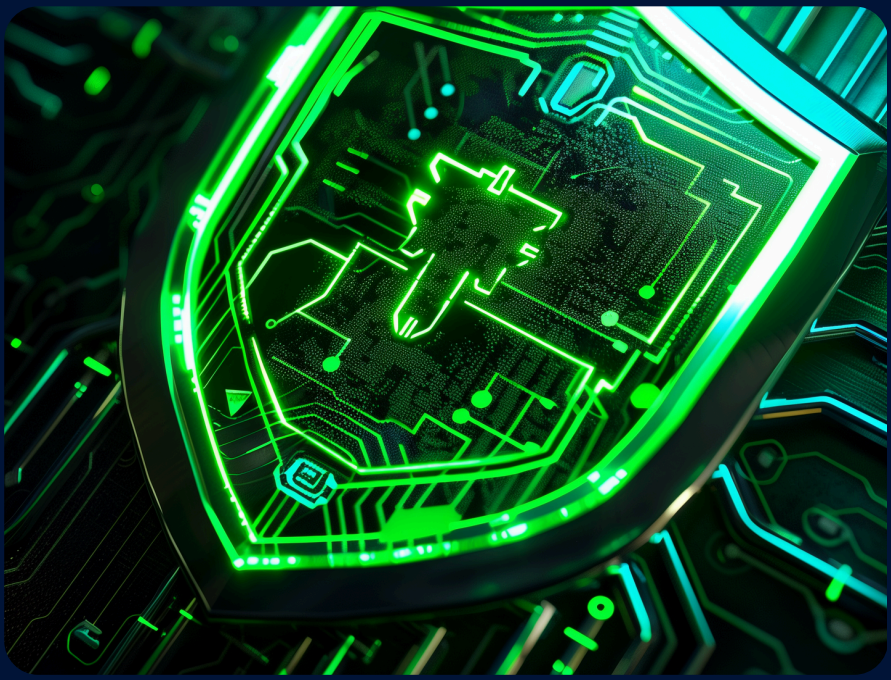
trecom

WHITE PAPER

Zbieranie Informacji o Cyberzagrożeniach i Podatnościach w Kontekście Wymogów NIS 2



NIS2@trecom.pl
+48 600 945 962

Spis treści

Wprowadzenie do NIS 2

KONTEKST

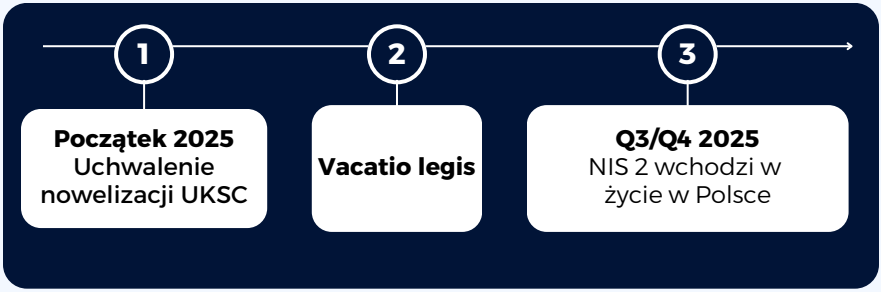
NIS 2 stanowi znaczący krok w poprawie ochrony i odporności przed cyberzagrożeniami organizacji w UE.

W Polsce dyrektywa NIS 2 będzie implementowana poprzez nowelizację ustawy z dnia 5 lipca 2018 roku 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 roku.

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?

W jednym z naszych pierwszych materiałów przedstawiliśmy, jak powinien wyglądać proces zarządzania incydentami. W tym white paper skupimy się na przedstawieniu ogólnej myśli strategicznej w zakresie zbierania informacji o cyberzagrożeniach i podatnościach. Ponadto przedstawimy obszar CTI i możliwości wykorzystania feedów CTI w narzędziach czy procesie analizy ryzyka.

TREŚĆ PORADNIKA

- Myśl strategiczna w zbieraniu informacji o cyberzagrożeniach i podatnościach
- Cyber Threat Intelligence
- Zbieranie informacji i zarządzanie podatnościami
- Priorytetyzacja podatności - case study

O AUTORACH WHITE PAPER

Aleksander Bronowski
Trecom
GTM Menadżer

Mirosław Maj
TrecomSEC
Dyrektor

Cyprian Gutkowski
TrecomSEC
Konsultant

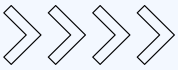
Wojciech Korus
Inżynier ds.
cyberbezpieczeństwa

Zapraszamy do lektury

Myśl strategiczna

WSTĘP

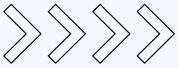
Każda próba wdrożenia zabezpieczeń w organizacji powinna być poprzedzona myślą strategiczną na poziomie najwyższego kierownictwa. To część tzw. governance, risk and compliance. Przede wszystkim należy zrozumieć/ustalić:



- Wymagania biznesowe/funkcjonalne w kontekście cyberbezpieczństwa. W jaki sposób cele cyberbezpieczeństwa mają wspierać cele biznesowe/funkcje organizacji?
- Ramy i priorytety zarządzania ryzykiem. Co jest dla nas (dla naszego biznesu) największym zagrożeniem, jakie podatności będą krytyczne, jaki jest profil ryzyka naszej organizacji? Jakie ryzyko możemy zaakceptować?
- Jaką wartość dla organizacji przyniesie optymalizacja inwestycji w cyberbezpieczeństwo?
- Czy możemy zdefiniować metryki sukcesu zarządzania naszym cyberbezpieczeństwem? Jak mierzyć skuteczność procesów zarządzania incydentami, podatnościami i zagrożeniami?
- Czy i w jaki sposób możemy zintegrować i skoordynować procesy biznesowe i procesy bezpieczeństwa, by uzyskać tzw. strategiczne dostosowanie (strategic allignment)?

PRACE ANALITYCZNE

W następstwie wypracowania strategicznego podejścia do cyberbezpieczeństwa, należy przystąpić do prac analitycznych, które dostarczą informację o tym w jakim punkcie jest nasza organizacja i co należy poprawić. Ramy określone w strategii i politykach mają sprawić, że będzie to ciągły proces doskonalenia. Prace analityczne powinny objąć:

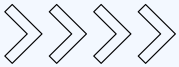


- Szczegółową inwentaryzacją aktywów informacyjnych.
- Analizę wpływu niedostępności na biznes (BIA – business impact analysis). Dzięki temu zrozumiemy jakie są krytyczne procesy, a tym samym powiązane z nimi aktywa i usługi informatyczne.
- Szacowanie i ocenę ryzyka cyberbezpieczeństwa dla aktywów informacyjnych, z uwzględnieniem wiedzy zebranej podczas BIA.

Efektem powyższych analiz powinna być identyfikacja właściwych zabezpieczeń cyberbezpieczeństwa, zarówno na poziomie procesowym, organizacyjnym, jak i technologicznym. Zabezpieczenia takie jak monitoring zagrożeń (cyber threat intelligence), zarządzanie podatnościami i incydentami, muszą być odpowiednio zaplanowane i wpisywać się w potrzeby określone na poziomie nadzoru.

MINIMALNE POTRZEBY OPERACYJNE

W praktyce, minimalne potrzeby operacyjne w kontekście tych zabezpieczeń są następujące:



- Opracowanie procesu obsługi incydentów w oparciu o zdefiniowane role specjalistów, czynności analityczne, komunikację pomiędzy interesariuszami, zakres odpowiedzialności i narzędzia/systemy wspierające (ten obszar został pokryty w white paper w obszarze zarządzania incydentami)

- Zrozumienie krajobrazu zagrożeń na poziomie technicznym, taktycznym i strategicznym, by móc reagować na ciągłą ewolucje i zmiany, nowe ataki i procedury cyberprzestępców. Narzędzia i ręczna analiza danych o zagrożeniach oraz przetwarzanie ich w użyteczną informację jest celem dobrego threat intelligence.

- Wnikliwie zrozumienie potencjalnych płaszczyzn ataku oraz obecnego stanu konfiguracji bezpieczeństwa aktywów. Skanowanie podatności, analiza konfiguracji, badanie hardeningu i testy penetracyjne to elementy, które pozwolą to określić. Niezbędnym komponentem jest „ułożenie" tego zagadnienia na linii cyberbezpieczeństwo-informatyka (chodzi o działy).

Cyber Threat intelligence

DEFINICJA CYBER THREAT INTELLIGENCE

Dobrze przeprowadzona analiza ryzyka w przypadku NIS 2 wymaga od organizacji analizy szerszego kontekstu zagrożeń, które gwarantuje Cyber Threat Intelligence. CTI to zbiór narzędzi i procesów umożliwiających identyfikację i analizę działań wszelkiego rodzaju adwersarzy.

ZBIERANIE DANYCH

Etap zbierania skupia się na pozyskiwaniu nieprzetworzonych danych z różnych źródeł, aby zbudować pełny obraz potencjalnych zagrożeń. Dane mogą pochodzić m.in. z:

- Źródeł zewnętrznych, takich jak bazy open-source, fora internetowe czy informacje od komercyjnych dostawców feedów CTI
- Danych wewnętrznych, czyli danych pochodzące z systemów i infrastruktury organizacji, takich jak logi sieciowe czy urządzania końcowe

PRZETWARZANIA DANYCH CTI

Gdy dane zostaną zebrane przechodzimy do przetwarzania, czyli przekształcenia danych w użyteczne informacje poprzez agregację i normalizację danych. Jest to kluczowy krok, który przygotowuje dane do następnego etapu, czyli analizy.

Ponadto należy zweryfikować potencjalne złośliwe źródła.

INDICATORS OF COMPROMISE (IOC)

Indicators of Compromise (IOC) to kluczowe informacje wykorzystywane do wykrywania i śledzenia złośliwych aktywności.

Są to konkretne wskazówki jak hashe plików, adresy IP, nazwy domen czy sygnatury złośliwego oprogramowania, które wskazują na potencjalne naruszenie bezpieczeństwa.

IOC pomagają organizacjom monitorować i wykrywać konkretne zagrożenia w czasie rzeczywistym, służąc jako kryteria wyszukiwania w logach sieciowych lub systemach bezpieczeństwa.

Wskaźniki kompromitacji (IOC) związane ze złośliwym oprogramowaniem, takie jak hashe plików czy sygnatury, są szczegółowo analizowane w celu zrozumienia taktyk, technik i procedur (TTP) stosowanych przez atakujących. Proces analizy obejmuje badanie działania złośliwego oprogramowania, ocenę potencjalnych szkód dla systemów i danych oraz identyfikację ewentualnych powiązań z grupami cyberprzestępczymi.

Domeny i adresy IP służą do śledzenia i monitorowania infrastruktury przeciwnika, wspierając wykrywanie zagrożeń i reagowanie na incydenty poprzez identyfikację pochodzenia i struktury cyberataków.

KATEGORIE INFORMACJI

W ramach obszaru threat intelligence wymieniamy 4 główne kategorie informacji:

TECHNICZNE

Mowa o konkretnych informacjach potwierdzających wystąpienie ataku - dowody na to, że atak ma miejsce lub zidentyfikowano IOC

OPERACYJNE

Dane operacyjne o zagrożeniach to dane, które można wykorzystać w ramach aktywnego zarządzania zagrożeniami umożliwiając podjęcie działań przeciwko konkretnemu atakowi

TAKTYCZNE

Taktyczne informacje zapewniają szczegóły dotyczące scenariuszy, technik czy narzędzi wykorzystywanych w ramach ataków

STRATEGICZNE

W tym przypadku chodzi o informacje natury strategiczno-biznesowej, które pokażą wpływ decyzji biznesowej na ekspozycje na różnego rodzaju zagrożenia

CELE CTI

Informacje z CTI na różnych poziomach mają więc za zadanie identyfikację zagrożeń zewnętrznych dla bezpieczeństwa informacji i ciągłości działania.

Zbieranie informacji CTI powinno mieć ciągły charakter umożliwiając monitorowanie aktywności adwersarzy i ich technik

WYKORZYSTANIE CYBER THREAT INTELLIGENCE W NARZĘDZIACH

Dane Cyber Threat intelligence możemy również wykorzystywać w różnego rodzaju narzędziach. Przykładowo, możemy proaktywnie analizować sieci i nietypowe zdarzenia w ramach rozwiązań SIEM.

W momencie otrzymania alertu ze SIEM, dotyczącego np. wykrycia podejrzanego pliku lub odnotowania niepokojącego połączenia sieciowego, analityk weryfikuje dane zdarzenia i zapoznaje się z jego szczegółami. Zwraca uwagę na występujące w nim artefakty takie jak adresy IP, adresy URL, domeny czy hashe plików.

W zależności od narzędzia z jakim pracuje (dostawcy SIEM) oraz jego konfiguracji ma możliwość uzyskać więcej informacji na temat tych artefaktów bezpośrednio w SIEM - ze względu na integracje z innymi narzędziami - bądź posiłkuje się zewnętrznymi źródłami informacji, tzw. bazami reputacyjnymi.

W tych bazach analityk ma możliwość sprawdzić czy znane jest powiązanie analizowanego pliku (hash), domeny, adresu IP itd. ze złośliwym oprogramowaniem lub złośliwą działalnością np. skanowaniem sieci, rozsyłaniem spamu lub phishingu.

Informacje z baz reputacyjnych wzbogacają analizę specjalisty SOC i nadają szerszy kontekst sytuacji, która może mieć miejsce w związku z alertem.

WYKORZYSTANIE CYBER THREAT INTELLIGENCE W PRACY ANALITYCZNEJ

Przykładowo: Analityk otrzymał alert związany z wielokrotnymi połączeniami, których źródłem jest jeden adres publiczny, ale docelowych adresów jest więcej. Analizując logi widzi on, że celem kolejnych połączeń są kolejne adresy IP z puli organizacji. Na ten moment, na podstawie tych informacji, wstępnie zakłada, że ma miejsce skanowanie sieci z zewnątrz.

Sprawdzając źródłowy adres IP w bazach reputacyjnych napotyka informacje, że ten adres IP w przeszłości był wykorzystywany do skanowania i nie ma on pozytywnej reputacji. W takim przypadku analityk podejrzewa skanowanie sieci i ma informacje o adresie IP, które niejako potwierdzają jego tezę. W tym momencie, jeśli jest to zgodne z procedurami SOC, może ten adres zablokować i odpowiednio udokumentować zdarzenie.

Zbieranie danych z CTI

JAK POWINNO WYGLĄDAĆ ZBIERANIE DANYCH Z CTI W KONTEKŚCIE NIS 2

Zbieranie informacji o zagrożeniach powinno zostać uwzględnione w procesie analizy ryzyka oraz zarządzania incydentami.

Organizacje powinny w pierwszej kolejności zidentyfikować kluczowe źródła informacji o zagrożeniach.

Na dole prezentujemy przykłady podstawowych źródeł, które powinny zostać uwzględnione w obszarze CTI.

PRZYKŁADY ŹRÓDEŁ DANYCH O CTI

Pierwszym przykładem źródeł danych i informacji z zakresu CTI są blogi i fora dostawców technologii cyberbezpieczeństwa.

Wspomniane źródła zapewniają podstawowe informacje o atakach hakerskich, aktywnościach grup przestępczych czy aktualnie wykorzystywanych podatnościach.

Kolejnym z źródeł mogą być ogólne fora i strony agregujące informacje o cyberbezpieczeństwie. Innym przykładem agregatorów danych są ogólnodostępne bazy reputacyjne.

Dane z tych źródeł (nowe wydarzenia) powinno się agregować w jednym miejscu, które umożliwi analizę w czasie rzeczywistym. Ponadto warto rozważyć zbieranie danych z Darknetu np. od zewnętrznych dostawców. W Trecom również aspekt Darknetu jest częścią usługi CTI.

Uwzględnienie pozostałych źródeł powinno wynikać z indywidualnej analizy potrzeb każdej organizacji. Na niektórych aspektach skupią się firmy z branży energetycznej, a na innych działające w ochronie zdrowia.

Skanery podatności

PRZYKŁADY DZIAŁANIA SKANERÓW PODATNOŚCI

Drugim ważnym obszarem w zakresie zbierania informacji o zagrożeniach są informacje o podatnościach, czyli wszelkiego rodzaju lukach czy wadach na warstwie systemów informatycznych, sieci czy pozostałych elementów infrastruktury. Kluczowe w identyfikacji podatności są narzędzia do skanowania sieci, aplikacji, kontenerów itd.

SKANERY SIECIOWE

Skanery sieciowe służą kompleksowej analizie infrastruktury IT. Do przykładowych narzędzi należą Nessus czy Qualys.

SKANERY APLIKACJI

Skanery odpowiedzialne za testy bezpieczeństwa aplikacji webowych czy identyfikację podatności ma poziomie kodu. Do przykładowych narzędzi należą Acunetix czy Burp Suite.

SKANERY KONTENERÓW

W przypadku korzystania z kontenerów warto rozważyć inwestycje w narzędzia do skanowania środowiska Docker i identyfikacji zagrożeń w mikrousługach. Dostawcy oferujący wspomniane technologie to Anchore czy Clair.

Do pozostałych grup skanerów należą m.in. skanery chmurowe czy mobilne.

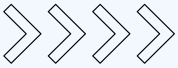
Zbieranie informacji i zarządzanie podatnościami

WSTĘP

Po zebraniu informacji o podatnościach należy nimi zarządzić. Składa się na to ich ocena, przypisanie do odpowiednich jednostek w organizacji oraz ustalenie priorytetów obsługi.

Znaczącym wyzwaniem w obszarze zarządzania podatnościami jest identyfikacja i priorytetyzacja podatności w celu obsługi luk, które stanowią największe zagrożenia dla organizacji.

W praktyce trudność obsługi podatności wynika z kilku elementów:



Ograniczeń na warstwie zasobów

Ograniczonym przełożeniem na inne działy czy osoby w ramach organizacji, które są odpowiedzialne za obszar związany z podatnością

Ograniczeniami na warstwie widoczności zagrożeń oraz podatności

Jednym ze sposobów na priorytetyzację podatności jest szacowanie szerszego profilu ryzyka podatności (charakterystyki aktywa, stopnia zabezpieczenia, ekspozycji na ryzyko itd.).

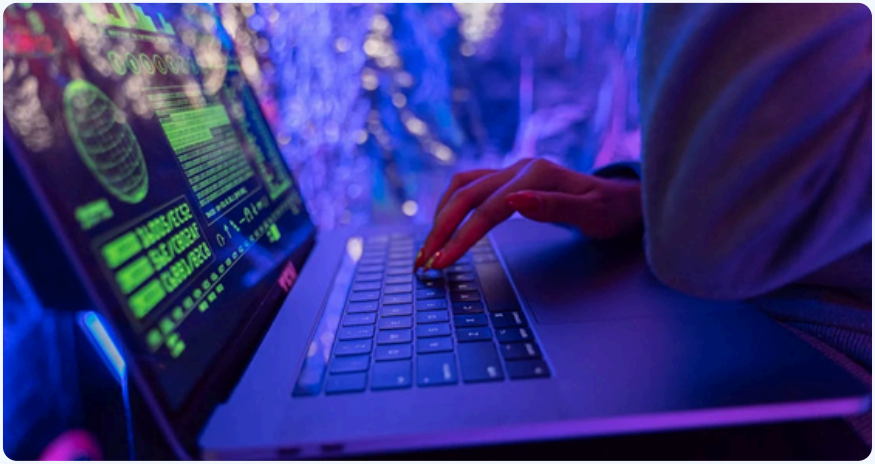
Wspomniane podejście jest rekomendowane przez wiele podmiotów odpowiedzialnych za techniczne rekomendacje (jak Gartner).

NA CZYM OPIERA SIĘ OBECNIE ZARZĄDZANIE PODATNOŚCIAMI?

Obecnie znacząca część organizacji korzysta z dwóch możliwości w zakresie zarządzania podatnościami:

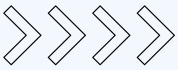
- Pierwszą możliwością jest współpraca z zewnętrznym partnerem czy dostawcą w ramach obszaru zarządzania podatnościami w oparciu o jasno zdefiniowane wymogi w ramach SLA tj. zamknięcie jasno określonej liczby podatności w konkretnej jednostce czasu (np. tygodniu czy miesiącu)

- Drugim przykładem jest zarządzanie podatnościami w ramach wewnętrznych zespołów, które najczęściej opierają się na standardach jak Common Vulnerabilities and Exposures czy Common Vulnerability Scoring System. Wspomniane standardy ujednolicają ocenę podatności nie uwzględniając indywidualnych ryzyk w ramach organizacji.



KWESTIE TECHNICZNE

Sam proces zarządzania podatnością może okazać się dodatkowo złożony z powodów czysto technicznych:



Poprawki mogę być dostępne po dłuższym okresie od publikacji

Poprawki wymagają walidacji oraz testów w celu ograniczenia negatywnych wpływów na organizację

Powyższe czynniki oraz statystyki na temat wykorzystania podatności pokazują jak ważna jest szybka priorytetyzacja podatności w oparciu o realne ryzyko w celu jak najszybszej reakcji.

KLUCZOWE STATYSTYKI O PODATNOŚCIACH W 2023 (QUALYS)

44 DNI

Średni czas do wykorzystania podatności

25%

Procent podatności wykorzystanych w dniu publikacji

75%

Procent podatności wykorzystanych w ciągu 19 dni

Priorytetyzacja podatności - case study

JAK MOŻE WYGLĄDAĆ PROCES ZBIERANIA I ZARZĄDZANIA PODATNOŚCIAMI W PRAKTYCE?

1) SKANOWANIE SYSTEMÓW

Pierwszym punktem w zarządzaniu podatnościami jest uruchomienie skanera podatności jak Tenable, Rapid7, Greenbone, Qualys czy Nuclei.

Wspomniane narzędzia skanują systemy, identyfikują otwarte porty czy korelują zebrane informacje z zidentyfikowanymi podatnościami.

Skanery analizuję wybrane elementy infrastruktury, w tym serwery fizyczne, maszyny wirtualne, komputery, bazy danych czy narzędzia z obszaru cyberbezpieczeństwa (jak zapory sieciowe).

Skanery zbierają również informacje m.in. o posiadanej wersji oprogramowania, otwartych portach, konfiguracji systemów i urządzeń czy wielu innych danych w celu weryfikacji podatności w globalnych bazach danych zbierających informacje podatnościach.

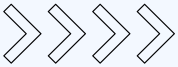
2) OCENA I PRIORYTETYZACJA PODATNOŚCI

Kolejnym punktem po zebraniu podstawowych informacji ze skanera podatności powinna być analiza ryzyka związana z podatnością. Niezwykle przydatnym standardem w ocenie ryzyka jest Common Vulnerability Scoring System, który pomaga w ocenie krytyczności podatności.

OCENA PODATNOŚCI

Kluczem w ocenie podatności jest indywidualna ocena ryzyka dla organizacji wynikająca z podatności oraz sama priorytetyzacja działań, czyli odpowiedź na pytanie czym warto zająć się w pierwszej kolejności.

Do tego zadania niezwykle przydatne mogą okazać się narzędzia do zarządzania podatnościami, które przypisują indywidualne poziomy ryzyka do podaności. Tak przykładowo prezentują się kluczowe czynniki analizowane przez SecureVisio w ramach analizy podatności:



- Stopień krytyczności aktywa
- Powiązane procesy biznesowe
- Zabezpieczenie aktywa
- Unikalne cyber ryzyka aktywa
- Wektory ataku
- Krytyczność podatności (systemy scoringowe)
- i wiele innych

OCENA PODATNOŚCI

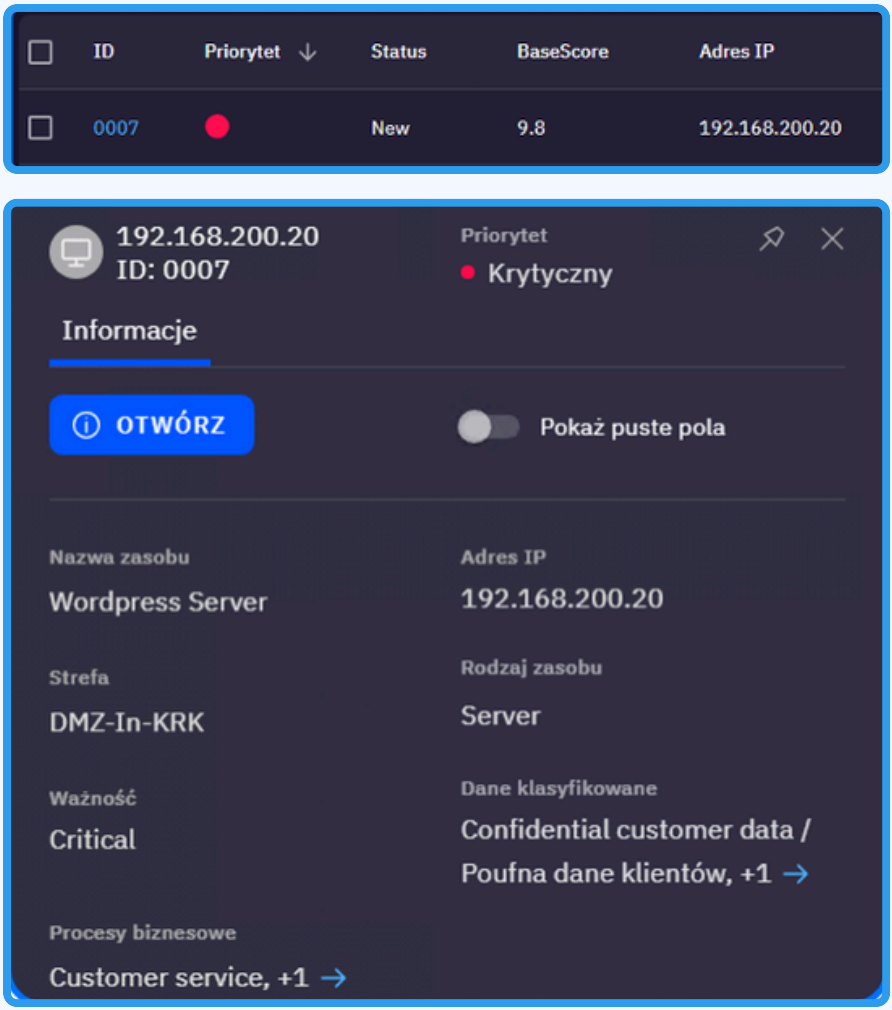
Poniższy screen SecureVisio pokazuje zebrane podatności, które system spriorytetyzował w oparciu o unikalny profil ryzyka dla organizacji. Dodatkowo SecureVisio zapewnia kluczowe informacje jak adres IP czy nazwę aktywa (np. serwer Wordpress)

ID	Priority	Status	BaseScore	IP address	Asset name
0007		New	9.8	192.168.200.20	Wordpress Server
0009		New	7.2	192.168.200.20	Wordpress Server
0016		New	9.8	192.168.73.102	nuc-lf.nuc.lab
0017		New	9.8	192.168.73.102	nuc-lf.nuc.lab
0020		New	0.0	192.168.73.50	SRV-in-WAW
0005		New	5.3	192.168.200.20	Wordpress Server
0006		New	5.3	192.168.200.20	Wordpress Server
0001		New	0.0	192.168.191.242	Internal applicatic
0004		New	0.0	192.168.200.20	Wordpress Server
0008		New	9.8	192.168.200.20	Wordpress Server

ZEBRANE PODATNOŚCI W ROZWIĄZANIU SECUREVISIO

ANALIZA KONKRETNEJ PODATNOŚCI

Po kliknięciu w konkretną podatność dostajemy informacje o krytyczności, nazwie zasobu, powiązanych procesach biznesowych i wielu innych informacjach.

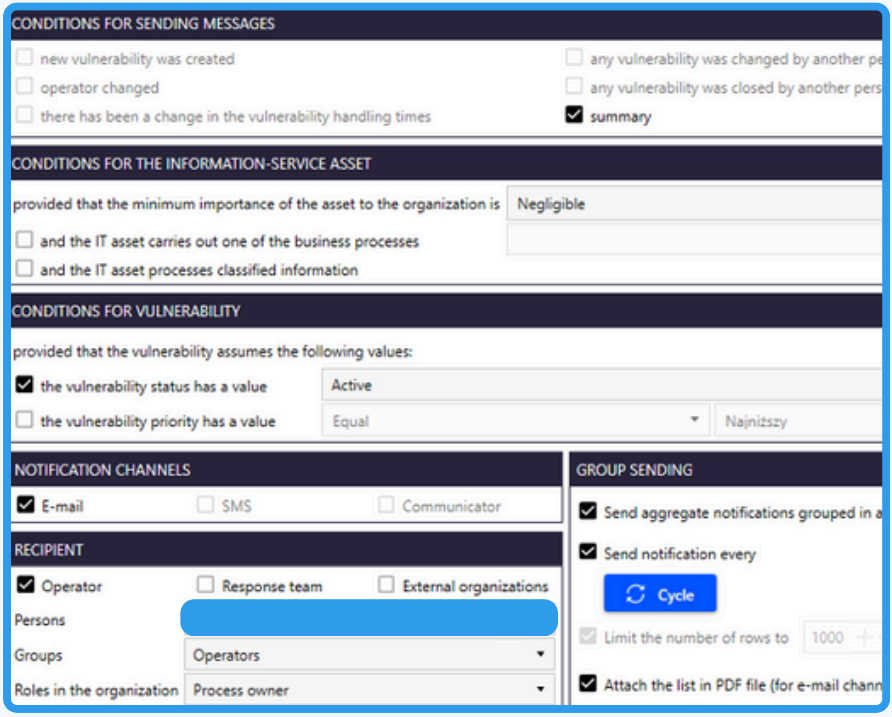


ANALIZA WYBRANEJ PODATNOŚCI W ROZWIĄZANIU SECUREVISIO

REAKCJA NA PODATNOŚĆ

3) REAKCJA

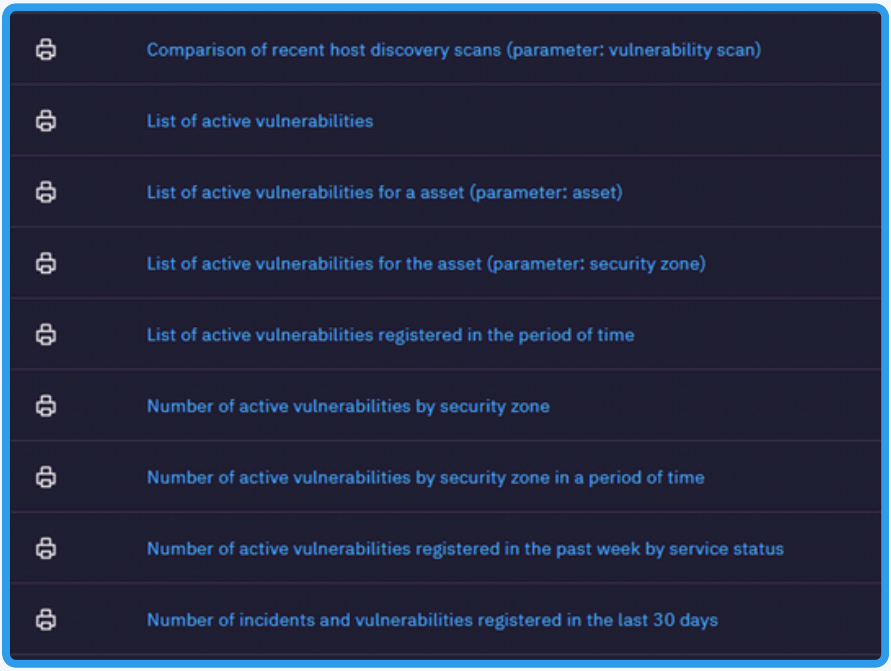
Reakcja na podatność to kwestia indywidualnego kontekstu. Przykładowo możemy mówić o aktualizacji oprogramowania czy systemów operacyjnych, zmiany konfiguracji systemów czy innych inicjatywach. Wspomniane obszary wymagają często współpracy między zespołami bezpieczeństwa, DevOps, administracji IT czy innymi jednostkami. Systemy jak SecureVisio zapewniają "workflow" umożliwiający kompleksową komunikację i współpracę między zespołami w obszarze zarządzania podatnościami:



PRZYKŁAD USTAWIANIA KOMUNIKACJI W ROZWIĄZANIU SECUREVISIO

REAKCJA NA PODATNOŚĆ

Wraz z samą komunikacją kluczowe jest zapewnienie wspierających informacji (np. listy aktywnych podatności czy podatności dla danego okresu) wraz z wykresami i raportami. Dzięki temu osoby odpowiedzialne za reakcję na podatność mogą podejmować efektywne decyzje. SecureVisio oferuje pakiet gotowych raportów, które można wysyłać do różnych zespołów w ramach organizacji.



TWORZENIE RAPORTÓW O PODATNOŚCIACH W ROZWIĄZANIU SECUREVISIO

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 tworzenia metodyki szacowania ryzyka, tworzenia dokumentacji SZBI czy przeprowadzenia szkoleń

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 szacowanie podatności
- 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
- Metodyka szacowania ryzyka i SZBI
- Szkolenia
- Rozwiązania klasy IAM
- 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