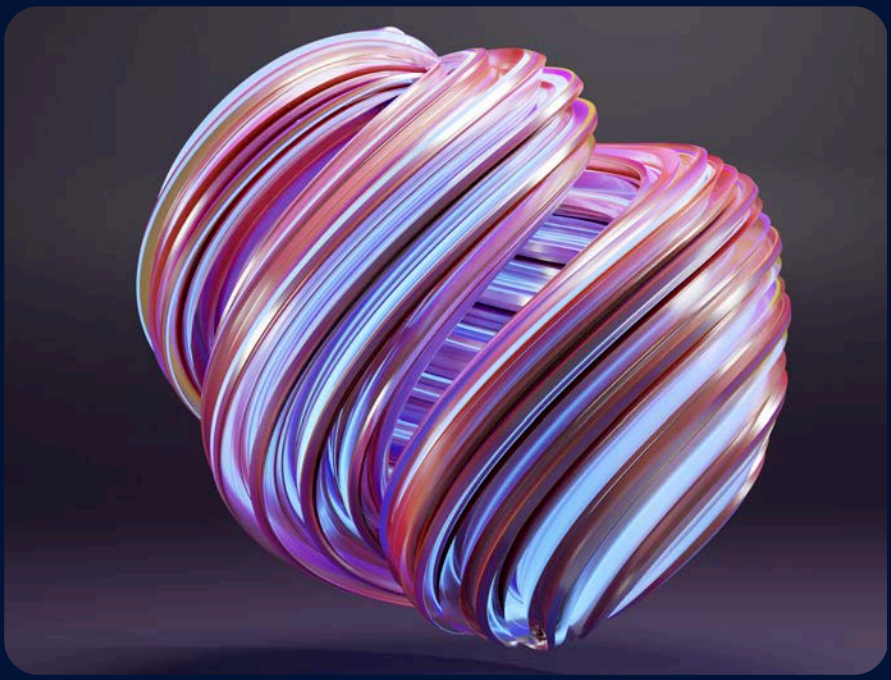
trecom

WHITE PAPER

Bezpieczeństwo Łańcucha Dostaw W Kontekście NIS 2



Spis treści

Wprowadzenie do NIS 2

KONTEKST

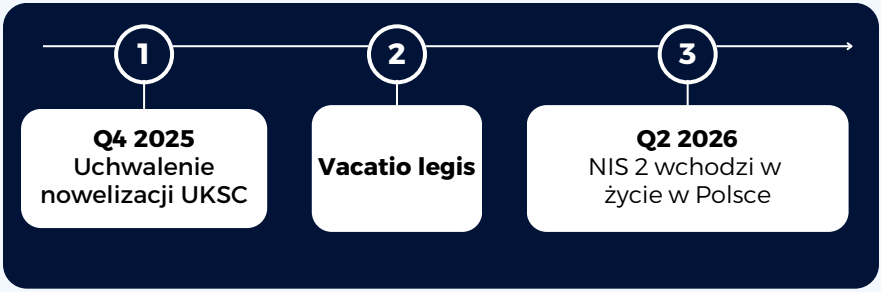
NIS 2 stanowi znaczący krok w poprawie ochrony i odporności przed cyberzagrożeniami organizacji w UE.

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 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?

White paper ma pomóc przygotować się organizacjom na wymogi NIS 2 dotyczące bezpieczeństwa łańcucha dostaw. White paper jest częścią serii na temat NIS 2, którą będziemy kontynuować w kolejnych tygodniach.

TREŚĆ WHITE PAPER

- Definicja elementów łańcucha dostaw
- Ryzyka i kierunki ataków w ramach łańcucha dostaw
- Zabezpieczenie łańcucha dostaw od strony procesowej
- Narzędzia wykorzystywane w zarządzaniu ryzykiem łańcucha dostaw
- Przykłady rozwiązań do zabezpieczania łańcucha dostaw

O AUTORACH WHITE PAPER

Piotr Kępski
TrecomSEC
Analityk systemów bezpieczeństwa

Mirosław Maj
TrecomSEC
Dyrektor

Cyprian Gutkowski
TrecomSEC
Konsultant

Marcin Fronczak
TrecomSEC
Konsultant

Zapraszamy do lektury

Bezpieczeństwo łańcucha dostaw

WPROWADZENIE DO BEZPIECZEŃSTWA ŁAŃCUCHA DOSTAW

NIS 2 wymusza na firmach wprowadzenie środków technologicznych, procesowych i operacyjnych umożliwiających zabezpieczenie łańcucha dostaw.

Sam łańcuch dostaw jest niezwykle złożonym zagadnieniem wymagającym indywidualnej analizy potrzeb i zależności na wielu warstwach, w tym:

- **zależności czysto biznesowych**
- **zależności na warstwie kodu**
- **zależności operacyjnych**
- **indywidualnego kontekstu**

Zarządzanie łańcuchem dostaw to nie tylko wprowadzenie cyklicznej oceny i szacowania ryzyka związanego z łańcuchem dostaw czy inwestycje na warstwie technologicznej, ale również:

- **Tworzenie standardowych wymagań oraz umów dla procesu pozyskiwania partnerów i dostawców**
- **Wdrożenie wytycznych i szablonów do oceny ryzyka partnerów i dostawców**
- **Szacowanie zgodności partnerów i dostawców z zobowiązaniami wynikającymi z umów**
- **Stworzenie, planowanie i testowanie planów reakcji na incydenty cyberbezpieczeństwa u dostawców i partnerów**
- **I wiele innych**

Problem braku odpowiedniej ochrony łańcucha dostaw

STATYSTYKI NA TEMAT BEZPIECZEŃSTWA ŁAŃCUCHA DOSTAW

Wiele statystyk pokazuje znaczące braki na warstwie zabezpieczenia łańcucha dostaw. Najlepiej pokazują to statystyki ENISA opracowane na podstawie ankiet z dostawcami usług cyfrowych oraz usług krytycznych (1080 podmiotów) w UE w 2022:

47%

Podmiotów alokuje budżet na bezpieczeństwo łańcucha dostaw

76%

Organizacji nie posiada zdefiniowanych ról w ramach łańcucha dostaw

86%

Podmiotów wdrożyło polityki w zakresie bezpieczeństwa łańcucha dostaw

61%

Respondentów zbiera certyfikaty z zakresu bezpieczeństwa od partnerów

46%

Podmiotów zarządza krytycznymi podatnościami w ciągu miesiąca

43%

Organizacji korzysta z agencji ratingowych w ocenie partnerów

Wyzwania w zabezpieczaniu łańcucha dostaw

WYZWANIA W ZABEZPIECZANIU ŁAŃCUCHA DOSTAW

Wyzwania związane z brakiem odpowiednich środków zabezpieczających wynikają częściowo z braku uwzględniania obszaru partnerów zewnętrznych w cyberbezpieczeństwie.

Nie jest to jednak jedynie obszar cyberbezpieczeństwa ponieważ organizacje powinny systemowo podejść do zarządzania łańcuchem dostaw na poziomie całej firmy i analizować ryzyko, zarządzać relacjami z dostawcami czy podatnościami. Firmy powinny również usystematyzować sam proces współpracy z dostawcami.

PROCENT FIRM POSIADAJĄCYCH POLITYKI W ZAKRESIE BEZPIECZEŃSTWA ŁAŃCUCHA DOSTAW W UE (ENISA)

Elementy łańcucha dostaw

CO MOŻE WEJŚĆ W SKŁAD ŁAŃCUCHA DOSTAW?

Łańcuch dostaw organizacji różni się w zależności od skali organizacji, branży czy indywidualnych charakterystyk organizacji. Wśród najczęściej powtarzających się elementów wyróżniamy:

- **Dostawców komponentów fizycznych stosowanych w systemach informatycznych (np. komputerów, serwerów, urządzeń sieciowych czy pozostałych specjalistycznych urządzeń)**
- **Dostawców wszelkiego rodzaju oprogramowania**
- **Dostawców usług w chmurze**
- **Dostawców usług zewnętrznych, w tym dostawców usług płatności, analityki danych czy systemów do zarządzania relacjami z klientami**
- **Partnerów logistycznych**
- **Podmioty odpowiedzialne za rozliczenia**
- **Pozostałe podmioty zaangażowane w produkcję fizycznych dóbr, w tym komponentów elektronicznych**

W ostatnich pięciu latach byliśmy świadkami wielu ataków na łańcuchy dostaw. Warto wspomnieć między innymi o atakach na SolarWinds czy Ledger.

Niezwykle pouczającym case study pod katem konsekwencji biznesowych i komplikacji operacyjnych jest atak na UnitedHealth Group.

Konsekwencje ataku na UnitedHealth Group

KONTEKST ATAKU

W lutym 2024 roku UnitedHealth Group, jedna z największych firm z sektora opieki zdrowotnej w USA (>350 miliardów dolarów przychodu) padła ofiarą ataku ransomware przez grupę BlackCat.

Wpływ ataku w sprawozdaniu za pierwszy kwartał 2024 został oszacowany przez zarząd spółki na 872 milionów dolarów choć całkowity wpływ w 2024 jest szacowany na od 1.3 mld dolarów do 1.6 mld dolarów.

Atak był ukierunkowany na systemy rozliczeniowe i płatnicze jednej ze spółek zależnych UnitedHealth Group przyczyniając się do znaczącego spadku ceny giełdowej (z ok. 500 dolarów do ok. 450 dolarów).

Zmiana ceny akcji UnitedHealth Group po ataku - Źródło CNBC

PROCES REAGOWANIA NA INCYDENT

ZNACZENIE ŁAŃCUCHA DOSTAW W ATAKU NA UNITEDHEALTH GROUP

Change Healthcare (spółka zależna UnitedHealth Group, która była celem ataku) jest kluczowym podmiotem działającym w ramach rozliczeń na rynku ochrony zdrowia. Change Healthcare łączy pacjentów, placówki medyczne oraz pozostałe podmioty w ramach rynku ochrony zdrowia procesując rocznie 15 mld transakcji docierając do ponad 30% pacjentów w USA.

Atak wiązał się z wyłączeniem ponad 100 usług i ogromnym chaosem w szpitalach czy aptekach. Część podmiotów nie miała dostępu do środków finansowych przez wiele dni, a niektóre apteki nie mogły realizować recept.

Ponadto UnitedHealth Group musiało wyłożyć ponad 6 mld dolarów w formie pożyczek w celu wsparcia dostawców usług dotkniętych incydentem. Wspomniany atak pokazuje jakie konsekwencje niesie za sobą atak na dostawcę usług krytycznych osadzonych w ramach szerszego łańcucha dostaw.

Ryzyka i kierunki ataków w ramach łańcucha dostaw

WPROWADZENIE

Ryzyka związane funkcjonowaniem w łańcuchu dostaw kojarzone są często z atakami na poziomie “upstream” czyli np. zainfekowanie systemu, który w konsekwencji przekłada się na użytkownika końcowego (np. za sprawą pobrania konkretnego pliku z systemu). W praktyce możliwości pośredniego ataku na organizację są niezwykle złożone.

Jednym z przykładów obszaru ryzyka są różnego rodzaju manipulacje kodem, który jest wykorzystywany w środowiskach aplikacyjnych (np. na poziomie repozytorium dostępnego w open-source).

Kolejnym popularny atakiem są ataki na infrastrukturę CI/CD, która służy do systemowego testowania i wdrażania zmian na poziomie oprogramowania.

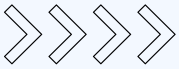
ATAKI UKIERUNKOWANE NA PARTNERA W RAMACH ŁAŃCUCHA DOSTAW

Kluczowym obszarem łańcucha dostaw są ataki na konkretnego partnera biznesowego i wykorzystanie wspomnianego ataku jako środek do kompromitacji pozostałych podmiotów w ramach łańcucha czy samego końcowego klienta.

W tym przypadku mówimy o kilku obszarach ataków, w tym np. ataków ukierunkowanych w jedno lub więcej z zasobów czy procesy biznesowe tak żeby uzyskać dostęp do krytycznego systemu lub wywołać inne szkodliwe skutki.

ATAKI NA WARSTWĘ PROGRAMOWĄ

Jednym z kluczowych wyzwań w zakresie zabezpieczania warstwy programowej jest stopień korzystania z rozwiązań open-source. Kod open-source jest podstawą w efektywnym tworzeniu produktów cyfrowych.



Według raportu "Open Source Security and Risk Analysis" z 2020 roku, prawie 99% baz kodu zawiera przynajmniej jeden komponent open source.

Oprogramowanie jest często udostępniane na różnego rodzaju serwisy jak GitHub bez spełnienia odpowiednich wymogów z zakresu cyberbezpieczeństwa. Celem cyberprzestępców są m.in. menadżery pakietów (jak np. n.p.m. w przypadku JavaScript). Cyberprzestępcy modyfikują oprogramowanie dodając złośliwe pakiety.

Cyberprzestępcy atakują firmy na trzech poziomach:

- **Etap pozyskiwania i tworzenia kodu, w tym tworzenia dedykowanego kodu, korzystania z kodu dostępnego open-source, działań z kontenerami itd.**
- **Etap przekształcania kodu źródłowego w postać gotową do wdrożenia, w tym stosowanie narzędzi CI/CD w celu testowania i wdrażania zmian na warstwie programowej**
- **Konsolidacja wszystkich elementów oprogramowania i zależności w formę gotową do wdrożenia**

PRZYKŁADY ZAGROŻEŃ

Wspomniany podział otwiera wiele możliwości dla cyberprzestępców, w tym:

- **Ataki na platformę, na której zbudowano oprogramowanie**
- **Kompromitację serwerów, na którym znajduje się właściwe oprogramowanie**
- **Dodawanie zależności do bazy kodu**
- **Dodawanie różnego rodzaju podatności do oprogramowania**
- **Pozostałe**

Zabezpieczenie łańcucha dostaw od strony procesowej

WPROWADZANIE Poniżej przedstawiamy podsumowanie oraz szczegółowy opis najważniejszych obszarów w ramach systemowego zabezpieczenia łańcucha dostaw.

1 IDENTYFIKACJA KLUCZOWYCH ELEMENTÓW ŁAŃCUCHA DOSTAW

2 ANALIZA ZALEŻNOŚCI W RAMACH ŁAŃCUCHA DOSTAW

3 IDENTYFIKACJA KRYTYCZNYCH PROCESÓW BIZNESOWYCH

4 WDROŻENIE DEDYKOWANYCH PROCEDUR DLA WSZYSTKICH PARTNERÓW

5 SYSTEMOWA ANALIZA RYZYKA PARTNERÓW

6 SZACOWANIE RYZYKA WYBRANYCH PARTNERÓW

7 WDROŻENIE ROZWIĄZAŃ OGRANICZAJĄCYCH RYZYKO

8 AKTYWNY MONITORING

1. IDENTYFIKACJA KLUCZOWYCH ELEMENTÓW ŁAŃCUCHA DOSTAW

Proces identyfikacji dostawców czy partnerów działających w ramach łańcucha dostaw łączy kompetencje techniczne oraz biznesowe. Z jednej strony działy odpowiedzialne za cyberbezpieczeństwo oraz IT muszą zidentyfikować powiązania na poziomie środowiska aplikacyjnego, IoT czy OT.

Z drugiej strony działy biznesowe czy operacyjne muszą zidentyfikować kluczowych dostawców m.in. maszyn, komponentów, usług krytycznych oraz pozostałych elementów uzależnionych od modelu biznesowego.

Poza warstwą fizyczną niezwykle ważna jest inwentaryzacja oprogramowania, w tym zebranie dokumentacji wykorzystywanego oprogramowania oraz pozostałych kluczowych informacji, w tym:

- **Powiązanych procesów**
- **“Właścicieli” konkretnego oprogramowania oraz osób mających dostęp do oprogramowania**
- **Lokalizacji oprogramowania**
- **Pozostałych kluczowych informacji**

2. ANALIZA ZALEŻNOŚCI W RAMACH ŁAŃCUCHA DOSTAW

Po identyfikacji partnerów powinniśmy przejść do analizy powiązań i procesów w ramach współpracy z partnerami.

Na początku warto zidentyfikować komórki w ramach organizacji odpowiedzialne za współpracę z konkretnym dostawcą. Chodzi o działy technologiczne, zakupowe, prawne, logistyczne czy finansowe.

Warto zrozumieć sposób działania indywidualnych procesów, w tym informacji o rodzaju współpracy, częstotliwości współpracy czy stopień wymiany informacji.

Należy zidentyfikować osoby odpowiedziane za współprace, poziom indywidualnych odpowiedzialności oraz role jakie odgrywa zespół cyberbezpieczeństwa.

Kolejnym ważnym zagadnieniem jest regularna obserwacja zmian w działalności partnera. Wszelkie zmiany organizacyjne czy biznesowe powinny zostać przeanalizowane z perspektywy bezpieczeństwa, w tym:

- **Ekspansja zagraniczna czy współpraca z podmiotami z krajów wysokiego ryzyka**
- **Zmiany na poziomie właścicielskim organizacji**
- **Znaczące zmiany w modelu biznesowym**
- **Świadczenie nowego rodzaju usług**
- **Pozostałe zmiany**

3. IDENTYFIKACJA KRYTYCZNYCH PROCESÓW BIZNESOWYCH

Szczególną uwagę należy objąć krytyczne procesy. Rozważania o krytycznych procesach i zasobach warto zacząć od odpowiedzi na poniższe pytania.

- **Czy dany proces lub zasób stanowi “single point of failure”?**
- **Czy proces jest powiązany z przechowywaniem wrażliwych danych?**
- **Kto posiada dostęp do procesu?**
- **Jakie konsekwencje niesie za sobą awaria konkretnego procesu?**
- **Jakie operacje zostaną zakłócone w przypadku wystąpienia awarii?**

4. WDROŻENIE DEDYKOWANYCH PROCEDUR DLA PARTNERÓW

Warto również wdrożyć dedykowane procedury dla partnerów. Niektórzy partnerzy mogą być bardziej krytyczni od innych stąd warto rozważyć stworzenie dla nich dedykowanych procedur, obok standardowej "polityki stron trzecich". Decyzja o krytyczności powinna opierać się na podstawie wielu czynników, w tym:

- **Poziomu dostępu partnera do systemów organizacji**
- **Ryzyka ataku na partnera (sektor, historia ataków, osadzenie w ramach szerszego łańcucha dostaw, krytyczność usługi itd.)**
- **Poziomu dostępu do danych wrażliwych czy własności intelektualnej**
- **Znaczenia biznesowego partnera (wpływ na klientów, udział w przychodach itd.)**
- **Skali konsekwencji z tytułu komplikacji organizacyjnych i biznesowych**

5. SYSTEMOWA ANALIZA RYZYKA PARTNERÓW

Systemową analizę partnerów pod kątem ryzyka i stopnia zabezpieczeń należy wdrożyć na wczesnym etapie (najlepiej przed formalną współpracą z partnerem).

Przed współpracą z partnerem należy zweryfikować certyfikację czy wdrożone środki z zakresu cyberbezpieczeństwa (np. wysyłając specjalny kwestionariusz - szczegóły w dalszej części materiału).

Wspomniane wymogi powinny zostać opracowane zgodnie z indywidualnymi potrzebami organizacji. W procesie definiowania wymogów warto zaangażować kluczowych interesariuszy (zarząd, jak i stronę techniczną, operacyjną czy biznesową organizacji).

Organizacje powinny komunikować partnerom konieczność spełnienia minimalnych wymogów z zakresu bezpieczeństwa oraz weryfikować zgodność z podstawowymi wymogami.

Spełnienie podstawowych wymogów z zakresu bezpieczeństwa powinno zostać zdefiniowane jako jeden z wymogów w ramach współpracy z partnerem (oraz jako jeden z kryteriów oceny partnera).

KWESTIONARIUSZ DO ANALIZY RYZYKA PARTNERA

Efektywną praktyką z perspektywy zarządzania łańcuchem dostaw jest indywidualna analiza partnerów w oparciu o kwestionariusz. Kwestionariusz umożliwia indywidualną ocenę ryzyk potencjalnego partnera.

Kwestionariusz powinien zostać wypełniony przez partnera, jak i organizację analizującą ryzyka partnera. Na dole prezentujemy przykłady informacji z kwestionariusza.

WYBRANE ELEMENTY KWESTIONARIUSZA DO ANALIZY RYZYKA PARTNERA

PODSTAWOWE DANE O PARTNERZE

- Nazwa partnera
- Siedziba
- Kontakt do partnera
- Pozostałe kluczowe informacje o partnerze

PODSTAWOWE ŚRODKI ZABEZPIECZAJĄCE

- Posiadanie podstawowych technologii zabezpieczających (firewalle itd.)
- Wdrożenie procedur zapobiegających nieautoryzowanemu korzystaniu z systemów
- Implementacja technologii do identyfikacji nieautoryzowanego dostępu czy modyfikacji danych
- Pozostałe

ZARZĄDZANIE PODATNOŚCIAMI	• Ocena, priorytetyzacja i zarządzanie podatnościami • Analiza podatności w celu identyfikacji głównej przyczyny
BEZPIECZEŃSTWO INFORMACJI	• Zgodność z branżowymi standardami czy ogólnymi standardami w zakresie bezpieczeństwa informacji (jak ISO 27001 czy SOC 2) • Posiadanie wewnętrznych polityk umożliwiających zarządzanie informacjami
BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW	• Posiadanie polityk do walidacji i kontroli jakości wśród dostawców • Posiadanie polityk do zarządzania ryzykiem w ramach łańcucha dostaw
BEZPIECZEŃSTWO OBSZARU HR	• Wdrożenie programu poprawy świadomości z zakresu cyberbezpieczeństwa • Posiadanie polityk do zarządzania bezpieczeństwem pracowników
POZOSTAŁE	• Wdrożenie programu w zakresie governance • Ochrona IP oraz kluczowych aktywów • Wdrożenie ochrony kluczowych procesów (np. produkcji czy dystrybucji)

6. SZACOWANIE RYZYKA WYBRANYCH PARTNERÓW

Na podstawie zebranych wcześniej informacji można przejść do samego szacowania ryzyka wybranych partnerów.

Samo szacowanie ryzyka powinno opierać się na podstawie indywidualnego systemu scoringowego. Na dole prezentujemy kluczowe czynniki, które mogą okazać się pomocne w ocenie ryzyka:

- **Krytyczność powiązanych procesów biznesowych i zasobów**
- **Znaczenie partnera dla biznesu**
- **Reputacja partnera**
- **Zgodność z najlepszymi praktykami z zakresu bezpieczeństwa partnera oraz stopień wdrożonych zabezpieczeń**
- **Pozostałe czynniki**

7. WDROŻENIE ROZWIĄZAŃ OGRANICZAJĄCYCH RYZYKO

Wdrożenie środków umożliwiających ograniczenie ryzyka uzależnione jest od indywidualnych potrzeb i powinno być częścią skoordynowanego programu do zarządzania ryzykiem łańcucha dostaw. Na dole prezentujemy listę środków umożliwiających ograniczenie ryzyk związanych z funkcjonowaniem w ramach łańcucha dostaw.

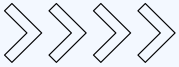
- **Regularne audyty**
- **Kwestionariusze do analizy ryzyka**
- **Standaryzacja procesu dokumentacji**
- **Wdrożenie rozwiązań do zarządzania dostępem i tożsamością**
- **Procedury w zakresie quality assurance**
- **Wdrożenie efektywnych standardów i procedur dotyczących bezpieczeństwa informacji**
- **Wdrożenie środków z zakresu bezpieczeństwa fizycznego**
- **Pozostałe**

W kolejnym rozdziale przedstawimy, krótką charakterystykę wybranych narzędzi.

8. AKTYWNY MONITORING I OCENA RYZYKA PARTNERÓW

Ryzyko w łańcuchu dostaw powinno być na bieżąco monitorowane. Efektywnym rozwiązaniem z punktu widzenia ograniczenia ryzyka jest stworzenie wewnętrznego zespołu odpowiedzialnego za bieżące monitorowanie i zarządzanie ryzykiem w łańcuchu dostaw.

Zespół powinien składać się zarówno z ekspertów z zakresu cyberbezpieczeństwa, jak i ekspertów z pozostałych obszarów (np. zakupowego, ale również ekspertów z pozostałych obszarów mających styczność z partnerami).



Warto zastanowić się również nad stworzeniem stanowiska w ramach organizacji wyłącznie dedykowanego obszarowi bezpieczeństwa łańcucha dostaw (np. dyrektora ds. bezpieczeństwa łańcucha dostaw)

Osoba kierująca działaniami w zakresie bezpieczeństwa łańcucha dostaw powinna mieć całkowitą odpowiedzialność za zarządzanie bezpieczeństwem łańcucha dostaw oraz stworzenie polityk zapewniających wytyczne dla wszystkich działów w ramach organizacji.

Narzędzia wykorzystywane w zarządzaniu ryzykiem łańcucha dostaw

NARZĘDZIA DO ANALIZY RYZYKA

Z punktu widzenia samego ryzyka przydatnym rozwiązaniem mogą okazać się skonsolidowanie narzędzia do analizy partnera, jak i samego procesu onboardingu partnera. Wspomniane narzędzia umożliwiają:

- **Standaryzację procesu wdrażania partnerów do organizacji (on-boarding)**
- **Wdrożenie jednego procesu oceny ryzyka partnerów**
- **Proaktywną analizę partnera pod kątem różnych obszarów ryzyka, takich jak stabilność finansowa czy bezpieczeństwo**
- **Przeprowadzanie wstępnego due diligence dostawcy**
- **Proaktywne monitorowanie działania partnerów i wykrywanie potencjalnych ryzyk w czasie rzeczywistym**
- **Dokumentację i rejestrowanie ryzyk oraz tworzenie raportów na temat partnerów**

Przykłady rozwiązań wspierających zabezpieczenie łańcucha dostaw

WPROWADZENIE

Istnieje wiele rozwiązań, które umożliwią zabezpieczenie konkretnych elementów w ramach łańcucha dostaw.

Z punktu widzenia procesowego niezwykle przydatnym rozwiązaniem mogą okazać się narzędzia klasy Identity and Access Management (IAM), które umożliwiają zdefiniowanie dostępów do poszczególnych systemów organizacji.

Dobra definicja dostępu opierająca się na potrzebach operacyjnych i biznesowych umożliwia ograniczenie powierzchni ataku.

Narzędzia lasy IAM ograniczają również wszelkiego rodzaju wewnętrzne ryzyka kompromitacji.

NARZĘDZIA DO ZABEZPIECZENIA WARSTWY PROGRAMOWEJ

Obszar zabezpieczenia warstwy programowej jest bardzo szeroki natomiast warto wspomnieć o kilku kluczowych grupach rozwiązań:

- **Narzędzia do zarządzania cyklem życia oprogramowania**
- **Narzędzia zabezpieczające pipeliny CI/CD**
- **Narzędzia do ochrony kontenerów**
- **Narzędzia do zarządzania dostępami do oprogramowania**
- **Narzędzia do monitorowania, skanowania czy analizy podatności w obszarze SBOM (Software Bill of Materials)**

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)

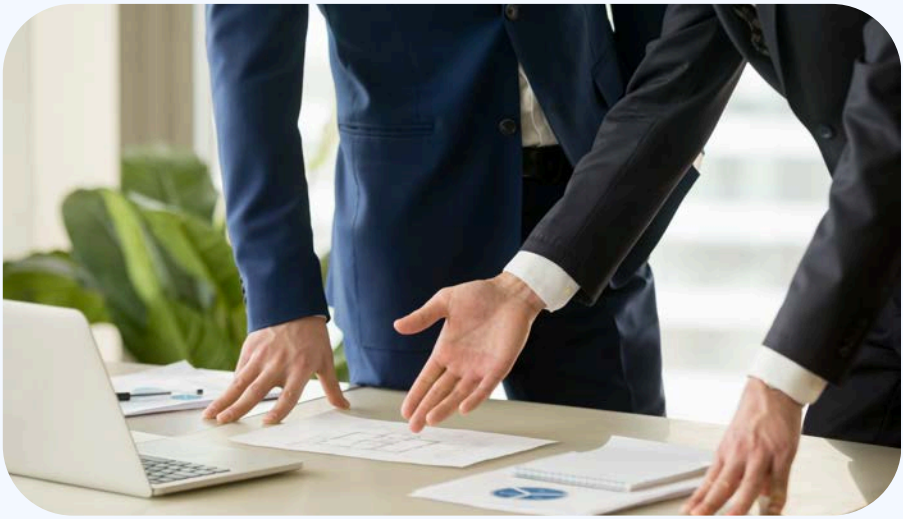
TRECOM SOC

- 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.