Dyrektywa NIS2: Przygotowanie do zgodności z Sekoia

Pod koniec 2022 roku Unia Europejska przyjęła kluczową dyrektywę, której celem jest ochrona wszystkich najważniejszych sektorów gospodarki europejskiej przed zagrożeniami cybernetycznymi. Dyrektywa (UE) 2022/2555, znana jako NIS2 (Network and Information Security 2), wprowadza zestaw środków mających na celu podniesienie poziomu bezpieczeństwa sieci i systemów IT w UE. Kraje członkowskie zostały zobligowane do adaptacji rozporządzenia w prawie lokalnym, co wprowadzi szereg nowych wymogów dla organizacji z ujętych w nim sektorów.

Z uwagi na konieczność szybkiego planowania, wdrożenia i testowania nowych narzędzi, strategii oraz procedur, kluczowe jest, aby działać natychmiast. Niniejszy przewodnik przedstawia najważniejsze zmiany wynikające z NIS2 oraz pokazuje, jak Sekoia może wesprzeć Twoją organizację w spełnieniu wymagań tej dyrektywy.

Trzy filary NIS2

Obowiązki państw członkowskich	Zarządzanie ryzykiem	Współpraca i wymiana informacji
Władze krajowe	Odpowiedzialność kadry kierowniczej	Grupa współpracy
Strategie krajowe	Środki zarządzania ryzykiem dla kluczowych i ważnych podmiotów	Sieć CSIRT
Skoordynowane ujawnianie słabych punktów (CVD)	Powiadomienie o incydencie w krótkim czasie	Sieć CyCLONe
Zarządzanie Kryzysowe		Unijna baza danych znanych luk w zabezpieczeniach
		Wzajemne oceny

Drugi filar dotyczy głównie firm prywatnych i organizacji publicznych

ZAKRES ZASTOSOWANIA

Aby zapewnić ciągłość działania kluczowych usług i stabilność europejskiej gospodarki, dyrektywa NIS2 rozszerza zakres ochrony na dodatkowe sektory, których sieć oraz systemy teleinformatyczne muszą być zabezpieczone przed potencjalnymi zagrożeniami. Oprócz wcześniej chronionych branż, nowe przepisy obejmują teraz m.in. sektor gospodarki ściekowej, rolno-spożywczy, a także administracji publicznej.

Perspektywa

Oczekuje się, że NIS2 obejmie ponad 300 000 organizacji w Europie - w porównaniu do kilku tysięcy w przypadku NIS1.

Kluczowe i ważne podmioty

W dyrektywie NIS1 podmioty zostały sklasyfikowane jako operatorzy usług kluczowych (OSE) i dostawcy usług cyfrowych (PSN). Dyrektywa NIS2 wprowadza teraz klasyfikację podmiotów jako „kluczowych" lub „ważnych" w powyższych sektorach, odzwierciedlając stopień krytyczności usług, sektor działalności, wielkość i obroty.

Średnie organizacje zatrudniające mniej niż 250 osób, których roczny obrót nie przekracza 50 mln euro (lub których suma bilansowa nie przekracza 43 mln euro) i działające w bardzo krytycznych sektorach są uznawane za ważne, podobnie jak duże organizacje działające w krytycznych sektorach. Tylko duże organizacje, które przekraczają pułapy ustalone dla średnich organizacji i należą do sektorów o bardzo krytycznym znaczeniu, są uważane za kluczowe.

Główne różnice między kluczowymi podmiotami a ważnymi podmiotami polegają na środkach, które należy wdrożyć, oraz na monitorowaniu zgodności z obowiązkami. W przypadku kluczowych podmiotów kontrola będzie miała charakter proaktywny (ex ante). Oznacza to, że organizacje te będą aktywnie monitorowane w celu weryfikacji, czy przepisy są przestrzegane. W przypadku ważnych podmiotów nadzór odbywa się ex post, jeżeli pojawiły się sygnały o incydencie. Jeśli po incydencie okaże się, że nie podjęto niezbędnych środków, organizacja może również otrzymać grzywnę i/lub inną sankcję określoną przez organ krajowy.

Łańcuch dostaw - również objęty

Dostawcy zarządzanych usług bezpieczeństwa Managed Service Providers (MSP) i Managed Security Service Providers (MSSP) są wyraźnie włączeni do sektorów „krytycznych" i będą musieli spełniać wymogi bezpieczeństwa. NIS2 ma również na celu zabezpieczenie szerszego łańcucha dostaw. Kluczowe i ważne podmioty będą mogły przenieść pewne obowiązki na swoich dostawców i usługodawców.

WYMAGANIA DOTYCZĄCE CYBERBEZPIECZEŃSTWA

Organizacje objęte NIS2 muszą wdrożyć aktywną strategię ochrony cybernetycznej, która obejmuje zapobieganie, wykrywanie, monitorowanie, analizę i łagodzenie skutków.

W art. 21 dyrektywy wymieniono 10 głównych „środków zarządzania ryzykiem cyberbezpieczeństwa":

01 Zasady dotyczące analizy ryzyka i bezpieczeństwa systemów informatycznych

02 Obsługa incydentów

03 Ciągłość działania

04 Bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące relacji między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami

05 Bezpieczeństwo w pozyskiwaniu, rozwijaniu i utrzymywaniu sieci oraz systemów informatycznych, w tym obsługa i ujawnianie luk w zabezpieczeniach

06 Zasady i procedury oceny skuteczności środków zarządzania ryzykiem cyberbezpieczeństwa

07 Podstawowe praktyki higieny cybernetycznej i szkolenia w zakresie cyberbezpieczeństwa

08 Zasady i procedury korzystania z kryptografii/szyfrowania

09 Bezpieczeństwo zasobów ludzkich, zasady kontroli dostępu i zarządzanie zasobami

10 Korzystanie z uwierzytelniania wieloskładnikowego (MFA) lub rozwiązań uwierzytelniania ciągłego, zabezpieczona komunikacja głosowa, wideo i tekstowa

WYTYCZNE DLA DOSTAWCÓW USŁUG CYFROWYCH

Komisja przyjmie kilka aktów wykonawczych. W szczególności określą one wymogi dotyczące środków związanych z dostawcami usług DNS, rejestrów nazw TLD, dostawcami usług przetwarzania w chmurze, dostawcami usług centrów danych, dostawcami sieci nadawczych, dostawcami treści, dostawcami usług zarządzanych, dostawcami zarządzanych usług bezpieczeństwa, dostawcami internetowych platform handlowych, wyszukiwarkami i platformami usług mediów społecznościowych oraz dostawcami usług zaufania. Kraje UE muszą przyjąć i opublikować środki niezbędne do zapewnienia zgodności z dyrektywą NIS2.

Te ogólnounijne środki zostaną podzielone na krajowe punkty odniesienia i określone w przepisach. Na przykład we Francji przekłada się to na „cele zgodności", które same dzielą się na „akceptowalne środki zgodności" (ponad sto z nich, obecnie opracowywanych przez ANSSI). Zobacz także odpowiedzi udzielone przez Sekoia na te wymagania techniczne w załączniku.

Środki te powinny:

- *Być proporcjonalne do ryzyka, kosztów, skutków i wagi incydentów*
- *Uwzględniać aktualny stan wiedzy oraz, w stosownych przypadkach, odpowiednie normy europejskie i międzynarodowe*

UE może:

- *Przeprowadzić ocenę ryzyka związanego z krytycznymi usługami, systemami ICT lub łańcuchami dostaw*
- *Nałożyć obowiązki certyfikacyjne*
- *Przyjąć akty wykonawcze określające wymogi techniczne*

Powiadamianie o istotnych incydentach

NIS2 nakłada stopniowe obowiązki sprawozdawcze na kluczowe i ważne podmioty w przypadku incydentów, które mają „znaczący wpływ" na świadczenie usług. Zgłoszenia te muszą być kierowane do właściwego organu lub CSIRT.

W stosownych przypadkach podmioty informują odbiorców swoich usług o istotnych incydentach. W przypadku gdy uzasadnia to interes publiczny, CSIRT lub właściwy organ może powiadomić opinię publiczną o istotnym incydencie lub zażądać tego od podmiotu.

Odpowiedzialność kadry kierowniczej

Kadra kierownicza wyższego szczebla jest ostatecznie odpowiedzialna za zarządzanie ryzykiem cyberbezpieczeństwa w krytycznych i ważnych podmiotach. W związku z tym organy zarządzające będą musiały zatwierdzać środki zarządzania ryzykiem i nadzorować ich wdrażanie w podmiocie. Dyrektorzy generalni (osoby fizyczne) mogą zostać pociągnięci do osobistej odpowiedzialności za naruszenie dyrektywy NIS2 przez spółkę i mogą zostać tymczasowo zawieszeni w wykonywaniu swoich obowiązków. Są oni również zobowiązani do odbycia szkoleń z zakresu cyberbezpieczeństwa i zapewnienia ich swoim pracownikom.

Sankcje

Zwiększony pułap związany z sankcjami, które mogą zostać nałożone przez władze krajowe:

- Do 10 000 000 EUR lub 2% rocznych globalnych przychodów dla istotnych podmiotów
- Do 7 000 000 EUR lub 1,4% rocznych globalnych przychodów dla ważnych podmiotów

Oprócz sankcji finansowych, państwa będą miały możliwość wydawania ostrzeżeń i podejmowania innych środków ograniczających, takich jak cofnięcie certyfikacji, w przypadku naruszenia dyrektywy NIS2.

SEKOIA WSPIERA UŻYTKOWNIKA W ZAPEWNIENIU ZGODNOŚCI Z NIS2

Czy jesteś sklasyfikowany jako kluczowy lub ważny podmiot? Sekoia pozwala poprawić ochronę, ułatwiając wykrywanie cyberzagrożeń i reagowanie na nie. W szczególności nasze rozwiązania SIEM, SOAR i CTI pomagają spełnić wiele wymagań NIS2, w tym (szczegóły w załączniku):

- **Ocena ryzyka:**

Wiedza o atakujących dzięki analizie cyberzagrożeń (Cyber Threat Intelligence) pozwala, na poziomie strategicznym i operacyjnym, lepiej zrozumieć ryzyko, na jakie narażona jest organizacja.

- **Obsługa incydentów:**

Monitorowanie zdarzeń w czasie rzeczywistym, wykrywanie incydentów bezpieczeństwa i automatyzacja reakcji dzięki Sekoia Defend. Nowe reguły wykrywania zostaną opracowane w celu ułatwienia wdrożenia dyrektywy w firmie lub organizacji publicznej.

- **Powiadomienie władz:**

Niski „średni czas do wykrycia" (MTTD) Sekoia Defend zapewnia wyraźny wskaźnik wydajności, aby spełnić obowiązek powiadamiania o istotnych incydentach w ciągu 24 godzin.

- **Udostępnianie informacji:**

Standaryzacja informacji na platformie Sekoia Defend ułatwia zgłaszanie incydentów i dzielenie się informacjami na temat cyberzagrożeń promowanych przez dyrektywę.

- **Ciągłość działania:**

Sekoia pomaga opracować odpowiednie ćwiczenia z zakresu zarządzania kryzysowego, a także zapewnia narzędzie do przeprowadzania tych ćwiczeń. Jest to na przykład platforma wykorzystywana przez NATO CCDOE w ramach ćwiczenia Crossed Swords 2023.

Sekoia, zaufany producent zapewniający odporność Twojej organizacji

Sekoia już teraz wdraża najlepsze praktyki w zakresie zapewniania bezpieczeństwa (MFA, testy antywłamaniowe itp.).

Bezpieczeństwo w chmurze

Rozwiązanie może korzystać z kwalifikowanego hostingu SecNumCloud, który gwarantuje surowe standardy i dobre praktyki w zakresie bezpieczeństwa danych. Sekoia została również wybrana do kwalifikacji SecNumCloud platformy SaaS.

Certyfikaty

Sekoia to rozwiązanie SaaS certyfikowane zgodnie ze standardem bankowym PCI-DSS w niektórych regionach chmury. Nasz program certyfikacji przewiduje uzyskanie ISO27001, a następnie SOC2.

Wewnętrzny CERT

Sekoia prowadzi również własny CSIRT, który jest uznanym członkiem InterCERT.

Dyrektywa NIS2 nie powinna być traktowana jako kwestia zgodności, ale jako szansa na poprawę poziomu cyberbezpieczeństwa.

Załącznik

Jak platforma Sekoia odpowiada na wymagania NIS2

Standardowe ramy bezpieczeństwa informacji, takie jak ISO27001, PCI-DSS lub NIST, mogą być wykorzystane do przygotowania się do NIS2, identyfikacji luk technologicznych i organizacyjnych oraz wdrożenia działań mających na celu zapewnienie zgodności. Poniższa tabela mapuje wymagania NIS2 do odpowiadających im domen bezpieczeństwa ISO27001. Trzecia kolumna wskazuje, w jaki sposób rozwiązania Sekoia przyczyniają się do zgodności Twojej organizacji.

Środki zarządzania ryzykiem (art. 21 NIS2)	Załącznik ISO27001	Jak pomaga Sekoia
A) Zasady dotyczące analizy ryzyka i bezpieczeństwa systemów informatycznych	A.5: Zasady bezpieczeństwa informacji	**Ocena ryzyka:** Znajomość zagrożeń dzięki cyber threat intelligence pozwala na poziomie strategicznym i operacyjnym lepiej zrozumieć ryzyko, na jakie narażona jest organizacja. Raporty FLINT (raporty Flash Intelligence) zintegrowane z ofertą Sekoia mają na celu zapewnienie decydentom strategicznej wizji zagrożenia. **Sekoia Intelligence** **Sekoia Defend**
B) Obsługa incydentów	A.16: Zarządzanie incydentami związanymi z bezpieczeństwem informacji	**Nadzór w czasie rzeczywistym:** Platforma Sekoia umożliwia monitorowanie zdarzeń w czasie rzeczywistym i wykrywanie incydentów bezpieczeństwa tak szybko, jak to możliwe (KPI: MTTD ~3 sek). **Sekoia Defend** **Wykrywanie:** Sekoia udostępnia liczne reguły wykrywania w prostym, interoperacyjnym i otwartym formacie (SIGMA), nadające się do natychmiastowego działania. Nowe reguły zostaną opracowane w celu ułatwienia wdrożenia dyrektywy w organizacji. **Sekoia Intelligence** **Sekoia Defend** **Reagowanie:** Dzięki modułowi SOAR platforma Sekoia pozwala szybciej reagować na incydenty i automatyzować reakcję dzięki playbookom i ponad 180 integracjom. **Sekoia Defend**
C) Ciągłość biznesowa, taka jak zarządzanie kopiami zapasowymi i odzyskiwanie danych po awarii oraz zarządzanie kryzysowe	A.17: Aspekty ciągłości działania związane z bezpieczeństwem informacji	**Ćwiczenia kryzysowe:** Analiza zagrożeń pomaga opracować odpowiednie ćwiczenia zarządzania kryzysowego, oparte na rzeczywistych zagrożeniach cybernetycznych, podczas gdy platforma zapewnia narzędzie do przeprowadzania tych ćwiczeń. **Sekoia Defend** **Zarządzanie kryzysowe:** Moduł SOAR umożliwia definiowanie playbooków w odpowiedzi na zidentyfikowany scenariusz kryzysowy oraz automatyzację reakcji. **Sekoia Defend**

		Odporność: Platforma Sekoia została zaprojektowana z myślą o elastyczności i redundancji, a przetwarzane przez nią logi są przechowywane w chmurze. Dzięki temu wzmacnia odporność organizacji w sytuacjach poważnych kryzysów, takich jak atak ransomware, który może doprowadzić do blokady systemu IT. **Sekoia Defend**
D) Bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące relacji między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami	A.15: Relacje z dostawcami	**Monitorowanie narzędzi innych firm:** Platforma SOC ma dużą liczbę integracji, aby pokryć duży obszar bezpieczeństwa i wdrożyć nową architekturę w ciągu kilku godzin. **Sekoia Defend**
E) Bezpieczeństwo w nabywaniu, rozwijaniu i utrzymywaniu sieci i systemów informatycznych, w tym obsługa i ujawnianie luk w zabezpieczeniach	A.12: Bezpieczeństwo operacyjne A.14: Pozyskiwanie, rozwój i utrzymanie systemów	**Rejestrowanie:** Platforma Sekoia może być zintegrowana z zewnętrznym źródłami logów, co umożliwia ich przechowywanie przez określony czas, zgodnie z wymogami prawa dla niektórych organizacji, a także certyfikatami, takimi jak PCI-DSS w branży bankowej. System korelacji i analizy logów wzmacnia zdolności wykrywania zagrożeń. **Sekoia Defend** **Bezpieczeństwo platformy Sekoia:** Podejście CI/CD Sekoia (ciągła dystrybucja i wdrażanie) oraz jej postawa bezpieczeństwa pozwalają na posiadanie wzmocnionego i stale aktualizowanego systemu bezpieczeństwa. **Sekoia Intelligence** **Sekoia Defend**
F) Zasady i procedury oceny skuteczności środków zarządzania ryzykiem cyberbezpieczeństwa	A.5: Zasady bezpieczeństwa informacji	**Raportowanie:** Funkcja mapowania reguł związanych z wykrywaniem zgodnie z ramami MITRE ATT&CK pozwala zidentyfikować rzeczywisty poziom jej pokrycia. **Sekoia Defend**
G) Podstawowe praktyki higieny cybernetycznej i szkolenia w zakresie cyberbezpieczeństwa		**Higiena cybernetyczna:** Utworzenie SOC z najnowocześniejszym rozwiązaniem bezpieczeństwa jest dobrą praktyką zapewniającą higienę cybernetyczną organizacji. **Sekoia Defend**
H) Zasady i procedury dotyczące korzystania z kryptografii oraz, w stosownych przypadkach, szyfrowania	A.10: Kryptografia	**Szyfrowanie:** Platforma Sekoia wykorzystuje szyfrowanie danych w tranzycie i w spoczynku. **Sekoia Intelligence** **Sekoia Defend**
I) Bezpieczeństwo zasobów ludzkich, polityka kontroli dostępu i zarządzanie zasobami	A.5: Polityka bezpieczeństwa informacji A.7: Bezpieczeństwo pracowników A.8: Zarządzanie aktywami A.9: Kontrola dostępu A.11: Bezpieczeństwo fizyczne i środowiskowe	**Kontrola dostępu:** Funkcja „Asset discovery” umożliwia identyfikację zasobów obecnych w wewnętrznym systemie informatycznym i odpowiednie zdefiniowanie polityk bezpieczeństwa (funkcja w fazie rozwoju, może podlegać modyfikacjom). **Sekoia Defend**

J) Korzystanie z uwierzytelniania wieloskładnikowego lub rozwiązań ciągłego uwierzytelniania, zabezpieczonych systemów komunikacji	A.13: Bezpieczeństwo komunikacji	**MFA:** Platforma Sekoia implementuje uwierzytelnianie wieloskładnikowe i SSO. Sekoia Intelligence Sekoia Defend

Inne środki NIS2	
Powiadamianie o istotnych incydentach (art. 23): Podmioty ważne muszą powiadamiać CSIRT o „istotnych" incydentach za pomocą wczesnego ostrzeżenia w ciągu 24 godzin, a następnie powiadomienia o incydencie w ciągu 72 godzin. Muszą również informować odbiorców swoich usług.	**Powiadomienie w ciągu 24h:** Czas MTTD platformy wynoszący ~3 sekundy pozostawia organizacji maksymalny możliwy czas na ocenę potrzeby wysłania wczesnego ostrzeżenia. CTI natywnie zintegrowane z platformą zapewnia wizję 360° i kontekst niezbędny do podjęcia decyzji o potrzebie ostrzeżenia. Sekoia Intelligence Sekoia Defend **Powiadamianie o incydentach:** Korzystając z możliwości automatyzacji platformy, Sekoia pracuje nad stworzeniem playbooka, aby ułatwić powiadamianie organów właściwych. Sekoia Defend **Raport końcowy:** Sporządzanie ułatwione dzięki przechowywaniu alertów i zgłoszeń lub „spraw" (nieograniczony czas trwania), a także przechowywaniu w tzw. „cold archive" (od 90 dni do jednego roku). Sekoia Defend
Informacje (art. 29 i 30)	Standaryzacja informacji na platformie Sekoia (CTI w formacie STIX/TAXII, reguły wykrywania SIGMA, playbooki CACAO itp.) ułatwia zgłaszanie incydentów i dobrowolne udostępnianie informacji o cyberzagrożeniach promowanych przez dyrektywę. Sekoia Intelligence Sekoia Defend

Więcej o rozwiązaniu Sekoia

Sekoia jest wiodącym europejskim dostawcą rozwiązań Security Information and Event Management (SIEM)/Security Orchestration, Automation, and Response (SOAR) wspieranych przez Cyber Threat Intelligence (CTI). Jej misją jest dostarczanie firmom i organizacjom publicznym najlepszych technologii ochrony przed cyberatakami. Łącząc przewidywanie zagrożeń poprzez wiedzę o atakujących z automatyzacją wykrywania i reagowania, platforma Sekoia SOC zapewnia zespołom bezpieczeństwa ujednolicony widok i całkowitą kontrolę nad ich systemami informatycznymi. Jej interoperacyjność z rozwiązaniami innych firm i zgodność z międzynarodowymi standardami technicznymi umożliwiają organizacjom pełne wykorzystanie istniejących technologii. Sekoia daje swoim klientom możliwość skoncentrowania zasobów ludzkich na misjach o wysokiej wartości dodanej, optymalizacji strategii cyberobrony i odzyskania przewagi nad zaawansowanymi cyberzagrożeniami.

Masz pytania? Skontaktuj się z nami!

Dawid Dziobek
Product Manager Sekoia
tel. +48 538 857 641 | dziobek.d@dagma.pl

sekoia × DAGMA BEZPIECZEŃSTWO IT