trecom

WHITE PAPER

Podstawowe Praktyki Cyberhigieny i Cyberochrony W Kontekście Wymogów NIS 2

NIS2@trecom.pl
+48 600 945 962

Spis treści

3 **Wprowadzenie do NIS 2**

7 **Kontekst i znaczenie cyberhigieny**

10 **Podstawowe procesy i narzędzia wspierające cyberochronę i bezpieczeństwo informacji**

22 **Wdrożenie programu podnoszenia świadomości cyberbezpieczeństwa**

28 **Cyberochrona i cyberhigiena - checklista**

33 **Jak Trecom pomaga spełnić wymogi NIS 2?**

Wprowadzenie do NIS 2

KONTEKST

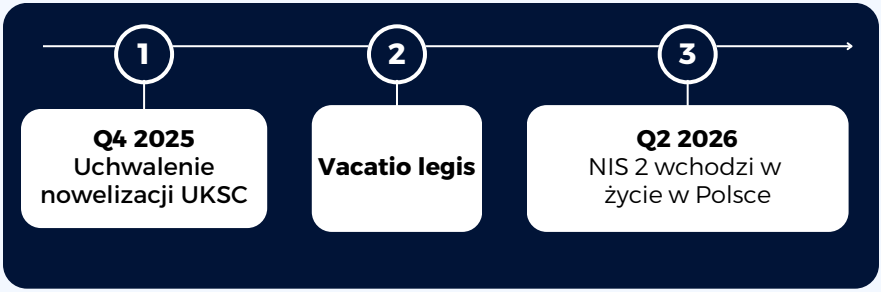
NIS 2 stanowi znaczący krok w poprawie ochrony i odporności przed cyberzagrożeniami organizacji w UE.

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 Q2 2026 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?

Przygotowany przez nas white paper ma pomóc przygotować się organizacjom na wymogi NIS 2 w zakresie podstawowych procesów i narzędzi wspierających cyberochronę i bezpieczeństwo informacji oraz cyberhigieny. White paper jest częścią serii na temat NIS 2, którą będziemy kontynuować w kolejnych tygodniach.

TREŚĆ WHITE PAPER

- Kontekst i znaczenie cyberhigieny
- Podstawowe procesy i narzędzia wspierające cyberochronę i bezpieczeństwo informacji
- Najlepsze praktyki w zakresie inwentaryzacji zasobów, zarządzania podatnościami czy danymi
- Wdrożenie programu podnoszenia świadomości cyberbezpieczeństwa
- Checklista dla cyberhigieny i podstawowych procesów i narzędzi wspierających cyberochronę i bezpieczeństwo informacji

O AUTORACH WHITE PAPER

Aleksander Bronowski
Trecom
GTM Menadżer

Mirosław Maj
TrecomSEC
Dyrektor

Cyprian Gutkowski
TrecomSEC
Konsultant

Artur Markiewicz
Trecom
Konsultant

Marcin Fronczak
TrecomSEC
Konsultant

Cyprian Gutkowski
TrecomSEC
Analityk systemów bezpieczeństwa

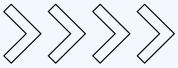
Zapraszamy do lektury

Kontekst i znaczenie cyberhigieny

KONTEKST I ZNACZENIE CYBERHIGIENY

Proaktywny rozwój i promocja cyberbezpieczeństwa oraz najlepszych praktyk cyberhigieny umożliwia organizacjom poprawienie skuteczności ochrony przed zmieniającym się krajobrazem zagrożeń cybernetycznych.

To właśnie te z pozoru najbardziej oczywiste ryzyka (jak nadanie nieodpowiednich uprawnień czy brak aktualizacji systemu) mogą doprowadzić do strat wizerunkowych i biznesowych.



Microsoft szacuje, że wdrożenie odpowiednich zasad cyberhigieny **uniemożliwia 98% ataków.**

W praktyce promocja cyberhigieny i spełnienie wymogów w tym zakresie powinno odbywać się na poziomie systemowego zaadresowania podstaw cyberochrony i bezpieczeństwa informacji oraz ogólnej promocji i podnoszenia świadomości o cyberbezpieczeństwie (np. w formie programu podnoszenia świadomości cyberbezpieczeństwa).

Systemowe podejście to zbiór praktyk i działań, które zapewniają bezpieczeństwo i dobrą ochronę systemów, użytkowników czy danych. Przykładem takich inicjatyw jest chociażby edukacja pracowników, regularna aktualizacja kluczowych systemów czy odpowiednia kontrola dostępu.

Spełnienie podstawowych wymogów cyberhigieny umożliwia również dalsze tworzenie dopasowanych strategii dla indywidualnych potrzeb w ramach cyberbezpieczeństwa.

OD CZEGO ZACZĄĆ?

Rozważania do każdego zagadnienia definiowanego w ramach NIS 2 powinniśmy rozpocząć od analizy indywidualnych potrzeb organizacji. Niemniej w tym white paper postaramy się zdefiniować najważniejsze elementy, które będą stanowić podstawę w podejmowaniu konkretnych kroków w ramach cyberhigieny czy podstawowych procesów i narzędzi wspierające cyberochronę i bezpieczeństwo informacji. Temat cyberhigieny i powiązanych wymogów jest często definiowany w różnego rodzaju normach czy poradnikach agencji (jak np. CIS, ENISA czy NIST).

Poniżej przedstawiamy procesowe podejście do spełnienia wymogu cyberhigieny oraz podstaw cyberochrony i bezpieczeństwa informacji. Wspomniane elementy można podzielić na 1) wdrożenie podstawowych procesów i narzędzi wspierających cyberochronę i bezpieczeństwo informacji oraz 2) wdrożenie programu podnoszenia świadomości cyberbezpieczeństwa.

WDROŻENIE PODSTAWOWYCH PROCESÓW I NARZĘDZI WSPIERAJĄCYCH CYBEROCHRONĘ I BEZPIECZEŃSTWO INFORMACJI

W pierwszym punkcie mówimy o wdrożeniu procesów i narzędzi m.in. w zakresie:

- **aktualizacji oprogramowań i systemów**
- **tworzenia kopii zapasowych**
- **stosowania uwierzytelniania wieloskładnikowego**
- **ochrony danych**
- **ochrony przed atakami typu malware czy phishing**
- **pozostałych zagadnień**

W ramach white paper skupimy się na pierwszych czterech zagadnieniach. Pozostałe obszary pokryte będą w formie checklisty na końcu materiału.

WDROŻENIE PROGRAMU PODNOSZENIA ŚWIADOMOŚCI O CYBER-BEZPIECZEŃSTWIE

W drugim punkcie mówimy m.in. o:

- **edukacji pracowników z samych zasad cyberhigieny oraz narzędzi z zakresu cyberbezpieczeństwa**
- **inicjatywach wspierających świadomość pracowników o cyberbezpieczeństwie**

Podstawowe procesy i narzędzia wspierające cyberochronę i bezpieczeństwo informacji

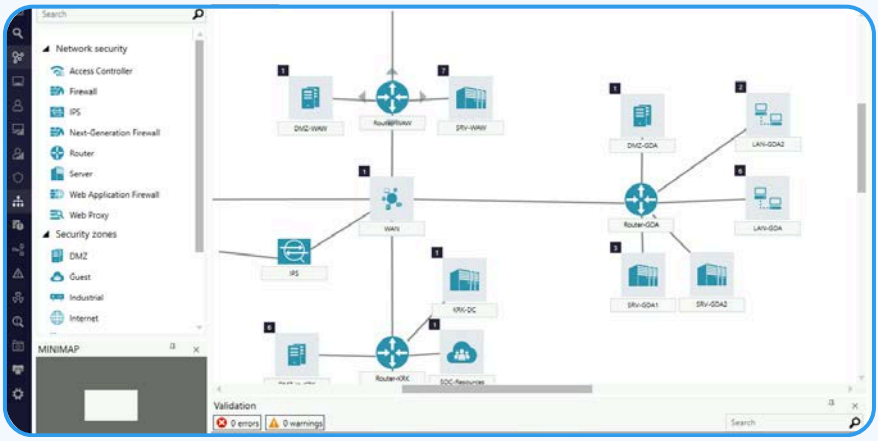
INWENTARYZACJA ZASOBÓW

Pierwszym krokiem przed wdrożeniem podstawowych procesów i narzędzi w ramach cyberhigieny powinna być inwentaryzacja obecnie posiadanych zasobów. Proces ten będzie stanowił podstawę w wdrożeniu dopasowanych rozwiązań w ramach cyberhigieny.

Brak aktualnych map z zasobami otwiera możliwości do wykorzystania podatności oraz niezabezpieczonych zasobów.

Inwentaryzacji zasobów w kontekście cyberbezpieczeństwa to zebranie specyfikacji oraz zależności posiadanego sprzętu, oprogramowania, urządzeń, serwerów, danych, środowiska chmurowego czy urządzeń IoT.

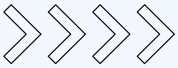
Inwentaryzacja może odbywać się na wiele sposobów. Organizacje mogą zarówno manualnie dokonywać inwentaryzacji oraz posiłkować się gotowymi narzędziami jak np. bazami CMDB.



PRZYKŁAD BAZY CMDB W ROZWIĄZANIU SECUREVISIO

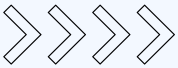
ZARZĄDZANIE PODATNOŚCIAMI

Dzięki odpowiedniej inwentaryzacji posiadanych zasobów organizacje zyskują pełne zrozumienie aktywów do ochrony oraz potencjalnych luk w zabezpieczeniach. Jednym z przykładów wspomnianych luk są podatności czyli słabości w systemach, które cyberprzestępcy mogą wykorzystać na swoje potrzeby. Istnieje wiele przykładów podatności:



- błędy w konfiguracjach
- podatności w sieciach (np. źle skonfigurowane zapory)
- podatnosci na poziomie systemów operacyjnych
- ogólne braki na poziomie aktualizacji oprogramowania

Cyberprzestępcy skanują różnego rodzaju zasoby w poszukiwaniu podatności stąd proaktywne działanie umożliwia ograniczenie wpływu wspomnianych aktywności.

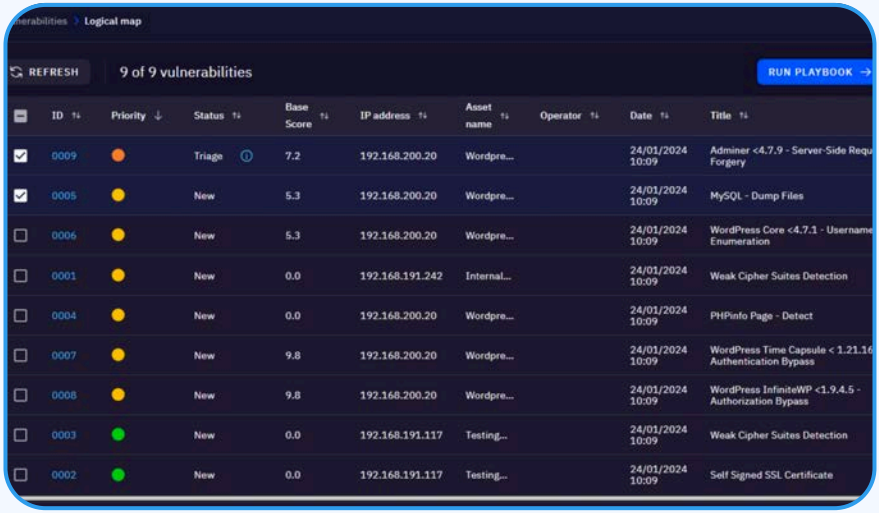


29 000 Liczba nowych luk wykryta w 2023 (CVEDetails)

Sam proces zarządzania podatnościami powinniśmy zacząć od oceny i analizy podatności, które standardowo przeprowadzone są przez różnego rodzaju skanery.

SKANERY PODATNOŚCI

Na rynku rozwiązań znajdziemy narzędzia wyspecjalizowane w konkretnym obszarze jak np. skanowaniu sieci, aplikacji internetowych, środowisk IoT i kontenerów czy narzędzia konsolidujące zebrane podatności z kluczowych systemów.



PRZYKŁAD KONSOLIDACJI ZARZĄDZANIA PODATNOŚCIAMI W ROZWIĄZANIU SECUREVISIO

Skanery wykorzystują publicznie zgłaszane dane na temat podatności do identyfikowania i klasyfikowania podatnych na ataki urządzeń i oprogramowań w infrastrukturze organizacji.

Najważniejszym zadaniem skanerów podatności jest identyfikacja słabych punktów zabezpieczeń i dostarczanie kluczowych danych.

ZARZĄDZANIE PODATNOŚCIAMI

Skanery podatności wykorzystują wspomniane informacje do identyfikowania podatnych na ataki systemów czy oprogramowań w infrastrukturze. Skanery weryfikują m.in. wersje oprogramowania czy ustawienia konfiguracji organizacji w celu walidacji luk.

Narzędzia do zarządzania podatnościami oferują różnego rodzaju analityki czy raporty podsumowujące najważniejsze dane na temat podatności, które mogą okazać się kluczowe z punktu widzenia systemowego zarządzania podatnościami w ramach organizacji.

Po skanowania podatności organizację muszą ocenić krytyczność podatności i odpowiedzieć na kluczowe pytania, w tym:

- **Czy mamy do czynienia z realną podatnością?**
- **Jakie skutki dla firmy miałoby wykorzystanie tej podatności?**
- **Pozostałe**

Po pozytywnej weryfikacji podatności i stwierdzeniu potencjalnego ryzyka kluczowe jest ustalenie priorytetów. Priorytety powinny zostać oparte o indywidualny kontekst biznesowy i systemy scoringowe.

Po ustaleniu priorytetu organizacja powinna przejść do etapu naprawy podatności zaczynając od najbardziej krytycznych problemów. Ten punkt wiąże się to z opracowaniem strategicznego planu naprawczego, który może skutkować np. aktualizacją czy rekonfiguracją systemów.

ZARZĄDZANIE DANYMI

Wdrożenie odpowiednich narzędzi i procesów zarządzania danymi powinno zacząć się od przeprowadzenia dokładnej inwentaryzacji danych.

Inwentaryzacja pomoże w doborze odpowiednich środków gwarantujących m.in. ochronę danych osobowych.

W doborze procesów i narzędzi pomoże odpowiedź na kluczowe pytania:

KLUCZOWE PYTANIA

- **Jaki jest poziom krytyczności posiadanych danych?**
- **Jakiego rodzaju informacje zawierają dane?**
- **Kto i do jakich danych musi mieć dostęp?**
- **Czy dane podlegają wymogom regulacyjnym?**
- **Czy dane muszą być utrzymane w prywatności?**
- **Czy dane muszą być przechowywane przez określony czas?**
- **Jak często dochodzi do zmiany danych?**
- **Jak szybko należy odzyskać dane w przypadku kompromitacji?**

STRATEGIA OCHRONY DANYCH

Wspomniane pytania pozwolą dobrać najlepsze rozwiązania. Odpowiedź na pytanie jak często dane ulegają zmianie narzuca częstotliwość tworzenia kopii. Z kolei klasyfikacja danych pod kątem otoczenia regulacyjnego pomoże spełnić najważniejsze wymogi w zakresie compliance.

Kolejnym krokiem w tworzeniu strategii ochrony danych jest określenie polityk archiwizacji oraz przechowywania danych w oparciu o cele biznesowe. Polityka powinna zawierać kryteria oraz okres przechowywania danych czy role i obowiązki właścicieli danych.

Po określeniu polityk organizacje muszą wdrożyć odpowiednie narzędzia i procesy. Narzędzia uzależnione są od konkretnych potrzeb - do najważniejszych narzędzi należą:

- **Narzędzia do tworzenia kopii zapasowych**
- **Narzędzia do szyfrowania**
- **Rozwiązania do ochrony baz danych**
- **Narzędzia do zarządzania cyklem życia danych (ang. Data Lifecycle Management)**
- **Narzędzia klasy Data Loss Prevention (DLP) pozwalające chronić dane w sieci oraz na urządzeniach końcowych**

TWORZENIE KOPII ZAPASOWYCH

Podstawowym narzędziem wymaganym w niemal każdej organizacji są kopie zapasowe, na które składają się m.in. kopie baz danych, środowisk wirtualnych czy poczty. Kopie zapasowe należy zabezpieczyć, najlepiej poprzez odizolowanie od sieci lub poprzez wdrażanie uwierzytelniania wieloskładnikowego i szyfrowania.

Zarządzanie kopiami zapasowymi jest powiązana z obszarem ciągłość działania (zdefiniowanym w NIS 2), dla którego stworzymy dedykowany white paper w kolejnych seriach.

Podobnie jak w przypadku poprzednich punktów proces tworzenia kopii zapasowych warto poprzedzić dokładną inwentaryzacją i mapowaniem danych w celu identyfikacji wszystkich kluczowych danych (w tym danych osobowych), które organizacje przetwarzają i przechowują. Proces ten pomaga w zrozumieniu zakresu wymagań dotyczących tworzenia kopii zapasowych i zapewnieniu odpowiednich środków do zarządzania danymi osobowymi.

Organizacje powinny również ustalić jasne zasady dotyczące przechowywania i usuwania danych z kopii zapasowych. Zasady te powinny być zgodne z wymaganiami wynikającymi z RODO.

Dane z kopii zapasowych, które nie są już wymagane powinny być bezpiecznie usuwane, aby uniknąć niepotrzebnego przechowywania danych i potencjalnego braku zgodności z przepisami.

STRATEGIA W ZAKRESIE KOPII ZAPASOWYCH

Stworzone kopie zapasowe należy regularnie testować, aby zapewnić dostępność i integralność danych. Organizacje powinny przeprowadzać okresowe testy kopii zapasowych, aby weryfikować czy pliki kopii zapasowych są kompletne i mogą być pomyślnie przywrócone.

Ważne jest ponadto regularne przeglądanie i aktualizowanie strategii tworzenia kopii zapasowych, aby dostosować się do zmieniających się potrzeb biznesowych i wymagań prawnych.

Organizacje powinny śledzić wszelkie aktualizacje lub zmiany w RODO czy UoKSC i odpowiednio dostosowywać swoje praktyki w zakresie kopii zapasowych.

Cyprian Gutkowski
Konsultant TrecomSEC

Organizacje podnoszą bezpieczeństwo wdrażając dokument "Zasady korzystania z systemów teleinformatycznych", uwzględniający w swym zakresie nadawanie i odbieranie uprawnień oraz kontrolę dostępu.

Jasno określone zasady korzystania z systemów teleinformatycznych pomagają pracownikom zrozumieć, jakie są ich prawa, obowiązki i odpowiedzialności w kontekście bezpieczeństwa przetwarzanych danych. Poprzez zdefiniowanie, kto i na jakich zasadach ma dostęp do danych, organizacja zmniejsza ryzyko nieautoryzowanego dostępu do krytycznych systemów.

Takie działanie redukuje również ryzyko nieumyślnych błędów i zachowań sprzecznych z politykami wewnętrznymi, które w efekcie mogą prowadzić do incydentów bezpieczeństwa.

Wdrażając i utrzymując dokument "Zasady korzystania z systemów teleinformatycznych", organizacja nie tylko chroni swoje zasoby, ale także buduje kulturę bezpieczeństwa, która jest niezbędna w dzisiejszym dynamicznym i złożonym krajobrazie cyberzagrożeń.

UWIERZYTELNIANIE WIELO-SKŁADNIKOWE

Uwierzytelnianie wieloskładnikowe (ang. MFA) to proces ochrony dostępu do zasobów cyfrowych poprzez używanie dodatkowych składników w procesie weryfikacji tożsamości.

MFA powinno zostać uruchomione we wszystkich dostępnych systemach, aplikacjach i kontach dla użytkowników uprzywilejowanych i administracyjnych oraz dla każdego dostępu do krytycznych i wrażliwych danych.

Proces MFA powinien zostać wdrożony w zasobach krytycznych czy zdalnych aplikacjach.

W oparciu o inwentaryzację aktywów i danych organizacje powinny zidentyfikować wszystkie systemy i aplikacje, do których można uzyskać zdalny dostęp.

PRZYKŁADOWE NARZĘDZIA

Istnieje wiele typów narzędzi do wprowadzenia procesów MFA. Rynek oferuje zarówno narzędzia skoncentrowane stricte na procesie MFA lub integrujące MFA w ramach szerszego obszaru zarządzania tożsamością (ang. Identity Access Management).

Rozwiązania IAM oferują złożone systemy umożliwiające pełną ochronę przed zaawansowanymi zagrożeniami wliczając zagrożenia ze strony wewnętrznych użytkowników systemu.

NARZĘDZIA IAM

Rozwiązania IAM mogą być niezwykle skuteczne w rozbudowanych i złożonych organizacjach, które przy okazji mogą poprawić ochronę w ramach bezpieczeństwa łańcucha dostaw (jeden z wymogów NIS 2). Zaawansowane narzędzia w ramach IAM pomagają w wielu obszarach, w tym:

ROLA NARZĘDZI IAM

- **Ochronie i zarządzaniu danymi kont uprzywilejowanych**
- **Kontroli dostępu do systemów**
- **Ochronie danych uwierzytelniających**
- **Monitorowaniu i kontroli sesji uprzywilejowanych**
- **Analizowaniu aktywności na kontach uprzywilejowanych i ostrzeganiu o szkodliwych działaniach**

Z kolei podstawowe narzędzia oferujące MFA zapewniają uwierzytelnianie wieloskładnikowe na najważniejszych środowiskach (np. aplikacjach).

NAJLEPSZE PRAKTYKI W RAMACH MFA

Poniżej wymieniamy najlepsze praktyki w ramach wdrażania MFA:

- **Wprowadź uwierzytelnianie w oparciu o wcześniej zidentyfikowane ryzyka w ramach polityk ryzyka oraz pozostałe kluczowe czynniki (jak np. krytyczność urządzenia)**
- **Wdróż uwierzytelnianie i szyfrowanie kanałów dla wszystkich kont administracyjnych**
- **Wprowadź usługę MFA dla wszystkich zdalnych logowań do sieci firmowej**
- **Wymagaj MFA dla najbardziej krytycznych i wrażliwych danych lub systemów**

Wdrożenie programu podnoszenia świadomości cyberbezpieczeństwa

WPROWADZENIE

Wdrożenie szkoleń z zakresu cyberbezpieczeństwo jest powiązane z wdrożeniem kompleksowego programu podnoszenia świadomości cyberbezpieczeństwa.

Tworzenie programu warto zacząć od zdefiniowania kto i do jakiego stopnia powinien podlegać programowi. Zupełnie inną wiedzę powinien posiadać pracownik IT, osoba pracująca blisko z klientem czy członek zespołu compliance.

CIS definiuje cztery kluczowe etapy w ramach tworzenia i egzekwowania efektywnego programu wspierającego świadomość w ramach cyberbezpieczeństwa:

1 OCENA METOD DOTARCIA DO PRACOWNIKA

Zgromadź informacje na temat najlepszych metod dotarcia do Twoich pracowników:

Kluczowe pytania

- jaki kanał dotarcia wybrać (np. szkolenia online czy stacjonarne)?
- czy korzystać z zewnętrznych narzędzi czy wewnętrznie opracowanych materiałów?

2 STWORZENIE PROGRAMU

Stwórz program szkoleniowy dla swojej organizacji obejmujący inwestycje w narzędzia lub stworzenie dedykowanych materiałów edukacyjnych:

Kluczowe pytania

- jak często przeprowadzać szkolenia?

3 EDUKUJ

Dostarcz treści szkoleniowe dotyczące cyberbezpieczeństwa pracownikom organizacji:

Kluczowe pytania

- Które zagadnienia w ramach cyberbezpieczeństwa powinny znaleźć się w materiałach?

4 WERYFIKUJ

Upewnij się, że zastosowane metody przynoszą korzyści i spełniają cele:

Kluczowe pytania

- Jakie mechanizmy wdrożyć w celu kontroli ukończenia szkoleń? (np. testy phishingowe)
- Jak często aktualizować materiały?

ZAKRES SZKOLEŃ

Zakres szkoleń będzie uzależniony od indywidualnych potrzeb oraz charakterystyki organizacji (środowisk, ryzyk itd.). Niezależnie od indywidualnych potrzeb, organizacje powinny uwzględnić następujące zagadnienia:

- **Rozpoznanie i zgłaszanie ataków phishingowych**
- **Bezpieczeństwo w pracy zdalnej**
- **Bezpieczne korzystanie z nośników danych i zarządzanie danymi firmowymi**
- **Tworzenie silnych haseł**
- **Zapewnienie bezpieczeństwa fizycznego**
- **Bezpieczeństwo mobilne**
- **Bezpieczeństwo w chmurze i aplikacjach**
- **Inżynieria społeczna**
- **Reagowanie na incydenty**

Artur Markiewicz
Konsultant Trecom

Każdy z nas jest użytkownikiem.
W zakresie edukacji użytkownika musimy wiedzieć jak dokładnie reagować w sytuacjach, kiedy mamy podejrzenia oszustwa.

Dla każdej próby ataku teleinformatycznego, oszustwa, wyłudzenia istnieją osobne czerwone flagi, które użytkownik powinien znać. Dzięki temu będzie lepiej wiedział na co, jak i kiedy reagować.

Dla osób odpowiedzialnych za podnoszenie poziomu cyberbezpieczeństwa ważne jest by wiedzieć co mają chronić oraz jaka jest krytyczność danych i systemów w organizacji. Dzięki temu przedstawimy najbardziej optymalne środki techniczne, procesowe, na które zdecyduje najwyższe kierownictwo.

Świadomość zagrożeń czy sposobów reagowania jest istotna dla każdego pracownika w organizacji.

Zebranie tego wszystkiego pozwala na projektowe podejście do wdrożenia programu podnoszenia świadomości cyberbezpieczeństwa.

Edukacja jest najtańszym sposobem podnoszenia poziomu cyberbezpieczeństwa jednocześnie mając największy wpływ.

PRZYKŁAD DOBORU TECHNIK SZKOLENIOWYCH DLA RÓŻNYCH ODBIORCÓW

W 2023 roku ENISA opublikowała zestaw narzędzi, które sugerują gotowe techniki w zakresie tworzenia programów do podnoszenia świadomości cyberbezpieczeństwa. Na dole prezentujemy metody organizacji szkoleń w podziale na grupy odbiorców.

Grupa pracowników	Kluczowe techniki i kanały dotarcia
MARKETING, HR, OPERACJE, R&D ORAZ POZOSTALI PRACOWNICY (NIEZDEFINIOWANI NIŻEJ)	• Gry online oraz quizy • Materiały video • Grupy dyskusyjne • Zestawy wspomagające budowanie świadomości (infografiki, plakaty itd.)
DZIAŁY FINANSOWE, ZAKUPOWE, DYREKTORZY I MENADŻEROWIE POSZCZEGÓLNYCH JEDNOSTEK	• Newslettery • Zestawy wspomagające budowanie świadomości (infografiki, plakaty itd.) • Materiały video • Kursy online • Konferencje • Webinary
DZIAŁY ICT ORAZ EKSPERCI OD CYBER	• Kursy online • Materiały video • Certyfikacje i dyplomy • Webinary • Ćwiczenia techniczne

HARMONOGRAM PROGRAMU

ENISA przedstawiła również propozycję harmonogramu programu. Oczywiście sama długość programu powinna być dostosowana do indywidualnych potrzeb organizacji.

Cel	Implementacja
Podniesienie świadomości na temat zagrożeń związanych z phishingiem • Szkolenia • Kampanie symulacji phishingu	6 mesięcy
Promocja edukacji i kultury cyberbezpieczeństwa • Ogólne szkolenia z cyberbezpieczeństwa • Szkolenia z procesu raportowania w przypadku wystąpienia incydentu	12 miesięcy
Poprawa reakcji na incydent • Szkolenia dla działu ICT • Szkolenie powinno zostać połączone z praktycznymi ćwiczeniami technicznymi	6 miesięcy

IMPLEMENTACJA PROGRAMU

Moment organizacji szkoleń i typ szkolenia powinien być podzielony na trzy tryby:

- Szkolenia organizowane w momencie dołączenia pracownika do organizacji (szkolenie powinno być częścią procesu wprowadzającego pracownika do organizacji)
- Szkolenie po wystąpieniu incydentu (szkolenie po wystąpieniu incydentu to dobry moment na dodatkowe wskazanie procedur, ról i odpowiedzialności w ramach organizacji)
- Regularne szkolenia w ciągu roku

Cyberochrona i cyberhigiena - checklista

1. OGÓLNE WYMOGI

- CZY POSIADASZ ZINWENTARYZOWANĄ BAZĘ POSIADANYCH ZASOBÓW?
- CZY STWORZYŁEŚ PLAN DO ZARZĄDZANIA KAŻDYM ZIDENTYFIKOWANYM RYZYKIEM?
- CZY REGULARNIE AKTUALIZUJESZ I SPRAWDZASZ SKUTECZNOŚĆ POSIADANYCH POLITYK I NARZĘDZI?
- CZY PROWADZISZ REGULARNE SESJE SZKOLENIOWE W ZAKRESIE BEZPIECZEŃSTWA I POSIADANYCH NARZĘDZI DLA PRACOWNIKÓW ORGANIZACJI?
- CZY WDROŻYŁEŚ PROGRAM DO PODNOSZENIA ŚWIADOMOŚCI BEZPIECZEŃSTWA M.IN. NA TEMAT NAJWAŻNIEJSZYCH ZAGROŻEŃ (NP. PHISHINGU)?
- CZY WDROŻYŁEŚ PROCEDURY I NARZĘDZIA DO OCHRONY SIECI?

- CZY WDROŻYŁEŚ PROCEDURY W ZAKRESIE OCENY ZAGROŻEŃ BEZPIECZEŃSTWA DOSTAWCÓW ZEWNĘTRZNYCH?
- CZY WDROŻYŁEŚ PROCESY I NARZĘDZIA DO OCHRONY POCZTY I APLIKACJI WEBOWYCH?

2. ZARZĄDZANIE PODATNOŚCIAMI

- CZY NADAJESZ PRIORYTETY PODATNOŚCIOM I USUWASZ JE ZGODNIE Z WCZEŚNIEJ OKREŚLONYM PRIORYTETEM?
- CZY REGULARNIE SKANUJESZ INFRASTRUKTURĘ I SYSTEMY POD KĄTEM PODATNOŚCI?

3. ZARZĄDZANIA KOPIAMI ZAPASOWYMI

- CZY REGULARNIE TWORZYSZ KOPIE ZAPASOWE DLA KRYTYCZNYCH SYSTEMÓW?
- CZY KOPIE ZAPASOWE DANYCH SĄ REGULARNIE TESTOWANE?

4. UWIERZYTELNIANIE WIELOSKŁANIKOWE

- CZY WDROŻYŁEŚ UWIERZYTELNIANIE WIELOSKŁADNIKOWE DLA SYSTEMÓW KRYTYCZNYCH I KONT UPRZYWILEJOWANYCH?

5. ZARZĄDZANIE INCYDENTAMI

- CZY WDROŻYŁEŚ PLAN REAGOWANIA NA INCYDENTY?
- CZY POSIADASZ PRZESZKOLONY ZESPÓŁ DO REAGOWANIA NA INCYDENTY?
- CZY POSIADASZ SYSTEMY DO ZARZĄDZANIA INCYDENTAMI ZBIERAJĄCE LOGI Z WSZYSTKICH ŚRODOWISK?

6. ŚWIADOMOŚĆ I SZKOLENIA Z ZAKRESU CYBERBEZPIECZEŃSTWA

- CZY TWOI KLUCZOWI PRACOWNICY PRZECHODZĄ REGULARNE SZKOLENIA Z ZAKRESU CYBERBEZPIECZEŃSTWA?
- CZY WDROŻYŁEŚ PROCES WERYFIKACJI TOŻSAMOŚCI KLIENTÓW PRZED UDOSTĘPNIENIEM POUFNYCH INFORMACJI?
- CZY TWOI PRACOWNICY PRACUJĄCY BLISKO KLIENTÓW POSIADAJĄ PODSTAWOWĄ WIEDZĘ NA TEMAT CYBERBEZPIECZEŃSTWA (NP. JAK POSTĘPOWAĆ W PRZYPADKU ZAGROŻEŃ)?

5. ZARZĄDZANIE DANYMI

- CZY WDROŻYŁEŚ POLITYKĘ PRZECHOWYWANIA I OCHRONY DANYCH?
- CZY POLITYKA JEST ZGODNA Z BRANŻOWYMI REGULACJAMI ORAZ POZOSTAŁYMI WYMOGAMI?
- CZY ZIDENTYFIKOWAŁEŚ I SKLASYFIKOWAŁEŚ SWOJE KLUCZOWE WRAŻLIWE DANE I OGRANICZYŁEŚ DO NICH DOSTĘP?

- CZY KLUCZOWE DANE SĄ SZYFROWANE ZARÓWNO PODCZAS PRZESYŁANIA, JAK I PRZECHOWYWANIA?
- CZY REJESTRUJESZ I MONITORUJESZ DOSTĘP DO DANYCH?

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)

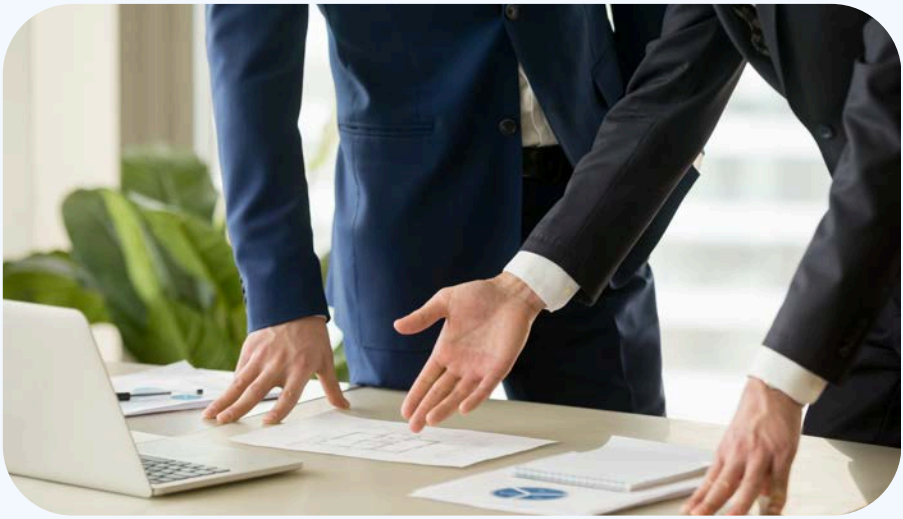
TRECOM SOC

- 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 Z NIS 2

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