WHITEPAPER

Najwyższy poziom zabezpieczeń
Wszystko co musisz wiedzieć o dyrektywie NIS2

Digital Security
Progress. Protected.

Dokument przygotowany przez ESET
we współpracy z Eversheds Sutherland

Spis treści

Wprowadzenie

Dziękujemy za zainteresowanie naszym dokumentem dotyczącym dyrektywy NIS2. Omówiliśmy w nim najważniejsze jej aspekty oraz zastosowanie dla organizacji w państwach UE.

Dyrektywa NIS2, zwana również jako nowa wersja Dyrektywy o bezpieczeństwie sieci i informacji, to ogólnoeuropejskie zarządzenie mające na celu wzmocnienie cyberbezpieczeństwa Unii Europejskiej (UE). Ma pomóc organizacjom chronić się przed zagrożeniami cybernetycznymi oraz zapewnić bezpieczną i solidną infrastrukturę informatyczną wewnątrz całej wspólnoty. Teraz, **gdy dyrektywa została oficjalnie opublikowana**, państwa członkowskie mają 21 miesięcy – tj. do 17 października 2024 r. – na włączenie zapisów dyrektywy do lokalnego prawodawstwa.

W niniejszym artykule zawarliśmy przegląd najważniejszych przepisów zawartych w NIS2 i ich zastosowanie. Omówiliśmy również obowiązki wynikające z rozporządzenia, jakie organizacje muszą przestrzegać oraz w jaki sposób my możemy w tym pomóc.

Mamy nadzieję, że nasze wskazówki okażą się przydatne dla wszystkich firm, które chcą się dowiedzieć więcej o tym, jak chronić się przed cyberzagrożeniami i wprowadzić przepisy NIS2 w życie.

Czym jest
dyrektywa NIS2?

Twoja firma jest średniej wielkości lub dużą organizacją i działa w jednym z kluczowych sektorów, takich jak energia, transport, zdrowie czy infrastruktura cyfrowa? Jeśli tak - nowe przepisy UE mogą mieć olbrzymi wpływ na wymagania dotyczące cyberbezpieczeństwa w Twojej organizacji. „Ta europejska dyrektywa pomoże około 160 000 podmiotów wzmocnić kontrolę nad bezpieczeństwem i uczynić Europę bezpieczniejszym miejscem do życia i pracy. Prawo powinno także umożliwiać wymianę informacji z sektorem prywatnym i partnerami na całym świecie.

„Jeśli zostaniemy zaatakowani w skali przemysłowej, w ten sam sposób powinniśmy odpowiedzieć" - powiedział holenderski eurodeputowany Bart Groothuis.

Ponieważ cyberbezpieczeństwo jest niezwykle ważnym aspektem ochrony naszego społeczeństwa, Unia Europejska wprowadziła w 2016 r. pierwszą dyrektywę w sprawie bezpieczeństwa sieci i informacji (NIS). Chociaż to europejskie rozporządzenie zapewniło większą spójność UE w obszarze sieci i bezpieczeństwa informacji, zdaniem Parlamentu Europejskiego jeszcze bardziej należy zwiększyć odporność cybernetyczną, aby chronić społeczeństwo. Wraz z rosnącą cyfryzacją i dużą ilością cyberataków dyrektywa NIS2 będzie miała szerszy zasięg i skupi się na większej ilości sektorów, aby wyrównać i zwiększyć odporność na ataki organizacji, mających swoje siedziby w UE.

"Ta europejska dyrektywa pomoże około 160 000 podmiotom wzmocnić kontrolę nad bezpieczeństwem i uczynić Europę bezpiecznym miejscem do życia i pracy."

Zarządzanie ryzykiem i współpraca:

W jaki sposób ta zmieniona dyrektywa zapewnić ma lepszą odporność cybernetyczną? NIS2 stara się na różne sposoby podnosić poziom bezpieczeństwa w państwach członkowskich. Dyrektywa wzmacnia nałożone wymogi bezpieczeństwa, koncentruje się na zabezpieczeniu łańcucha dostaw (produkcja i łańcuch dostaw), usprawnieniu obowiązków sprawozdawczych, zaostrzeniu nadzoru oraz wprowadzeniu wymogów wykonawczych wraz ze zharmonizowanymi sankcjami we wszystkich państwach członkowskich. Poruszono także w znacznym stopniu kwestię wymiany informacji i współpracy (między)narodowej w dziedzinie zarządzania kryzysowego.

Zakres NIS2:

Dyrektywa NIS2 wpływa na znacznie więcej sektorów niż jej pierwotna wersja. W NIS wyznaczono jedynie dostawców infrastruktury opieki zdrowotnej, transportu, bankowości i rynku finansowego, infrastruktury cyfrowej, zaopatrzenia w wodę, energii i usług cyfrowych, przy czym państwa członkowskie mogły określić, które organizacje uznają za niezbędne. NIS2 wprowadza jednolite zasady dla średnich i dużych podmiotów działających w sektorach krytycznych, takich jak energetyka, transport, zdrowie i infrastruktura cyfrowa. Obejmuje to obecnie „sektory bardzo krytyczne", w tym energię, transport, bankowość, infrastrukturę rynku finansowego, opiekę zdrowotną, zaopatrzenie w wodę pitną, odprowadzenie ścieków, infrastrukturę cyfrową, zarządzanie ICT (B2B), rządowe i astronautyka, a także „sektory krytyczne", takie jak poczta i usługi kurierskie, gospodarka odpadami, chemikalia, żywność, produkcja, dostawcy usług cyfrowych i badania naukowe. Przepisami zostaną objęte wszystkie średnie i duże przedsiębiorstwa z tych sektorów.

Czy Twoja organizacja
jest podmiotem krytycznym, czy ważnym?

Sposób egzekwowania prawa zależy od kategorii, do której organizacja jest zaliczana. W ramach NIS2 istnieją dwie kategorie, do których dany podmiot może być przydzielony. Organizacje można określić jako **krytyczne** lub **ważne**. To, czy firma zostanie określona jako krytyczna lub ważna, zależy od tego, czy należy ona do sektora krytycznego, czy też bardzo krytycznego oraz jej wielkości.

W KTÓRYM SEKTORZE OPERUJE TWOJA FIRMA?

- ENERGIA
- TRANSPORT
- BANKOWOŚĆ
- OCHRONA ZDROWIA
- ZAOPATRZENIE W WODĘ PITNĄ
- ODPROWADZANIE ŚCIEKÓW
- INFRASTRUKTURA SIECIOWA
- ZARZĄDZANIE USŁUGAMI ICT (B2B)
- RZĄDOWY
- ASTRONAUTYKA I PODRÓŻE KOSMICZNE
- INFRASTRUKTURA RYNKU FINANSOWEGO
- USŁUGI POCZTOWE I KURIERSKIE
- ZARZĄDZANIE ODPADAMI
- PRODUKCJA
- DOSTAWCY USŁUG SIECIOWYCH
- BADANIA NAUKOWE
- PRODUKCJA I DYSTRYBUCJA CHEMIKALIÓW
- PRODUKCJA, PRZETWARZANIE I DYSTRYBUCJA ŻYWNOŚCI

° Duża firma:
ponad 250 pracowników i roczny obrót co najmniej 50 milionów euro (lub suma bilansowa co najmniej 43 miliony euro).

° Średnia firma:
powyżej 50 i nie więcej niż 250 pracowników oraz roczny obrót nieprzekraczający 50 milionów euro (lub suma bilansowa nie przekraczająca 43).

JAK DUŻA JEST TWOJA ORGANIZACJA?

*** DUŻE PRZEDSIĘBIORSTWO**

*** ŚREDNIEJ WIELKOŚCI FIRMA**

DUŻA ORGANIZACJA

ŚREDNIEJ WIELKOŚCI ORGANIZACJA

PODMIOT KRYTYCZNY

(*) Istnieją pewne wyjątki od reguły, gdzie podmioty takie jak np. dostawcy kwalifikowanych usług zaufania, rejestry domen internetowych najwyższego poziomu, a także dostawcy usług DNS, mogą zostać uznane za krytyczne bez względu na wielkość firmy. Wszystkie wyjątki znajdziesz w art. 3 ust. 1.

PODMIOT WAŻNY

Za ważne uważa się średnie organizacje zatrudniające mniej niż 250 pracowników i osiągające roczny obrót do 50 milionów euro (lub suma bilansowa do 43 mln euro) działające w bardzo krytycznych sektorach, podobnie jak inne duże i średnie firmy operujące w sektorach krytycznych. Za krytyczne uważa się jedynie duże przedsiębiorstwa, które przekraczają pułap określony dla średnich organizacji i operują w bardzo krytycznych sektorach. Niektóre firmy są automatycznie uznawane za „krytyczne" niezależnie od ich wielkości, jeśli przerwa w świadczeniu usług miałaby poważne konsekwencje dla społeczeństwa lub jeśli są one wyłącznym krajowym dostawcom. Obejmuje to organizacje udostępniające publiczne sieci i usługi komunikacyjne, dostawców kwalifikowanych usług zaufania oraz rejestry domen internetowych najwyższego poziomu.

Co do zasady dyrektywa NIS2 nie jest skierowana do małych i mikroprzedsiębiorstw, które zatrudniają mniej niż 50 pracowników, i których roczny obrót jest mniejszy niż 7 mln euro (lub suma bilansowa jest mniejsza niż 5 mln euro). Jeżeli jednak odgrywają one kluczową rolę dla społeczeństwa, gospodarki, sektorów lub usług, państwa członkowskie muszą zapewnić objęcie ich tą dyrektywą.

Główna różnica między podmiotami krytycznymi i ważnymi polega na monitorowaniu przestrzegania przepisów. W przypadku krytycznych podmiotów, głównie podmiotów z kluczowych sektorów, nadzór będzie miał charakter proaktywny. Oznacza to, że organizacje te będą aktywnie monitorowane pod kątem przestrzegania przepisów. W przypadku podmiotów ważnych kontrola następuje w późniejszym terminie, jeśli istnieją przesłanki wskazujące na wystąpienie zdarzenia. Jeżeli po incydencie okaże się, że organizacja nie podjęła wymaganych kroków, może być zmuszona stawić czoła możliwym konsekwencjom wynikającym z nieprzestrzegania przepisów dyrektywy.

Czego można się spodziewać po wprowadzeniu NIS2?

Wyjaśnimy to na podstawie dwóch przykładów.

1

Przedsiębiorstwo energetyczne BrightEnergies zatrudniające 500 pracowników musiało już uporać się z obowiązkami w zakresie bezpieczeństwa wraz z wprowadzeniem pierwszej dyrektywy NIS. W lokalnym ustawodawstwie NIS (w Holandii zawartym w ustawie o bezpieczeństwie sieci i systemów informatycznych) sektor, w którym operuje firma („energia") został sklasyfikowany jako dostawca kluczowy. Obecny dyrektor Lennard nie pracował jeszcze w BrightEnergies, istnieje jednak dokumentacja wskazująca, które środki i procesy zostały w tym czasie dostosowane lub zmienione. W 2022 r. dowiedział się, że powstaną nowe przepisy dotyczące NIS. Według nowych zasad przedsiębiorstwo energetyczne zostanie zaklasyfikowane jako „podmiot krytyczny". Wraz z wprowadzeniem NIS zaimplementowano już sporo zmian. Z uwagi na to, że hakerzy z innych krajów (takich jak Luksemburg, Włochy i Portugalia) już kilkakrotnie atakowali firmy z sektora energetycznego, Lennard chce zrobić wszystko, aby zapewnić, że nie wpłynie to na interesy BrightEnergies. Dlatego też wprowadzeniu przepisów wynikających z NIS2 nadano wysoki priorytet.

2

Firma przetwarzająca odpady i zajmująca się recyklingiem Waste2Resource nie była wcześniej objęta przepisami NIS ani innymi dotyczącymi cyberbezpieczeństwa. Jednak w ostatnich latach stało się jasne, że nawet przetwórca odpadów może paść ofiarą cyberataku: w 2021 r. konkurent został na kilka dni zamknięty z powodu ataku ransomware, który uniemożliwił przejazdy śmieciarek. Zespół IT w Waste2Resource cieszy się, że podlega dyrektywnie NIS2, ale przed nim wiele pracy. Zespół kierowany przez nowo zatrudnioną CISO Kayleigh jest obecnie zajęty przygotowaniami, takimi jak analiza ryzyka. W każdym razie ona i jej zespół już wiedzą, że są postrzegani jako podmiot ważny w rozumieniu dyrektywy NIS2 i dlatego muszą stawić czoła obowiązkowi dochowania należytej staranności i obowiązkowi reaktywnego raportowania.

Obowiązki wynikające z dyrektywy

Dyrektywa NIS2 wymaga od dodatkowych branż przyjęcia bardziej rozbudowanych wymogów w zakresie cyberbezpieczeństwa, a od ważnych i krytycznych podmiotów podjęcia działań w celu zarządzania ryzykiem bezpieczeństwa. Muszą między innymi tworzyć kopie zapasowe, przeprowadzać analizę ryzyka i mają obowiązek zgłaszania incydentów mających istotny wpływ na świadczenie usług. Aby utrzymać niskie obciążenia administracyjne, kierownictwo organizacji będzie odpowiedzialne za przestrzeganie przepisów dyrektywy NIS2.

Ta nowa polityka stanowi duży krok dla wielu organizacji, niezależnie od ich wielkości. Zarówno rząd, jak i organizacje będą musiały ponieść większą odpowiedzialność. Ma to również konsekwencje finansowe: budżet ICT firm, które nie są jeszcze objęte dyrektywą, ma wzrosnąć maksymalnie o 22%, a firm, które są już objęte, maksymalnie o 12%. Zwiększą się także obciążenia administracyjne. Czas pokaże, czy te dodatkowe wydatki na ICT będą opłacalne i zapewnią przedsiębiorcom przewagę konkurencyjną dzięki wyższemu poziomowi cyberbezpieczeństwa. Oczekuje się, że dyrektywa NIS2 doprowadzi nie tylko do bardziej rygorystycznego egzekwowania przepisów i obowiązków, ale także do bezpieczniejszej gospodarki cyfrowej w Unii Europejskiej i ochrony przed cyberatakami.

Co wprowadzenie NIS2 oznacza dla Twojej organizacji?

Jak wspomniano wcześniej, dyrektywa NIS2 rozróżnia dwie kategorie: podmioty krytyczne i ważne, gdzie wcześniej dokonano jedynie rozróżnienia pomiędzy organizacjami kluczowymi objętymi dyrektywą NIS i organizacjami nieistotnymi. Wszystkie sektory i organizacje, które zostaną objęte przepisami zawartymi w NIS2, mają ogromne znaczenia dla społeczności. Jeżeli organizacje te nie mogłyby już spełniać swojej roli, spowodowałoby to poważne problemy dla społeczeństwa.

Cyberataki mogą mieć znaczący wpływ nie tylko na organizacje, ale także na społeczeństwo.
Oto kilka przykładów poważnych ataków:

NotPetya

Rozprzestrzenienie się oprogramowania ransomware NotPetya w 2017 r., które spowodowało poważne zakłócenia, w tym zamknięcie portu w Rotterdamie.

2017

Mandemakers gr. & VDL

Podczas ataków oprogramowania ransomware na Mandemakers gr. & VDL działalność tych organizacji została poważnie zakłócona.

2021

Bakker Logistiek

W wyniku ataku na firmę Baker Logistiek przez kilka dni w supermarketach brakowało sera na półkach.

2021

Kaseya

Atak na dostawcę oprogramowania Kaseya zapewnił cyberprzestępcom dostęp do systemów tysięcy firm.

2021

Obie kategorie powstały, ponieważ nie wszystkie sektory o tej samej skali będą miały wpływ na społeczeństwo w przypadku incydentu. Poniżej wyjaśniamy różnicę pomiędzy tymi dwiema grupami – krytyczną i ważną – oraz jaki ma to wpływ na zmiany, jakie przyniesie NIS2.

Obowiązek dochowania należytej staranności i raportowania

Wszystkie organizacje objęte NIS2 – krytyczne i ważne – będą musiały spełnić swój obowiązek dochowania należytej staranności. Dyrektywa zawiera wykaz typów środków, których dostawcy muszą przestrzegać, w tym:

- zasady dotyczące analizy i informacji o ryzyku bezpieczeństwa systemu
- dbałość o zarządzanie kryzysowe i ciągłość działania w przypadku poważnego incydentu cybernetycznego
- zapewnienie bezpieczeństwa łańcucha dostaw
- obowiązek dochowania należytej staranności w zapewnianiu bezpieczeństwa sieci i systemów informatycznych
- wykorzystanie kryptografii i szyfrowania
- polityki i procedury oceny skuteczności środków zarządzania ryzykiem

Komisja Europejska zastrzega sobie prawo do doprecyzowania środków w drodze decyzji wykonawczych oraz rozszerzenia ich o środki dodatkowe. Państwa członkowskie mogą wówczas otrzymać swobodę nakładania konkretnych środków, biorąc pod uwagę okoliczności krajowe i sektorowe. Obowiązek raportowania będzie dotyczył także wszystkich organizacji objętych dyrektywą NIS2. Ten obowiązek zgłaszania oznacza, że organizacje, których to dotyczy, muszą zgłosić incydent bezpieczeństwa wyznaczonemu organowi w ciągu 24 godzin od uzyskania informacji o incydencie, a następnie w ciągu jednego miesiąca sporządzić raport podsumowujący.

NIS2 w pigułce

WAŻNE

Tak jak w przypadku **Waste2Resource**

Organizacje średniej wielkości działające w jednym z 11 bardzo krytycznych sektorów lub średnie i duże przedsiębiorstwa działające w jednym z 7 krytycznych sektorów.

KRYTYCZNE

Tak jak w przypadku **BrightEnergies**

Dużej wielkości firmy działające w jednym z bardzo krytycznych sektorów

OBOWIĄZEK DOCHOWANIA NALEŻYTEJ STARANNOŚCI

- utrzymanie podstawowego poziomu higieny cyfrowej i wdrażanie edukacji o cyberbezpieczeństwie
- ocena ryzyka bezpieczeństwa systemów informatycznych
- dbałość o zarządzanie kryzysowe i ciągłość działania w przypadku poważnego incydentu cybernetycznego
- zapewnienie bezpieczeństwa łańcucha dostaw
- obowiązek dochowania należytej staranności w celu zapewnienia bezpieczeństwa sieci i systemów informatycznych, w tym reagowania i komunikowania się w przypadku odkrycia luk w zabezpieczeniach
- zapewnienie bezpieczeństwa zasobów ludzkich, polityki dostępu i zabezpieczenie zasobów cyfrowych
- wykorzystanie kryptografii i szyfrowania
- wprowadzenie lub zastosowanie wieloetapowego uwierzytelniania i/lub bezpiecznej komunikacji wewnętrznej
- polityki i procedury oceny skuteczności metod zarządzania ryzykiem

Monitoring reaktywny
(po wystąpieniu incydentu)

Monitoring proaktywny
(nawet poza incydentami bezpieczeństwa)

OBOWIĄZEK RAPORTOWANIA (W 3 FAZACH)

- wczesne ostrzeganie w ciągu 24 godzin
- powiadomienie o incydencie w ciągu 72 godzin
- finalny raport podsumowujący po miesiącu (lub raport z postępu prac w przypadku trwającego incydentu)

Kara administracyjna za niedopełnienie obowiązku zachowania należytej staranności i raportowania:

- maksymalna kara pieniężna w wysokości co najmniej **7 000 000 euro**
- lub **co najmniej 1,4%** całkowitego rocznego przychodu z poprzedniego roku obrotowego; w zależności od tego, która kwota jest wyższa

Kara administracyjna za niedopełnienie obowiązku zachowania należytej staranności i raportowania:

- maksymalna kawa w wysokości **co najmniej 10 000 000 euro**
- lub **co najmniej 2%** całkowitego rocznego przychodu z poprzedniego roku obrotowego; w zależności od tego, która kwota jest wyższa

Dodatkowo istnieje możliwość czasowego zawieszenia zezwoleń lub zawieszenia osoby fizycznej, np. prezesa zarządu.

Monitorowanie

Różnica między wyznaczonymi kategoriami podmiotów polega na sposobie monitorowania, czy spełniają nałożone wymagania. W przypadku sektorów i organizacji uznanych za krytyczne będzie prowadzone proaktywne monitorowanie w celu weryfikacji czy wymagania są spełnione. W związku z tym prowadzony będzie aktywny monitoring, a kary za niewłaściwe zarządzenie będą nałożone przed wystąpieniem jakiegokolwiek incydentu.

Podmioty ważne, zaliczane do drugiej kategorii, będą weryfikowane w sposób reaktywny. Oznacza to, że organizacje te zostaną sprawdzone pod kątem zgodności z obowiązującymi przepisami dopiero po wystąpieniu incydentu. Jeśli okaże się, że nie podjęto wystarczających działań i nie spełniono wymagań, mogą zostać nałożone takie same sankcje, jak w przypadku podmiotów krytycznych.

Raportowanie

Dyrektywa NIS2 przewiduje trzyetapowe podejście do zgłaszania incydentów. Wczesne ostrzeganie w ciągu 24 godzin ma na celu ograniczenie potencjalnego rozprzestrzeniania się incydentów i umożliwienie innym podmiotom poszukiwania wsparcia. Powiadomienie o incydencie w ciągu 72 godzin musi zawierać wstępną ocenę incydentu, wykazując jego powagę i skutki oraz wskaźniki kompromisu (IOC). Sprawozdanie końcowe - sporządzone po miesiącu - musi zawierać wnioski wyciągnięte z incydentów. Podejście to ma na celu stopniową poprawę odporności poszczególnych podmiotów i całych sektorów na zagrożenia. Oprócz obowiązku wczesnego ostrzegania, uwaga dotycząca powiadamiania skupia się na postępowaniu z incydentem.

1 **Wczesne ostrzeganie**

Bez zbędnej zwłoki, a w każdym razie w ciągu 24 godzin od uzyskania informacji o istotnym incydencie, pierwsza informacja musi zostać skierowana do właściwego organu nadzorczego. W ostrzeżeniu tym należy wskazać, czy zdarzenie było spowodowane działaniem niezgodnym z prawem lub złośliwym, albo czy mogło mieć skutki transgraniczne. To są absolutnie niezbędne informacje. W ciągu 24 godzin od przekazania niniejszego ostrzeżenia podmiot zgłaszający otrzymuje odpowiedź zawierającą wstępną informację zwrotną od właściwego organu nadzorczego lub zespołu CSIRT. Na wniosek podmiotu można uzyskać wytyczne dotyczące wdrożenia ewentualnych środków łagodzących i dodatkowe wsparcie techniczne. W przypadku zaistnienia zdarzenia o charakterze karnym podmiot otrzyma także wskazówki dotyczące sposobu zgłoszenia zdarzenia organom ścigania.

2 **Powiadamianie o zdarzeniu**

Bez zbędnej zwłoki, do 72 godzin od wykrycia znaczącego incydentu, powiadomienie o incydencie musi zaktualizować informacje przekazane w ramach wczesnego ostrzegania i wskazać (i) wstępną ocenę incydentu, (ii) obejmującą jego wagę i wpływ, a także jeśli są dostępne, (iii) wskaźniki kompromisu (IOC).

3 **Raport podsumowujący**

Wreszcie, w ciągu miesiąca od powiadomienia o incydencie, złożony zostanie raport końcowy zawierający (i) szczegółowy opis incydentu, jego skutki, (ii) rodzaj zagrożenia lub pierwotną przyczynę infekcji, która wywołała incydent, (iii) zastosowane środki łagodzące skutki wystąpienia incydentu oraz (iv) jego wpływu transgranicznego. W uzasadnionych przypadkach i po konsultacji z właściwym organem nadzorczym można odstąpić od 24-godzinnego terminu zgłoszenia incydentu i miesięcznego terminu publikacji finalnego raportu.

1

Kryzys w BrightEnergies. Atakujący dostał się do sieci firmowej, nikt nie wie jak to się udało i co powinno się w takiej sytuacji zrobić. Okazuje się, że CISO nie jest osiągalna! Wszyscy pogrążyli się w chaosie, na szczęście jej miejsce zajął specjalista IT, Menno. W ciągu 24 godzin wysłał wczesne ostrzeżenie do RDI. Razem z podmiotem zewnętrznym odszukał kopie zapasowe firmowych danych. Udało się je odnaleźć i dzięki temu organizacja wie jak poradzić sobie z najgorszymi konsekwencjami, ponieważ ma dostęp do istotnych danych. Niemniej jednak od kilku dni firma nie działa, co pociąga za sobą wszystkie konsekwencje. Miesiąc po zdarzeniu szczegółowy opis, podjęte środki łagodzące i źródło ataku zostają przedstawione w końcowym raporcie. Fakt, że w dziedzinie bezpieczeństwa nie wszystko było tak dobrze zorganizowane, otworzył oczy dyrektorowi Lennardowi. Kryzys ten ma poważne konsekwencje dla BrightEnergies.

2

Waste2Resource stoi w obliczu ataku ransomware, podobnie jak jego konkurent w 2021 roku. Dzięki procesom, które CISO Kayleigh zdołała udokumentować, zespół IT może szybko przywrócić ostatnią kopię zapasową. Niecałe 24 godziny później organizacja znów działa. Dzięki wysiłkom mającym na celu spełnienie wymagań NIS2 szkody nie są aż tak duże. Kayleigh zapomniała tylko o jednym: wczesnym ostrzeżeniu. Na szczęście jeden z kolegów z zespołu zaalarmował ją w ostatniej chwili, że pierwszy raport należy wysłać do 24 godzin. „Nie zapomnij przesłać pierwszego ostrzeżenia o incydencie!" – powiedział kolega do Kayleigh zanim wyszła do domu.

Istotne zagrożenia dla cyberbezpieczeństwa

W dyrektywnie NIS2 ustawiono bardziej rygorystyczne zasady zgłaszania incydentów mających poważne konsekwencje. Organizacje powinny również zgłaszać wszelkie napotkane istotne zagrożenia cybernetyczne, które mogą prowadzić do poważnego incydentu. W zakresie koncepcji cyberbezpieczeństwa NIS2 jest zgodny z definicją Unii Europejskiej dotyczącą cyberbezpieczeństwa i certyfikacji IT. Incydent uznaje się za znaczący, jeśli powoduje dostrzegalne zakłócenia w działaniu lub straty finansowe dla organizacji lub może spowodować znaczące szkody materialne i niematerialne dla organizacji lub poszczególnych osób.

Dobrowolne powiadomienia

Organizacje nieobjęte zakresem dyrektywy NIS2 mogą dobrowolnie zgłaszać istotne incydenty, zagrożenia cybernetyczne lub potencjalne zdarzenia. Organ nadzorczy stosuje procedurę raportowania. W przypadku dobrowolnych zgłoszeń nie należy nakładać żadnych dodatkowych obowiązków.

Zakres obowiązków

Komisja Europejska może udzielić dalszych wskazówek dotyczących informacji, formatu i procesu zgłaszania zarówno w przypadku incydentów o dużym znaczeniu, jak i zagrożeń. Zakres obowiązków może zatem zostać rozszerzony.

Grzywny i kary

Obowiązek dochowania należytej staranności i obowiązek raportowania również stanowią formę egzekwowania prawa, zapewniając skuteczne przestrzeganie zasad. W tym celu organy będą miały do dyspozycji różne środki i zasoby nadzorcze.

Cyberbezpieczeństwo i odporność środowisk na zagrożenia stały się tematem obrad NIS2. Oprócz powszechnych sposobów egzekwowania prawa – obejmującego grzywny, kary i publiczne piętnowanie – w grę wchodzi odpowiedzialność osobista i zawieszenie dyrektorów. Skończyły się czasy ignorancji i delegowania zadań.
// **Olaf van Haperen - Eversheds Sutherland**

Sankcje minimalne

Dyrektywa NIS2 zawiera obowiązkową listę sankcji, obejmującą kontrolę, audyty bezpieczeństwa, skanowanie bezpieczeństwa, wnioski o przedstawienie informacji i wnioski o udzielenie dostępu do danych. Niektóre sankcje są takie same dla wszystkich krajów, inne nie, np. sankcje za poważne naruszenia. W takich przypadkach kraje muszą same zapewnić skuteczne, proporcjonalne i odstraszające kary. Rodzaj sankcji (karnych lub administracyjnych) jest również ustalany przez kraj docelowy. Kary powinny być dostosowane do powagi i charakteru naruszenia oraz powinny uwzględniać takie czynniki jak wyrządzona szkoda, współpraca z właściwym organem i inne okoliczności.

Kary administracyjne

Zamiast, lub dodatkowo do innych środków, w zależności od okoliczności sprawy, mogą zostać nałożone administracyjne kary pieniężne. Przy nakładaniu kary administracyjnej należy uwzględnić te same elementy, co w przypadku pozostałych sankcji. Naruszenia mogą zostać ukarane karami administracyjnymi w wysokości do 10 milionów euro lub 2% rocznego ogólnoświatowego obrotu danej firmy, w zależności od tego, która z tych kwot jest wyższa. Lokalne władze nadzorcze muszą opracować własne zasady nakładania kar.

GRZYWNY

Dyrektywa NIS2 nakłada kary pieniężne w wysokości co najmniej 10 milionów euro lub 2% całkowitego światowego obrotu.

ZAWIESZENIA

Osoby posiadające odpowiednie uprawnienia lub stanowiska krytyczne mogą zostać zawieszone.

1

Firmie **BrightEnergies** grożą sankcje po ataku ransomware. Jako podmiot krytyczny mają obowiązek posiadania najnowocześniejszych zabezpieczeń. CISO zostaje zawieszony i grozi mu wysoka grzywna. Dyrektor Lennard podsumowuje, że bezpieczeństwo jest obecnie najwyższym priorytetem dla zespołów IT i chce wdrożyć zaawansowane rozwiązania zabezpieczające, aby proaktywnie zapobiegać atakom.

2

Na szczęście firma **Waste2Resource** uniknęła sankcji. Incydent otworzył oczy Kayleigh, która zgłosiła dyrektorowi generalnemu potrzebę zwiększenia budżetu na zabezpieczenie organizacji przed zagrożeniami. Chociaż dyrektor generalny zdaje sobie sprawę z powagi problemu, jest już całkiem usatysfakcjonowany: „Świetnie spełniamy wymagania, prawda?". Keyleigh otrzymuje nieco zwiększony budżet, aby jeszcze bardziej zwiększyć bezpieczeństwo.

Razem pracujemy na rzecz większego bezpieczeństwa

Dyrektywa NIS2 zapewni również utworzenie europejskiej sieci organizacji łącznikowych ds. cyberkryzysów (EU-CyCLONe), aby zapewnić wsparcie i koordynację w przypadku cyberataku na dużą skalę w UE. Eksperci będą również nalegać na współpracę i uczenie się od siebie nawzajem między państwami członkowskimi, aby przekazywać wskazówki i zwiększać wzajemne zaufanie.

Potrzebujesz pomocy przy wdrożeniu NIS2?

Oto, co ESET oraz Dagma Bezpieczeństwo IT mogą zrobić dla Twojej organizacji

Jako europejski dostawca w dziedzinie rozwiązań i usług bezpieczeństwa cyfrowego, chętnie pomożemy w kwestiach związanych z NIS2 lub jego wdrożeniem.

Możliwości, jakie oferujemy w zakresie NIS2:

- dostarczanie rozwiązań i usług bezpieczeństwa, które przyczyniają się do zgodności
- interaktywne sesje, takie jak webinary i warsztaty
- dzielenie się wiedzą za pośrednictwem naszych kanałów w mediach społecznościowych oraz na naszym blogu
- nasi specjaliści są zawsze dostępni, aby odpowiedzieć na Twoje pytania

Oto, jak nasze usługi cybezbezpieczeństwa, mogą być odpowiedzią na potrzeby związane z NIS 2

Audyt zgodności z Ustawą o Krajowym Systemie Cyberbezpieczeństwa

Audyt KSC to ocena gotowości firmy do realizacji obowiązków wynikających z treści UoKSC, do której zostanie zaimplementowana dyrektywa NIS 2. Usługa ta opiera się o weryfikację Systemu Zarządzania Bezpieczeństwem Informacji, a jej podstawą, poza wspomnianą ustawą, są również normy ISO 27001 i ISO 223001. Audyt można wykonać zarówno na etapie przygotowywania ZSBI w organizacji, a także przeprowadzać go zgodnie z zaleceniami, czyli nie rzadziej niż na 2 lata.

Wdrożenie SZBI i przygotowanie klienta do zgodności z UoKSC

Dostarczymy metodykę, narzędzia, wiedzę i zespół ekspertów, którzy zapewnią kompleksowe wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w Twojej organizacji. Implementacja polega na przygotowaniu wraz z klientem procesów, procedur i dokumentów tak aby organizacja zaczęła pracować zgodnie z wymaganiami stawianymi przez UoKSC. Wdrożenie SZBI jest procesem, który powinien być stale monitorowany, utrzymywany i doskonalony.

Testy penetracyjne

Testy penetracyjne są przeprowadzane poprzez symulację ataku naszego pentestera na środowisko i/lub aplikacje webowe klienta, dzięki czemu weryfikujemy aktualny stan zabezpieczeń infrastruktury informatycznej w organizacji. Testy te powalają spełnić jedno z wymagań dyrektywy NIS2, mówiących o bezpieczeństwie w procesach rozwojowych i wsparciu czy także o bezpieczeństwie eksploatacji.

Security Operation Center

W naszej ofercie znajduje się również usługa SOC, w ramach której prowadzimy monitorowanie w trybie ciągłym 24/7, wykrywanie, reagowanie i zarządzanie zagrożeniami związanymi z bezpieczeństwem informacji i systemów. Tak kompleksowa obsługa pozwala spełnić wymagania dyrektywy NIS 2 w zakresie zapewnienia ciągłość działania oraz obsługi incydentów.

Chcesz wiedzieć więcej?
Skontaktuj się z nami!

Bartosz Różalski

Senior Product
Manager ESET

rozalski.b@dagma.pl

+48 668 642 849

Sebastian Cielecki

Junior Product
Manager ESET

cielecki.s@dagma.pl

+48 538 859 660

Krystian Paszek

Cybersecurity Services
Manager

paszek.k@dagma.pl

+48 784 492 442

Źródła:

https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022L2555&from=EN

•

https://www.europarl.europa.eu/news/nl/press-room/20221107IPR49608/cyberbeveiliging-parlement-neemt-nieuwe-wet-aan-om-veerkracht-eu-te-versterken

Digital Security
Progress. Protected.

Dokument przygotowany przez ESET
we współpracy z Eversheds Sutherland