufania obywateli jest szczególnie dotkliwa – mieszkańcy oczekują, że urząd będzie działał stabilnie, bezpiecznie i w sposób niezakłócony. Odbudowa zaufania po kryzysie, spowodowanym np. długotrwałą awarią systemu lub wyciekiem danych, bywa procesem długotrwałym i kosztownym.

Doświadczenia wielu podmiotów publicznych pokazują, że skuteczna współpraca z dostawcami IT nie wymaga wdrażania skomplikowanych i kosztownych mechanizmów. Wystarczy konsekwentne stosowanie prostego, uporządkowanego modelu opartego na pięciu krokach:

- **inwentaryzacja** – stworzenie pełnego rejestru dostawców wraz z przypisaniem do nich odpowiednich usług i systemów,
- **klasyfikacja** – podział dostawców według stopnia ich wpływu na działalność urzędu (krytyczni, istotni, pomocniczy),
- **wymagania** – określenie minimalnych standardów bezpieczeństwa, które muszą znaleźć się w każdej umowie, takich jak aktualizacje, szyfrowanie, raportowanie incydentów czy plan ciągłości działania,
- **monitorowanie** – bieżąca kontrola realizacji umów poprzez raportowanie, przeglądy SLA, a w przypadku dostawców krytycznych także audyty bezpieczeństwa,
- **plan awaryjny** – przygotowanie procedur na wypadek utraty kluczowego dostawcy lub awarii, obejmujących alternatywne rozwiązania i redundancję usług.

Stosowanie tego modelu pozwala jednostce na odzyskanie kontroli nad obszarem, który dotychczas bywał traktowany marginalnie, a który w praktyce ma kluczowe znaczenie dla stabilności działania urzędu. Wdrożenie prostych zasad i procedur umożliwia ograniczenie ryzyka technicznego, prawnego i wizerunkowego, a jednocześnie zwiększa odporność całej organizacji na zagrożenia związane z cyfrowym środowiskiem.

Przydatne normy:

- **ISO 9001:2015** - System zarządzania jakością
- **ISO 37000:2021** - Ład organizacyjny
- **ISO 44001:2017** - Zarządzanie relacjami partnerskimi
- **ISO 37500:2014** - Outsourcing – wytyczne
- **ISO 20400:2017** - Zrównoważone zakupy
- **ISO/IEC 27036** (1-4) - Bezpieczeństwo informacji w relacjach z dostawcami

Przydatne standardy:

- **NIST Cybersecurity Framework 2.0** (CSF) - kategoria Supply Chain (GV.SC)
- **NIST SP 800-53 Rev.5** - kontrolki SR (Supply Chain Risk Management)
- **NIST SP 800-161r1** - C-SCRM (Cyber Supply Chain Risk Management)
- **ENISA - Good Practices** for Supply Chain Cybersecurity

Dobre praktyki w zakresie zarządzania tożsamościami w organizacji w ramach AD

W coraz bardziej cyfrowym świecie tożsamość jest nową powierzchnią ataku. Dane użytkowników - szczególnie osobowe, finansowe i medyczne - interesują nie tylko nas, ale i osoby po „ciemnej stronie mocy". Dlatego IAM (Identity & Access Management) powinien być jednym z pierwszych filarów cyberbezpieczeństwa: uwierzytelnia, czyli weryfikuje kim jesteś, autoryzuje, czyli przyznaje do czego masz prawo, oraz monitoruje dostęp - wykrywając nadużycia i wspierając zgodność z przepisami.

Dlatego IAM (Identity & Access Management) powinien być jednym z pierwszych filarów cyberbezpieczeństwa: uwierzytelnia, czyli weryfikuje kim jesteś, autoryzuje, czyli przyznaje do czego masz prawo oraz monitoruje dostęp - wykrywając nadużycia i wspierając zgodność regulacyjną oraz normatywną.

LDAP i Kerberos - fundamenty AD (i gdzie kończą się mity)

Active Directory (AD) to usługa katalogowa systemów Windows, a nie „implementacja LDAP". LDAP jest głównym protokołem dostępu do katalogu AD – to standard IETF służący do łączenia się z katalogiem, wyszukiwania oraz modyfikacji jego zawartości. Operacje obejmują m.in. bind/unbind (uwierzytelnienie), search/compare (zapytania) oraz add/modify/delete (aktualizacje).

Kerberos jest natomiast protokołem uwierzytelniania (SSO) opartym na biletach oraz Centrum Dystrybucji Kluczy (KDC). W Windows stanowi domyślny mechanizm logowania w domenie, wykorzystując kryptografię klucza symetrycznego (np. AES) i obsługując delegację. W praktyce Kerberos weryfikuje tożsamość, a LDAP udostępnia i aktualizuje dane katalogowe.

Bezpieczny LDAP w AD. Zabezpieczaj ruch LDAP przez TLS/LDAPS i włącz LDAP Signing oraz Channel Binding (EPA/CBT), by zapobiegać podszyciom i atakom typu relay. Te ustawienia są przez Microsoft wprost rekomendowane i periodycznie wzmacniane aktualizacjami.

Pięć usług Active Directory – definicje wg Microsoft

AD Domain Services (AD DS) - przechowuje informacje o obiektach w sieci (użytkownicy, komputery itd.) i udostępnia je użytkownikom oraz administratorom; to „serce" domeny, działające na kontrolerach domeny.

AD Certificate Services (AD CS) - rola Windows Server zapewniająca infrastrukturę klucza publicznego (PKI): wystawianie, zarządzanie i unieważnianie certyfikatów do szyfrowania, podpisu i uwierzytelniania (użytkownicy, komputery, urządzenia).

AD Lightweight Directory Services (AD LDS) - elastyczna usługa LDAP directory dla aplikacji, niezależna od infrastruktury AD DS i bez ograniczeń domenowych; na jednym serwerze można uruchamiać wiele instancji z własnymi schematami.

AD Rights Management Services (AD RMS) - technologia ochrony informacji (IRM) do egzekwowania uprawnień wobec dokumentów i poczty (np. blokada drukowania, przekazywania) - ochrona „podąża" za plikiem. Dziś Microsoft zaleca migrację do Azure Rights Management / Microsoft Purview Information Protection.

AD Federation Services (AD FS) - federacja tożsamości i SSO do aplikacji WWW między organizacjami (standardy m.in. WS-Fed, SAML, OpenID Connect/OAuth). Pozwala bezpiecznie współdzielić atrybuty i uprawnienia (claims) poza granicami domeny.

Dobre praktyki IAM w środowisku AD

Model uprawnień i separacja ról

- Stosuj least privilege i grupowe nadawanie dostępu (RBAC). Chroń i regularnie przeglądaj grupy Enterprise Admins, Domain Admins, Administrators.
- Wdroż model dostępu uprzywilejowanego (tiering / Enterprise Access Model) i bezpieczne stacje administracyjne (PAW) - nie administruj z hostów użytkowych. Wymuszaj MFA dla kont uprzywilejowanych.
- Używaj Protected Users dla wybranych kont (bez buforowania poświadczeń, blokada NTLM, wymuszenie Kerberos z nowoczesnym szyfrowaniem).

Konta serwisowe i tożsamości techniczne

- W aplikacjach preferuj gMSA (Group Managed Service Accounts), aby automatyzować rotację haseł i ograniczyć interaktywny logon usług. (Zasada wynikająca z zaleceń Microsoft dot. zarządzania kontami w AD DS).

Uwierzytelnianie i protokoły

- Wymuś LDAP Signing + Channel Binding oraz preferuj LDAPS/StartTLS.
- Wyłącz NTLMv1 i planuj ograniczanie NTLM, preferując Kerberos/AES - aktualne wytyczne twardnienia AD.

Utwardzanie kontrolerów domeny

- Dbaj o fizyczne bezpieczeństwo DC, szyfruj dyski (BitLocker,

TPM), stosuj baseline'y GPO i separację roli wirtualizacji.

Audyt i detekcja

• Włącz zaawansowany audyt logowań Kerberos (m.in. 4768 - TGT, 4769 - TGS) i wysyłaj logi do centralnego kolektora/SIEM przez Windows Event Forwarding (WEF).
• Jeżeli używasz AD FS, włącz jego audytowanie i kieruj dzienniki do SIEM (np. wraz z Usage Analytics/Connect Health)

Ramka: praktyczne minimum wokół LDAP i Kerberos

• LDAP: stosuj TLS (LDAPS), Signing i Channel Binding; ogranicz anonimy; filtruj i paginuj zapytania; monitoruj błędy bind.
• Kerberos: wymuś algorytmy AES (wytyczne twardnienia), pilnuj synchronizacji czasu (NTP), monitoruj anomalie TGT/TGS (4768/4769).

Uwaga red.: Kerberos – jak mityczny Cerber – strzeże „bram" do zasobów; w AD to on odpowiada za bezpieczne SSO, a LDAP „podaje" dane z katalogu.

Rola Active Directory w kontekście systemów SIEM

W kontekście monitorowania infrastruktury przez systemy klasy SIEM Active Directory działa jednocześnie jako „źródło prawdy" o tożsamościach, mapa relacji uprawnień oraz wysoko-czuły sensor zdarzeń, dzięki czemu znacząco skraca czas korelacji, podnosi jakość detekcji i zmniejsza liczbę fałszywych alarmów.

Kontrolery domeny emitują ustandaryzowane logi bezpieczeństwa (m.in. 4624/4625 - logowania udane/nieudane, 4672 - przydział uprawnień uprzywilejowanych, 4648 - logowanie z jawnymi poświadczeniami), logi Kerberos (4768 - TGT, 4769 - TGS, 4771 - błąd pre-auth) oraz NTLM (4776), a także zdarzenia zarządzania kontami i grupami (4720/4722/4725/4726/4740 - tworzenie/aktywacja/dezaktywacja/usunięcie/lockout kont, 4728/4729, 4732/4733, 4756/4757 - dodanie/usunięcie członków odpowiednio w grupach globalnych, lokalnych i uniwersalnych). Włączenie kategorii „Directory Service Changes" daje dodatkowe, bardzo wartościowe telemetrie obiektowe (5136/5137/5139/5141 - modyfikacja/utworzenie/przeniesienie/usunięcie obiektów), które SIEM może wiązać z realnymi ryzykami (np. nieautoryzowana zmiana atrybutu servicePrincipalName, przygotowująca atak Kerberoasting).

AD dostarcza też kontekst atrybutów (OU, grupy, dział, krytyczność zasobu), co pozwala regułom korelacyjnym natychmiast ustalić, czy np. seria 4625 pochodzi z konta serwisowego, zwykłego użytkownika czy z członka Domain Admins i odpowiednio eskalować priorytet incydentu; podobnie modyfikacje grup Domain Admins/Enterprise Admins (np. 4728/4729) są klasycznym wskaźnikiem eskalacji uprawnień. W warstwie transportowej AD ułatwia bezagentowe zbieranie logów poprzez Windows Event Forwarding (WEF) z kontrolerów domeny, serwerów i stacji - centralny kolektor (konfigurowany GPO) dostarcza dane do SIEM bez konieczności utrzymywania złożonej siatki agentów, a ta sama polityka grup może włączyć właściwe podkategorie audytu („Account Logon", „Logon/Logoff", „Account Management", „Directory Service Access/Changes" czy zmiany polityk 4719, modyfikacje domeny 4739) i ich retencję.

W środowiskach, gdzie działają AD CS i AD FS, dzienniki z usług certyfikatów (np. rejestracje/odwołania certyfikatów urządzeń i użytkowników) oraz federacji (wydania tokenów, anomalie SSO) dodatkowo zasilają SIEM sygnałami o nadużyciach tożsamości, niefortunnych konfiguracjach PKI czy nadużyciach w dostępie do aplikacji chmurowych; po stronie DNS serwera w roli DC logi zapytań i aktualizacji dynamicznych pomagają łączyć aktywność sieciową z kontami i hostami AD. Dzięki temu SIEM może skuteczniej wykrywać całe spektrum technik MITRE ATT&CK, od brute force (wzorce 4625/4771), przez pass-the-ticket/hash (nietypowe korelacje 4672 + 4768/4769), DCSync/DCShadow (nietypowe operacje replikacyjne i uprawnienia do Replicating Directory Changes widoczne w 4662/5136), aż po ciche przejęcia kont serwisowych (nienaturalne żądania TGS do wielu SPN w krótkim czasie).

Co ważne, AD pełni też rolę warstwy wzbogacania (enrichment): SIEM zaciąga z katalogu metadane o użytkownikach/urządzeniach i politykach, dzięki czemu profile UEBA budują bazelines zachowań (kto, gdzie i do czego zwykle się loguje), a odstępstwa są wyłapywane szybciej i z większą pewnością; jednocześnie AD i GPO są kanałem dystrybucji konfiguracji telemetrycznych (np. Sysmon na DC/serwerach krytycznych), co ujednolica i „utwardza" podsystem logowania bez manualnych interwencji. W efekcie organizacja otrzymuje spójny, bogaty w kontekst strumień zdarzeń oraz jednolite mechanizmy ich dystrybucji i kontroli - co w praktyce przekłada się na krótszy MTTD/MTTR, prostsze „drille" reakcji, szybsze budowanie reguł detekcyjnych i wyraźne obniżenie kosztu całkowitego utrzymania monitoringu bezpieczeństwa na poziomie całej domeny.

Podsumowanie

Dobrze zaprojektowane Active Directory - z twardym Kerberosem, bezpiecznym LDAP, federacją na AD FS, PKI z AD CS oraz właściwym modelem uprawnień - daje organizacji spójne IAM i wyraźnie przyspiesza wdrożenia detekcyjne (np. SIEM). To nie tylko porządek w tożsamościach - to realne zmniejszenie ryzyka operacyjnego, szybsza reakcja na incydenty i łatwiejsza zgodność.

Checklista redakcyjna (skrót do wdrożenia)

- Przegląd i „odchudzenie" uprawnień grup EA/DA/Administrators; RBAC oparte o grupy.
- PAW i model uprzywilejowania (tiering); MFA dla adminów.
- LDAP Signing + Channel Binding; LDAPS wszędzie, gdzie to możliwe.
- Ogranicz/wyłącz NTLMv1; wymuś AES dla Kerberosa.
- Protected Users dla wrażliwych kont.
- gMSA dla usług i aplikacji; brak interaktywnego logowania.
- Twardnienie i monitoring DC (BitLocker/TPM, baseline'y GPO).
- WEF > SIEM; audyt Kerberos (4768/4769) i AD FS.
- PKI z AD CS na potrzeby 802.1X/TLS/mTLS.
- Jeśli używasz AD RMS - rozważ migrację do Azure RMS/Purview.


EUROSOC
SECURITY AWARENESS