WHITE PAPER

Jak Opracować i Wdrożyć Proces Zarządzania Incydentami w Kontekście Wymogów NIS 2?

NIS2@trecom.pl
+48 600 945 962

Spis treści

Wprowadzenie do NIS 2

KONTEKST

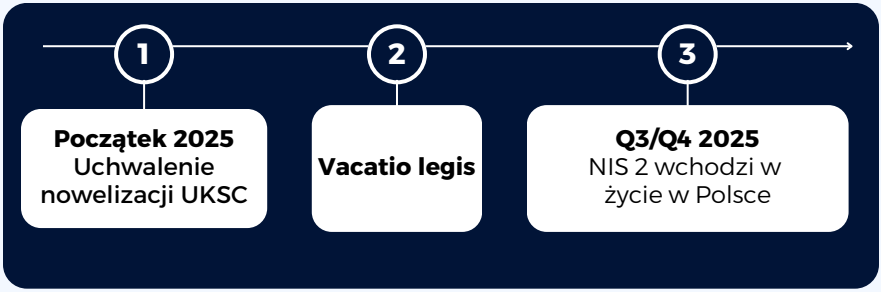
NIS 2 stanowi znaczący krok w poprawie ochrony i odporności przed cyberzagrożeniami organizacji w UE.

W Polsce dyrektywa NIS 2 będzie implementowana poprzez nowelizację ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Choć jeszcze nie wiadomo kiedy zostanie ona przyjęta, w projekcie został przewidziany jednomiesięczny okres vacatio legis.

Na realizację obowiązków wskazanych w ustawie podmioty kluczowe i ważne będą miały czas do jesieni 2025.

Wbrew pozorom nie jest to dużo czasu i w praktyce oznacza, że organizacje już dzisiaj powinny przystąpić do działań mających na celu przygotowanie się do wejścia w życie nowych przepisów.



WYMOGI NIS 2

NIS 2 definiuje elementy w ramach cyberbezpieczeństwa i ryzyka, co do których organizacje muszą opracować wewnętrzne procedury i polityki oraz wdrożyć narzędzia spełniające wymogi określone w dyrektywie.

KLUCZOWE WYMOGI NIS 2

Dyrektywa NIS 2 definiuje szereg wymogów i powinna zostać szczegółowo przeanalizowana przez ekspertów od IT, ryzyka i cyberbezpieczeństwa.

Nasi specjaliści, którzy mają już za sobą projekty wdrożeniowe z wymogów NIS 2, dzielą się swoją wiedzą i przygotowują serię white paper, która pozwoli organizacjom zrozumieć i wdrożyć wszystkie wymogi dyrektywy NIS 2. Na potrzeby tego projektu, zidentyfikowaliśmy wymogi w 10 kluczowych obszarach:

1. **Opracowanie i wdrożenie polityki bezpieczeństwa systemu informacyjnego i metodyki szacowania ryzyka**
2. **Opracowanie i wdrożenie procesu zarządzania incydentami i innych polityk tematycznych**
3. **Opracowanie i wdrożenie planów działania oraz polityk awaryjnych umożliwiających ciągłe i niezakłócone świadczenie usługi**
4. **Opracowanie i wdrożenie dokumentacji określającej bezpieczeństwo łańcucha dostaw produktów, usług i procesów, w tym polityk bezpieczeństwa stron trzecich**
5. **Zapewnienie bezpieczeństwa w procesie nabywania, rozwoju i utrzymania sieci i systemów**
6. **Wprowadzenie polityk i procedur służących ocenie skuteczności środków zarządzania ryzykiem**

7 **Zapewnienie podstawowych praktyk cyberhigieny między innymi poprzez szkolenia w zakresie cyberbezpieczeństwa**

8 **Wprowadzenie polityk i procedur stosowania kryptografii**

9 **Przygotowanie organizacji na zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty**

10 **Monitorowanie bezpieczeństwa systemów teleinformatycznych w trybie ciągłym**

NA JAKIE PYTANIA ODPOWIADA WHITE PAPER?

Przygotowany przez nas white paper ma pomóc przygotować się organizacjom na wymogi NIS 2 dotyczące zarządzania incydentami. White paper jest częścią serii na temat NIS 2, którą będziemy kontynuować w kolejnych tygodniach.

TREŚĆ PORADNIKA

- Czym są incydenty?
- Jak modelowo powinien wyglądać proces zarządzania incydentami?
- W jakich przypadkach warto stworzyć wewnętrzny SOC, a kiedy współpracować z zewnętrznym partnerem?
- Jakie technologie pomagają w procesie zarządzania incydentami?
- Jakie powinny być kluczowe kryteria w wyborze technologii SIEM?

O AUTORACH WHITE PAPER

Aleksander Bronowski
Trecom
Menadżer

Michał Kaczmarek
Trecom SOC
Menadżer

Przemysław Szalwa
Trecom SOC
Analityk

Mirosław Maj
TrecomSEC
Dyrektor

Cyprian Gutkowski
TrecomSEC
Konsultant

Zapraszamy do lektury

Incydenty cyberbezpieczeństwa

DEFINICJA

Rozważania o wdrożeniu narzędzi i polityk do zarządzania incydentami powinno się zacząć od zdefiniowania pojęcia incydentu.

Incydenty to efekt zdarzenia lub serii zdarzeń naruszających poufność i dostępność danych w systemach IT. Wspomniane zdarzenia wpływają na zakłócenie działania organizacji lub znacząco podnoszą prawdopodobieństwo wpłynięcia na zakłócenie działania organizacji.

Z kolei zdarzenia to sytuacja, w której stan systemu IT wskazuje na możliwe naruszenie polityki bezpieczeństwa, awarię zabezpieczeń lub nieznaną wcześniej sytuację, która może być istotna z punktu widzenia cyberbezpieczeństwa.

Zgodnie z definicją znowelizowanej ustawy o KSC incydentem jest zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych

CO MOŻE WYWOŁAĆ INCYDENT?

Istnieje wiele czynników wpływających na wystąpienie incydentu cyberbezpieczeństwa. Do przykładowych czynników należą:

- Ataki zewnętrzne (np. malware, phishing czy DDoS)
- Nieautoryzowany dostęp do systemów informacyjnych i aplikacji
- Naruszenia danych
- Błędy na warstwie programowaniowej

PRZYKŁADY ATAKÓW

Phishing
Atak polegający na pozyskiwaniu poufnych informacji od użytkowników poprzez podszywanie się pod zaufane instytucje, takie jak banki.

Distributed Denial of Service (DDoS)
Atak, w którym serwery lub urządzenia, często przejęte oraz skoordynowane przez botnet, nadmiernie obciążają infrastrukturę sieciową lub serwery, uniemożliwiając dostęp dla użytkowników.

Ataki na aplikacje internetowe
Rodzaj cyberataków, które są ukierunkowane na wykorzystanie luk w zabezpieczeniach aplikacji internetowych w celu uzyskania nieautoryzowanego dostępu lub wykonania szkodliwych działań.

Nieuprawniony dostęp
Ataki polegające na uzyskaniu nieuprawnionego dostępu do systemu lub sieci poprzez wykorzystanie luk w zabezpieczeniach czy obejście procesów uwierzytelniania. Obejmują one szeroki zakres różnych typów ataków, między innymi kradzież lub naruszenie danych.

Atak wewnętrzny
Sytuacja, w której osoba mająca legalny dostęp do systemu lub zasobów organizacji celowo lub nieumyślnie narusza bezpieczeństwo lub prywatność tych zasobów.

Atak APT
Atak zazwyczaj prowadzony przez dobrze zorganizowane grupy z dużymi zasobami i zaawansowaną wiedzą techniczną.

Trzy filary obsługi incydentu

DEFINICJA

Efektywne zarządzanie incydentami w ramach wymogów NIS 2 powinno opierać się na trzech elementach:

1. WDROŻENIE PROCESU ZARZĄDZANIA INCYDENTAMI

Zdefiniowanie procesu zarządzania incydentami, czyli systemowego podejścia uwzględniającego zbieranie incydentów, analizowanie i reagowanie na incydenty oraz eliminację zagrożeń czy przeprowadzenie działań po wystąpieniu incydentu.

KLUCZOWE PYTANIA

- Czy masz dostęp do informacji o cyberzagrożeniach i podatnościach?
- Czy posiadasz szczegółowy plan powstrzymywania ataku oparty o oceny i analizy ryzyka?
- Czy raportujesz incydenty do kluczowych organów w ramach organizacji oraz zewnętrznych instytucji, takich jak CSIRT?
- Czy prowadzisz działania wspierające poprawę świadomości o zagrożeniach?

2. SELEKCJA NARZĘDZI

Proces obsługi incydentu wymaga wdrożenia technologii, w tym narzędzi klasy SIEM oraz SOAR wspierających zbieranie danych z różnych źródeł, analizę oraz reakcję na incydenty.

Obszar technologii jest bardzo indywidualnym zagadnieniem natomiast istnieje kilka kluczowych pytań, które pomogą w wyborze nowych oraz walidacji obecnie używanych.

KLUCZOWE PYTANIA

- Czy posiadasz narzędzie, które agreguje logi ze wszystkich środowisk, w tym krytycznych (np. sieci, systemów IT, IoT czy OT) w jednym miejscu umożliwiając ich korelację i efektywną analizę?
- Czy posiadasz technologie, które gwarantują analizę zdarzeń w czasie rzeczywistym oraz automatyzację procesu zarządzania incydentami (np. SOAR)?

3. STWORZENIE ZESPOŁU DO ZARZĄDZANIA INCYDENTAMI

Stworzenie zespołu, który będzie posiadał zdefiniowane obowiązki i role związane z procesem zarządzania incydentami lub zlecenie zarządzania procesem obsługi incydentów zewnętrznemu partnerowi.

?

KLUCZOWE PYTANIA

- Czy Twój zespół zajmujący się zarządzaniem incydentami posiada kompleksowe kompetencje oraz role w zbieraniu, analizie, raportowaniu i reagowaniu na incydenty?
- Czy Twój zewnętrzny partner zajmujący się zarządzaniem incydentami w Twojej organizacji pokrywa pełen “incident response framework”?

Procedura reagowania na incydenty cyberbezpieczeństwa

STANDARD NIST

Istnieje wiele gotowych procedur reagowania na incydenty cyberbezpieczeństwa definiowanych przez różnego rodzaju organizacje i ekspertów. W tym white paper skupimy się na standardzie oferowanym przez **National Institute of Standards and Technology (NIST).**

NIST to amerykańska organizacja rządowa, która opracowuje standardy w wielu dziedzinach technicznych. Jest ona autorem najczęściej stosowanego standardu reagowania na incydenty.

W 2012 r. organizacja wydała przewodnik postępowania w przypadku incydentów związanych z bezpieczeństwem komputerowym. Proces ten obejmuje:

- Identyfikację czy dane zdarzenie ma charakter szkodliwy dla organizacji
- Podjęcie działań w celu szybkiego opanowania i zminimalizowania ewentualnych szkód
- Wyeliminowanie zagrożenia oraz wyciągnięcie wniosków z incydentu w celu usprawnienia procesu w przyszłości

ETAP I: PRZYGOTOWANIE

Etap przygotowania koncentruje się na wdrożeniu polityk i funkcji reagowania na incydenty oraz na zapobieganiu incydentom cyberbezpieczeństwa.

Etap ten kieruje swoją uwagę na cykliczną ocenę ryzyka zasobów oraz działania mające na celu zmniejszenie luk w zabezpieczeniach.

Przygotowanie obejmuje również działania mające na celu edukację pracowników oraz poszerzanie ich świadomości o cyberbezpieczeństwie. NIST sugeruje również wdrożenie szeregu narzędzi z wyprzedzeniem, aby być gotowym do analizy, izolacji i reagowania na incydent.

Jako Trecom oferujemy m.in. usługę modelowania zagrożeń dla aktywów, która może okazać się niezwykle przydatna na etapie przygotowania.

NARZĘDZIA

Pomocne na przekroju wszystkich etapów mogą okazać się narzędzia klasy SIEM czy SOAR mające za zadanie gromadzenie oraz korelację danych z różnych źródeł oraz automatyzację reakcji. Do takich danych należą logi systemowe i sieciowe, zdarzenia z dzienników systemowych czy alerty z narzędzi monitorowania.

Innym przykładem wspierającego narzędzia jest zapora sieciowa (sprzętowa bądź programowaniowa), która na samym wstępie zweryfikuje oraz zablokuje potencjalne zagrożenie.

NARZĘDZIA

Kolejnym przykładem ważnego narzędzia są rozwiązania EDR (ang. Endpoint Detection and Response), które monitorują, wykrywają oraz reagują na zagrożenia w czasie rzeczywistym na poziomie urządzeń końcowych (endpointów). W procesie przygotowania pomocne mogą okazać się również rozwiązania IDS (ang. Intrusion Detection System) i IPS (ang. Intrusion Prevention System).

IDS jest narzędziem przeznaczonym do wykrywania nieautoryzowanego dostępu, ataków lub niebezpiecznych zdarzeń w sieci poprzez analizę ruchu sieciowego lub logów. IPS poza wykrywaniem ataków posiada również zdolności do aktywnego blokowania lub zatrzymywania podejrzanej aktywności.

ETAP II: DETEKCJA I ANALIZA

Drugim krokiem w procesie reagowania na incydenty jest ustalenie czy zdarzenie, które miało miejsce jest incydentem oraz ocena istotności zdarzenia i jego typu. Składa się na to m.in.:

DETEKCJA I ANALIZA

- Identyfikacja sygnałów i oznak incydentu. Sygnał jest potencjalną przesłanką świadczącą o tym, że incydent ma się wkrótce wydarzyć. Oznaka natomiast informuje, że podejrzana aktywność już ma miejsce w środowisku.
- W kolejnym kroku ważne jest sklasyfikowanie aktywności. Polega to na oszacowaniu czy zebrane dane wskazują na incydent bezpieczeństwa, czy na fałszywy alarm.

DETEKCJA I ANALIZA

- Po sklasyfikowaniu zdarzenia jako incydent następuje udokumentowanie wszystkich faktów na temat danego wystąpienia.
- Następnie incydenty powinny zostać sklasyfikowane na podstawie wpływu na działalność organizacji, poufności informacji oraz tego jak długo będzie trwało przywrócenie pełnej sprawności operacyjnej.

ETAP III: POWSTRZYMANIE I LIKWIDACJA

Na tym etapie podejmowane są decyzje mające na celu najefektywniejsze usunięcie zagrożenia. Zespół reagowania na incydenty powinien mieć szczegółowy plan powstrzymywania dla każdego rodzaju ataku.

Pierwszym zadaniem powinno być odizolowanie hostów dotkniętych atakiem. Dopiero po upewnieniu się, że rozprzestrzenianie się incydentu zostało ograniczone do minimum, zespół reagowania przechodzi do usunięcia zagrożenia.

Obejmuje to usuwanie zarówno aktywnych, jak i pasywnych składników ataku. Dopiero po upewnieniu się, że organizacja jest w pełni zabezpieczona, zespół może przejść do przywracania pełnej sprawności.

Etap odzyskiwania i przywracania organizacji do normalnego funkcjonowania jest szeroki i może obejmować wgranie aktualizacji bezpieczeństwa, weryfikację reguł bezpieczeństwa zapory sieciowej, przywracanie systemów z kopii zapasowych czy poprawę zabezpieczeń stacji roboczych i kont użytkowników.

ETAP IV: DZIAŁANIA PO INCYDENCIE

Często pomijanym krokiem po uporaniu się z zagrożeniem jest wyciągnięcie wniosków z danej sytuacji. NIST wskazuje ten krok jako jeden z najważniejszych w całej procedurze.

Każdy zespół reagowania powinien stale poszerzać swoją wiedzę i spotykać się po incydencie w celu wyciągnięcia wniosków, które pomogą zabezpieczyć organizację przed ponownymi atakami. Kluczowym elementem takiego spotkania powinno być znalezienie odpowiedzi na następujące pytania:

KLUCZOWE PYTANIA

- **Co dokładnie się wydarzyło i w jakim czasie?**
- **Jak dobrze poradzono sobie z incydentem?**
- **Czy uprzednio przygotowane procedury zadziałały poprawnie?**
- **Czy cokolwiek na co zespół miał wpływ przeszkodziło w przywróceniu sprawności organizacji?**
- **Co można zrobić lepiej w przypadku ponownego wystąpienia incydentu?**
- **Czy pominięto jakieś oznaki, które umożliwiłyby wcześniejsze wykrycie incydentu?**

ETAP IV: DZIAŁANIA PO INCYDENCIE

Ostatecznym działaniem powinno być przygotowanie raportu podsumowującego incydent. Raport ten może być wykorzystywany do celów wewnętrznych organizacji, ale służy również jako informacja o incydencie dla podmiotów zewnętrznych, takich jak CSIRT.

Na co zwrócić uwagę przy wyborze narzędzi?

JAKIE NARZĘDZIA WYBRAĆ?

Wybór narzędzi powinien zostać poprzedzony dogłębną analizą indywidualnych potrzeb organizacji oraz możliwości integracji nowego rozwiązania do obecnie posiadanych narzędzi i procesów.

Dzięki tym informacjom, zespoły odpowiedzialne za cyberbezpieczeństwo są w stanie wybrać najbardziej pasujące narzędzia, które zapewnią efektywną ochronę.

NIS 2 nie definiuje konkretnych technologii umożliwiających spełnienie wymogu zarządzania incydentami. W praktyce spełnienie wymogu może odbyć się na wiele sposobów np. poprzez połączenie komplementarnych technologii (np. kilku grup rozwiązań jak zapory sieciowe, EDR, SIEM czy SOAR) lub wdrożenie jednej skonsolidowanej platformy (oferującej połączone zdolności SIEM, SOAR czy XDR).

Kluczowym wzywaniem w doborze narzędzi jest minimalizacja ryzyka związanego z lukami informacyjnymi - np. braku posiadania skonsolidowanej analityki logów z wszystkich potencjalnych wektorów ataku. Wdrożone narzędzia muszą gwarantować dane telemetryczne, metadane, dane sieciowe oraz dane z unikalnych środowisk (jak OT czy IoT).

Jako że na rynku istnieje wiele narzędzi, które integrują grupy produktów w ramach jednej platformy lub skupiają się analizie danych z konkretnych środowisk, rekomendujemy szczegółową analizę rozważanych rozwiązań w ramach matrycy zdolności.

NARZĘDZIA SIEM I SOAR

Narzędzia klasy SIEM i SOAR stają się dzisiaj standardem w wspomaganiu procesu obsługi incydentu. Jednym z czynników, który spowodował popularyzację SIEM jest możliwość konsolidacji informacji z różnych źródeł, w tym logów, danych z firewalli czy innych narzędzi.

Ponadto dostawcy rozwiązań SIEM oferują produkty wspierające automatyzację reakcji na incydenty oraz analizy behawioralne dzięki produktom SOAR czy UEBA.

Wspomniane czynniki podnoszę efektywność procesu zarządzania incydentami dzięki automatyzacji oraz konsolidacji.

Efektywność powinna być kluczowym kryterium w ocenie narzędzi jako, że w przypadku dużej liczby incydentów eksperci nie są w stanie reagować na krytyczne incydenty w wymaganym czasie.

KLUCZOWE KRYTERIA W DOBORZE TECHNOLOGII SIEM I SOAR

1. **Automatyzacja**
2. **Dostęp do analityki**
3. **Skalowalność**
4. **Konsolidacja danych**
5. **Intuicyjność i łatwość wdrożenia**

1

AUTOMATYZACJA

W związku z ilością alertów oraz złożonością procesu zarządzania bezpieczeństwem kluczowe jest zrozumienie kompetencji wspierających automatyzację.

Istnieje wiele funkcjonalności, które umożliwiają automatyzację zarządzania incydentami. Do kluczowych należą:

- **Posiadanie zdefiniowanych zastosowań (ang. use casów) czy akcji, które automatyzują powtarzalne i czasochłonne zadania.**
- **Scenariusze (ang. playbooks) czyli zdefiniowane standardowe procedury dla reagowania na incydenty.**
- **Posiadanie centralnej konsoli, ktora integruje dane z wszystkich źródeł.**
- **Integracje z zewnętrznymi rozwiązaniami oraz komercyjnymi bazami (np. do cyber threat intelligence).**

2

DOSTĘP DO ANALITYKI

Kolejnym ważnym elementem jest analiza w czasie rzeczywistym umożliwiająca wykrywanie i ustalanie priorytetów zdarzeń i działań.

SIEM powinien posiadać rozbudowane zdolności analityczne, które umożliwiają przeprowadzenie wielu niestandardowych analiz.

SIEM powinien również posiadać szerokie możliwości w tworzeniu spersonalizowanych raportów czy grafik.

3 SKALOWALNOŚĆ

Rozwiązania SIEM powinny bez większych problemów skalować się wraz z rozwojem organizacji. Licencjonowanie narzędzi powinno opierać się o jasno określone parametry (np. liczbę adresów IP).

4 KONSOLIDACJA DANYCH

Rozwiązania SIEM powinny zbierać i zarządzać danymi ze wszystkich dostępnych źródeł, w tym zasobów w chmurze, danych sieciowych, danych z zewnętrznych urządzeń czy różnych środowisk (jak IoT czy OT).

SIEM powinien gwarantować odpowiednie zasoby do przechowywania danych, jak również obsługiwać wymagane typy plików (jak np. CSV czy JSON).

5 INTUICYJNOŚĆ I ŁATWOŚĆ WDROŻENIA

SIEM powinien zapewniać łatwy do zrozumienia i przyjazny dla użytkownika interfejs zapewniający kluczowe informacje dla ekspertów. Dostawcy technologii powinni również zapewniać odpowiednią dokumentację i materiały wspierające wdrażanie i konfigurację rozwiązania.

Jak stworzyć zespół do zarządzania incydentami?

SECURITY OPERATION CENTER (SOC)

Systemowe zarządzanie incydentami wymaga stworzenie dedykowanego zespołu, który będzie obsługiwał narzędzia oraz wprowadzi polityki umożliwiające:

- **Zbieranie, analizę i raportowanie incydentów w ramach, jak i na zewnątrz organizacji**
- **Eliminację zagrożeń**
- **Prowadzenie dodatkowych operacji w ramach cyberbezpieczeństwa**

Chcąc podejść systemowo do zarządzania incydentami organizacje decydują się na stworzenie zespołów Security Operation Center (SOC), które tworzą lokalne centrum zarządzania cyberbezpieczeństwem.

Skład oraz wielkość zespołu uzależniona jest od konkretnych potrzeb organizacji natomiast typowy zespół SOC składa się z trzech linii.

LINIA I

Eksperci pierwszej linii odpowiedzialni są za zbieranie nieprzetworzonych danych oraz za pierwszą reakcję na nowy alert.

W tym przypadku eksperci muszą określić krytyczność alertów i wzbogacić je o odpowiednie dane i kontekst organizacyjny.

Przy każdym alercie specjalista identyfikuje zasadność alertu i sprawdza, czy nie mamy do czynienia z fałszywym alarmem (co jest jednym z kluczowych wyzwań współczesnych zespołów SOC).

LINIA II

Druga linia odpowiada za analizę incydentów cyberbezpieczeństwa o wyższym priorytecie, które zostały eskalowane przez specjalistów z linii I.

Eksperci tej linii przeprowadzają bardziej dogłębną ocenę przez co muszą rozumieć zakres ataku i być świadomi systemów, które zostały dotknięte.

Druga linia odpowiada również za powstrzymanie oraz ograniczenie zagrożeń.

LINIA III

Analitycy z linii III są najbardziej doświadczoną kadrą w SOC i zajmują się najbardziej krytycznymi incydentami, które zostały do nich eskalowane przez specjalistów linii II.

Dodatkowe kompetencje linii III to ocena podatności czy przeprowadzenie testów penetracyjnych.

Najbardziej doświadczony element zespołu SOC rekomenduje również działania, które mają optymalizować funkcjonowanie SOC, w tym m.in. sugeruje aktualizacje lub zmiany wdrożonych narzędzi.

POZOSTAŁE ZAGADNIENIA

W zależności od indywidualnych potrzeb zespół SOC może zostać wzbogacony o dodatkowe kompetencje jak np. cyber threat intelligence czy threat hunting.

W jakich przypadkach tworzyć wewnętrzny zespół SOC?

WYZWANIA W TWORZENIU SOC

Stworzenie wewnętrznego zespołu SOC może okazać się niezwykle skomplikowane dla wielu organizacji.

KLUCZOWE WYZWANIA

- **Znaczące inwestycje finansowe (koszty narzędzi, zespołu oraz pozostałe koszty, w tym koszty rekrutacji i szkoleń).**
- **Podaż ekspertów cyberbezpieczeństwa na polskim rynku nie pokrywa się z popytem firm.**
- **Stworzenie wewnętrznego SOC wymaga znaczącej inwestycji czasowej, w tym selekcji i integracji narzędzi, tworzenia procesów czy budowania świadomości wewnątrz firmy.**

ROZWIĄZANIE WYZWANIA

Jednym z sposobów na zaadresowanie wspomnianych problemów jest współpraca z zewnętrznym dostawcą usług SOC.

Firmy IT w ramach usługi zarządzanej zapewniają stworzenie dedykowanego centrum bezpieczeństwa opartego na narzędziach, politykach, procedurach oraz ekspertach zintegrowanych z wybranym środowiskiem.

Takie rozwiązanie pozwala na ograniczenie inwestycji czasowych oraz finansowych w cyberbezpieczeństwo oraz pozwala na skorzystanie z unikalnej wiedzy zewnętrznych ekspertów.

WEWNĘTRZNY VS ZEWNĘTRZNY SOC

Poza zarządzaniem obszarem incydentów oraz wspierających kompetencji (jak cyber threat intelligence) zewnętrzny SOC może kompleksowo rekomendować zmiany w organizacji mające za zadanie poprawę skuteczności cyberbezpieczeństwa oraz zarządzania ryzykiem. Zewnętrzny SOC rozwiązuje kluczowy problem rynku cyberbezpieczeństwa związany z brakiem wystarczającej liczby specjalistów.

Pozostaje pytanie od czego uzależnić decyzję o skorzystaniu z zewnętrznego SOC. Nie ma idealnych rozwiązań pasujących do każdej organizacji natomiast warto wspomnieć o największych przewagach wewnętrznych działów SOC.

Wewnętrzne zespoły mają nieograniczone możliwość dostosowania narzędzi czy polityk. Drugą kluczową zaletą zbudowania wewnętrznego zespołu jest możliwości unikalnego zaznajomienia się z systemami, architekturą oraz potrzebami organizacji.

CZY ZEWNĘTRZNY SOC MOŻE SPEŁNIĆ WYMOGI MOJEJ ORGANIZACJI?

Najczęściej wewnętrzne zespoły SOC tworzone są na potrzeby organizacji, które zarządzają dużą liczbą wrażliwych danych oraz oferują krytyczne i regulowane usługi (np. największe banki, firmy telekomunikacyjne czy instytucje publiczne).

Nie oznacza to oczywiście, że zewnętrzni dostawcy z założenia ustępują jakością świadczonych usług. W praktyce zewnętrzni dostawcy posiadają często unikalne know-how, zrozumienie narzędzi, dojrzałe procesy, certyfikacje i są bardzo doceniani na wielu obszarach.

Wybór między wewnętrznym, a zewnętrznym zespołem SOC to przede wszystkim kwestia preferencji oraz odpowiedź na pytanie czy wybrany (zewnętrzny) SOC może spełnić unikalne wymogi organizacji.

Na co zwrócić uwagę przy wyborze zewnętrznych SOC?

CZYNNIK FINANSOWY

Dzięki konsolidacji wydatków zewnętrzny SOC okazuje się być często najbardziej efektywnym kosztowo rozwiązaniem. Stworzenie wewnętrznego SOC to koszt ekspertów, narzędzi, dostępu do baz danych oraz suma wielu pozostałych wydatków (np. kosztów rekrutacji czy szkoleń).

POGLĄDOWE PORÓWNANIE KOSZTÓW MIĘDZY WEWNĘTRZNYM SOC, A ZEWNĘTRZNĄ USŁUGĄ SOC

W większości przypadków wewnętrzny SOC **jest zdecydowanie droższy od zewnętrznego zespołu SOC.**

Mimo przewag finansowych, najważniejszym czynnikiem, które skłania organizacje do współpracy z zewnętrznym dostawcą jest brak wystarczającej liczby ekspertów.

JAK OCENIAĆ PARTNERÓW OFERUJĄCYCH USŁUGI SOC?

Przy wyborze zewnętrznej usługi SOC kluczowe jest zrozumienie zakresu oferowanych usług i procesów (w tym przede wszystkim czy partner oferuje usługi eliminacji zagrożenia).

Część partnerów oferuje usługę SOC opierającą się na detekcji i analizie zagrożeń bez odpowiednich procesów likwidacji zagrożenia. Ten typ usługi znacząco ogranicza efektywność cyberbezpieczeństwa.

Organizacje decydując się na współprace z zewnętrznym partnerem powinny w pierwszej kolejności zapytać o zakres usług, w tym przede wszystkim posiadanie zdolności reakcji i eliminacji zagrożeń najlepiej połączonych z rekomendacjami oraz raportowaniem (czyli pełne spełnienie "incident response framework").

Kolejnym kluczowym elementem jest oferowanie usług wspierających podstawowe kompetencje SOC.

Kompetencje w zakresie threat hunting, cyber threat intelligence, testach penetracyjnych, analizie malware, analizie forensic czy zarządzaniu podatnościami znacząco poprawiają skuteczność cyberbezpieczeństwa.

Michał Kaczmarek
Menadżer SOC

Zewnętrzny zespół SOC powinien na etapie przygotowania wspomagać zmiany w systemie IT skutkujące dobrym poziomem telemetrii, fundamentalnym w procesie efektywnej detekcji.

Dojrzały zespół SOC może rozpocząć świadczenie usługi na posiadanych przez organizację narzędziach i wspomaga kreowanie przemyślanej strategii zarządzania incydentami (w tym doboru technologii i procesów).

Zewnętrzny zespół SOC odgrywa rolę eksperta i partnera do kreowania i utrzymywania strategii zarządzania cyberbezpieczeństwem.

SOC powinien również świadczyć usługę w oparciu o branżowe standardy potwierdzone certyfikacjami oraz rekomendowane procedury reagowania na incydenty cyberbezpieczeństwa (w tym posiadać kompetencje w pełnej eliminacji zagrożeń).

Jak Trecom pomaga spełnić wymogi NIS 2?

NASZE USŁUGI

Trecom pomaga organizacjom w spełnieniu wymogów dyrektywy NIS 2, wykorzystując najlepsze standardy branżowe oraz oferując zarówno ekspertyzę techniczną, jak również wsparcie w implementacji gotowych rozwiązań.

MIROSŁAW MAJ (DYREKTOR TRECOMSEC)

TRECOMSEC

- Trecom świadczy kompleksowe usługi audytu luki zgodności organizacji z wymogami NIS2 oraz DORA
- Zapewniamy również usługi wspierające budowanie zespołów od cyberbezpieczeństwa, wprowadzania procedur zachodzących w SOC czy modelowania zagrożeń

MICHAŁ KACZMAREK (MENADŻER SOC)

TRECOM SOC

- Trecom SOC oferuje kompleksowe zarządzanie incydentami (m.in wykrywanie, ocenę wpływu, eskalację i rozwiązanie)
- Oferujemy również szeroki zakres dodatkowych usług, w tym analizę ryzyka, CTI czy analizę malware
- Nasza usługa SOC jest zgodna z SIM3 oraz posiada status trusted introducer

NASZE ROZWIĄZANIA

Oferujemy szeroki zakres rozwiązań technologicznych wspierających spełnienie wybranych wymogów w zakresie NIS 2:

- Rozwiązania klasy SIEM, SOAR i UEBA
- Rozwiązania do zarządzania ryzykiem i podatnościami
- Rozwiązania klasy XDR czy EDR
- Firewall
- Rozwiązania klasy IAM
- Bazy CMDB
- Rozwiązania do ochrony sieci i środowiska chmurowego
- Rozwiązania do ochrony aplikacji
- i wiele innych

Przygotujemy Twoją organizację na NIS 2

BEZPŁATNE KONSULTACJE NIS 2

Wszystkich zainteresowanych NIS 2 zapraszamy na darmowe konsultacje, podczas których będziemy mogli porozmawiać o tym, jak spełnić wymogi NIS 2 w konkretnych przypadkach.

SKONTAKTUJ SIĘ Z NAMI

Aleksander Bronowski
NIS2@trecom.pl
+48 600 945 962