WHITE PAPER

Zgodność z NIS2: Przewodnik po zabezpieczaniu infrastruktury krytycznej

HOLM SECURITY

WHITE PAPER

Zgodność z NIS2: Przewodnik po zabezpieczaniu infrastruktury krytycznej

Dyrektywa NIS (Network and Information System Directive) jest pierwszym europejskim prawem w zakresie cyberbezpieczeństwa. Została wprowadzona w 2016 r. we wszystkich państwach członkowskich. W 2022 r. dyrektywa została zaktualizowana do wersji NIS2, z nowymi wymogami mającymi na celu zapewnienie wysokiego poziomu odpowiedzialności za zarządzanie ryzykiem w bezpieczeństwie sieci IT, a także harmonizacji standardów przyjętych w krajach Unii Europejskiej.

NIS2 i NIS - jaka jest różnica?

Dyrektywa NIS2 w dużej mierze opiera się na tych samych zasadach, co NIS, jednak wprowadza kilka ważnych zmian:

- Zwiększa liczbę podmiotów, które muszą spełniać wymogi dotyczące bezpieczeństwa IT.
- Nakłada na podmioty większą odpowiedzialność za zapewnienie bezpiecznej pracy dostawców.
- Aktualizuje wysokość sankcji dla firm, które nie przestrzegają przepisów lub je naruszają.
- Wymaga przeprowadzania specjalnych szkoleń dla pracowników.
- Wprowadza dwuetapowy proces zgłaszania incydentów.
- Wymusza zastosowanie szyfrowania.

Budowanie Cybersecurity framework

Profesjonalizacja grup cyberprzestępczych powoduje, że firmy zmuszone są redefiniować swoje strategie bezpieczeństwa. Właśnie dlatego posiadanie cybersecurity framework ma kluczowe znaczenie dla ochrony przed tymi podstępnymi hakerami.

Systematyczna ocena środowiska IT, edukacja pracowników w zakresie najlepszych praktyk i zgodności z przepisami to klucz do wielowarstwowej cyberochrony. Współpracując z odpowiednimi narzędziami i zasobami, można zbudować odporne cybersecurity framework, które ochronią organizację przed cyberprzestępcami.

Sektory kluczowe oraz ważne

NIS2 rozróżnia sektory **kluczowe** i **ważne**. W załączniku I do dyrektywy wyszczególniono te pierwsze, a w załączniku II te drugie. Organizacje muszą określić, czy należą do którejś z tych kategorii i odpowiednio przestrzegać wymogów dyrektywy.

W oryginalnej dyrektywie następujące sektory zostały uznane za krytyczne i wymagające wzmocnienia bezpieczeństwa:

- Energetyka
- Transport
- Zdrowie
- Infrastruktura rynków finansowych
- Wodociągi
- Bankowość
- Dostawcy usług cyfrowych

WHITE PAPER

Zgodność z NIS2: Przewodnik po zabezpieczaniu infrastruktury krytycznej

Dyrektywa NIS2 obejmuje teraz 8 kolejnych sektorów. Są to:

- Dostawcy środków łączności elektronicznej, sieci lub usług
- Usługi cyfrowe, takie jak platformy mediów społecznościowych lub centra danych
- Zarządzanie ściekami oraz odpadami
- Przestrzeń kosmiczna
- Wytwarzanie produktów krytycznych (farmaceutycznych, medycznych, chemicznych...)
- Usługi pocztowe i kurierskie
- Żywność i napoje
- Administracja publiczna

Wdrożenie środków cyberbezpieczeństwa

Aby skutecznie zapobiegać atakom hakerskim, organizacje muszą wdrożyć proporcjonalne do wielkości i charakteru organizacji rozwiązania cyberbezpieczeństwa. Powinny one obejmować procedury zarządzania incydentami, zabezpieczenie sieci i zasady kontroli dostępu.

Zgłaszanie incydentów bezpieczeństwa

Organizacje muszą zgłaszać odpowiednim organom krajowym wszelkie incydenty związane z cyberbezpieczeństwem. Wymagania dotyczące raportowania różnią się w zależności od powagi incydentu i sektora, w którym działa organizacja.

Przeprowadzanie oceny ryzyka

Organizacje muszą regularnie przeprowadzać oceny ryzyka w celu identyfikacji słabych punktów sieci i systemów informatycznych. Ocena powinna opierać się na zasobach organizacji, zagrożeniach i potencjalnym wpływie na organizację.

Edukacja pracowników

Organizacje powinny szkolić w zakresie cyberbezpieczeństwa na wszystkich poziomach - od zarządu po pracowników niższego szczebla. Szkolenie powinno obejmować wiedzę na temat ryzyka cyberataków, sposobów identyfikacji potencjalnych zagrożeń i reagowania na incydenty.

Monitorowanie zgodności

Organizacje muszą regularnie monitorować zgodność z wymogami NIS2, aby upewnić się, że spełniają jej kryteria. Cykliczny przegląd swojej infrastruktury IT, procedur zarządzania incydentami i ocen ryzyka, aby zidentyfikować wszelkie obszary wymagające poprawy.

Usprawnienie operacji biznesowych

W ramach dyrektywy NIS2 znajdziemy nowe obowiązki w kwestii cyberbezpieczeństwa. Bazują one na podejściu systematycznym, analitycznym i opartym na ryzyku, zgodnie z innymi regulacjami, takimi jak RODO. Zarządzanie ryzykiem i reagowanie na incydenty ma kluczowe znaczenie. Spełnienie tych wymogów może przynieść firmie następujące korzyści:

Zarządzanie ryzykiem

Regularne oceny ryzyka mogą pomóc zidentyfikować podatności i wdrożyć środki w celu ich złagodzenia, zmniejszając w ten sposób prawdopodobieństwo cyberataku.

Zarządzanie incydentami

Posiadanie procedur zarządzania incydentami, w tym wymagań dotyczących raportowania i planów reagowania, może pomóc firmie szybko i skutecznie reagować na incydenty, minimalizując ich wpływ i zapobiegając podobnym wydarzeniom w przyszłości.

Środki techniczne i organizacyjne

Wdrożenie odpowiednich środków technicznych i organizacyjnych, takich jak kontrola dostępu, szyfrowanie i systemy monitorowania, może znacznie zmniejszyć ryzyko cyberataków i naruszeń danych.

Ciągłość działania

Posiadanie planów ciągłości działania, w tym procedur tworzenia kopii zapasowych i odzyskiwania danych, może pomóc firmie w utrzymaniu działalności w przypadku incydentu i minimalizować przestoje, zapewniając ciągłość krytycznych usług.

Bezpieczeństwo łańcucha dostaw

Zapewnienie bezpieczeństwa łańcucha dostaw, w tym zewnętrznych dostawców i wykonawców, może pomóc zmniejszyć ryzyko cyberataków pochodzących ze źródeł zewnętrznych.

Założeniem dyrektywy NIS2 jest poprawa zbiorowej zdolności Unii Europejskiej do reagowania na cyberzagrożenia. W praktyce, nawet jeśli dyrektywa nie obejmuje wyraźnie organizacji, oczekuje się, że zwiększą one swoje bezpieczeństwo cyfrowe, jeśli świadczą usługi podmiotom, których dotyczy NIS2.

Przestrzegając wymogów NIS2, firma może proaktywnie zarządzać ryzykiem związanym z cyberbezpieczeństwem, minimalizować wpływ incydentów i zapewniać ciągłość krytycznych operacji. W rezultacie doprowadzi to do zwiększenia zaufania i satysfakcji klientów oraz przewagi konkurencyjnej na rynku.

Co zrobić w przypadku incydentu?

Jeżeli podmioty kluczowe lub ważne dowiedzą się o poważnym incydencie, powinny podjąć następujące działania:

1. Wstępne powiadomienie w ciągu 24 godzin od uzyskania informacji o incydencie, ze wskazaniem, czy podejrzewa się, że jest on spowodowany bezprawnymi lub złośliwymi działaniami albo może mieć wpływ transgraniczny.
2. Powiadomienie właściwych organów lub krajowego zespołu CSIRT w ciągu 72 godzin od uzyskania informacji o istotnym incydencie. W stosownych przypadkach aktualizuje ono poprzednie informacje i wskazuje wstępną ocenę jak poważny jest incydent, w tym jego dotkliwość i skutki, a także oznaki naruszenia integralności systemu, jeśli występują.
3. Przygotowanie raportu pośredniego dotyczącego istotnych aktualizacji statusu na wniosek właściwego organu lub CSIRT.

4. Sprawozdanie końcowe złożone nie później niż miesiąc po zgłoszeniu pierwszego raportu. Sprawozdanie musi zawierać co najmniej następujące informacje:
    - Szczegółowy opis incydentu, jego wagi i możliwego wpływu.
    - Rodzaj zagrożenia lub źródło, które prawdopodobnie spowodowało incydent.
    - Zastosowane środki zaradcze.
    - W stosownych przypadkach, transgraniczny wpływ incydentu.
5. Dostarczenie raportu z postępów, jeśli incydent nadal trwa w momencie składania raportu końcowego oraz raportu końcowego w ciągu miesiąca od obsługi incydentu.

Jak Holm Security pomaga w spełnieniu wymagań dyrektywy NIS2?

Holm Security oferuje systematyczne, analityczne, oparte na ryzyku podejście, które pomaga sprostać wymaganiom NIS2. Platforma Next-Gen Vulnerability Management umożliwia organizacji dostosowanie programu cyberbezpieczeństwa do jej konkretnych potrzeb i słabych punktów infrastruktury. Ustalając priorytety podatności w zabezpieczeniach z perspektywy ryzyka, można wzmocnić cykl ciągłego reagowania na nowe zagrożenia i luki.

Narzędzie to oferuje raportowanie nawet w przypadku podatności w zabezpieczeniach, które nie skutkują wystąpieniem incydentów, dzięki czemu można odkrywać trendy i wzorce dotyczące stanu cyberbezpieczeństwa. Regularne skany całego środowiska IT zapewniają maksymalną skuteczność. Dodatkowo utworzone raporty pozwalają zrozumieć zagrożenia i umożliwiają zachowanie zgodności z przepisami bezpieczeństwa, przy jednoczesnym określeniu, które kwestie wymagają naprawy.

Dzięki możliwości tworzenia szablonów raportów dotyczących zgodności z przepisami organizacja zyskuje pewność, że nie narazi się na związane z tym kłopoty prawne, w tym sankcje administracyjne, utratę pozwoleń, certyfikatów itp..

Dlaczego Holm Security?

Najlepsza ochrona uwzgledniająca różne wektory ataków

Uwzględnia najszerszy w branży zakres wektorów ataków (zarówno techniczne, jak i ludzkie), co pozwala szybko wykryć nowe luki.

Bądź o krok przed cyberprzestępcami

Z nami zidentyfikujesz podatności na całej powierzchni ataku i będziesz o krok przed cyberprzestępcami.

Ochrona danych

Wszelkie gromadzone przez nas dane dotyczące podatności na zagrożenia są przechowywane i szyfrowane, dzięki czemu możesz mieć pewność, że tylko Ty będziesz mieć dostęp do swoich danych.

Chcesz dowiedzieć się więcej?

Chcesz bezpłatnie przetestować? Skontaktuj się z nami!

Patryk Ćwięczek
Product Manager Holm Security

+48 660 471 728
+48 32 793 11 54

holmsecurity@dagma.pl

www.holmsecurity.pl

HOLM SECURITY