Bitdefender

Podstawowe kroki w celu zapewnienia zgodności z rozproszonym systemem NIS2

11.10.2024

Państwa członkowskie Unii Europejskiej (UE) ścigają się, aby dotrzymać terminu 17 października na uchwalenie ustawodawstwa, które transponuje dyrektywę w sprawie bezpieczeństwa sieci i informacji (NIS2) do prawa krajowego. Tylko dwa z 27 państw UE dotrzymały terminu legislacyjnego na miesiąc przed końcem, co wywiera presję na pozostałe 25 państw, aby uchwaliły prawo przed zakończeniem bieżących sesji ustawodawczych.

Wzmożenie aktywności w ciągu najbliższych kilku tygodni i zdecentralizowany charakter NIS2 z pewnością wywołają zamieszanie wśród firm prowadzących działalność w UE. Aby wyprzedzić szybko postępujący harmonogram, organizacje będą musiały rozpocząć działania na rzecz zgodności już teraz i dowiedzieć się, jak spełnić niepewne wymagania dotyczące zgodności, zachowując jednocześnie

integralność operacyjną i postawę bezpieczeństwa zarówno w perspektywie krótkoterminowej, jak i długoterminowej.

Choć może się wydawać, że to powód do paniki, dobrą wiadomością jest to, że NIS2 opiera się na sprawdzonych, najlepszych praktykach zarządzania ryzykiem cyberbezpieczeństwa i zgłaszania incydentów, które stosuje już większość organizacji.

Jak NIS2 wpłynie na niemal każdą firmę w Europie?

Według Raphaëla Peyreta, dyrektora ds. bezpieczeństwa w chmurze w Bitdefender, prawie każda organizacja prowadząca działalność w Europie będzie miała wpływ na ustawodawstwo NIS2. NIS2 stawia organizacjom prywatnym dwa główne wymagania: wdrożenie strategii zarządzania ryzykiem (artykuł 21) i zgłaszanie znaczących incydentów cyberbezpieczeństwa, które mogą prowadzić do przestoju – niezależnie od tego, czy intencja jest złośliwa czy przypadkowa. Artykuł 21 dyrektywy wymienia konkretne technologie – w tym analizę ryzyka, obsługę incydentów, ciągłość działania, bezpieczeństwo sieci, szyfrowanie, kontrolę dostępu, zarządzanie aktywami, uwierzytelnianie wieloskładnikowe (MFA) i inne – które organizacje muszą wdrożyć, aby spełnić wymogi.

NIS2 dotyczy średnich firm i dużych przedsiębiorstw w 18 branżach. Podczas gdy NIS2 dotyczy każdej organizacji działającej w tych sektorach, niektóre branże mogą podlegać bardziej rygorystycznym wymogom zgodności poprzez dodatkowe przepisy, takie jak Digital Operational Resilience Act (DORA), który dotyczy sektora finansowego.

Każde państwo członkowskie UE jest zobowiązane do opublikowania listy podmiotów podlegających NIS2 i dodatkowym przepisom do kwietnia 2025 r., ale wszystkim organizacjom prowadzącym działalność w Europie zdecydowanie zaleca się zapoznanie z proponowanymi przepisami już teraz i określenie obszarów zainteresowania.

Opanowanie zgodności z NIS2 poprzez ocenę ryzyka

„Im szybciej zrozumiesz, w jaki sposób przepisy NIS2 dotyczą Twojej organizacji, tym szybciej podejmiesz kroki, aby osiągnąć zgodność z dyrektywą. Zaczyna się to od dokładnej analizy obecnego stanu zabezpieczeń, w tym urządzeń i zasobów sieciowych oraz wszelkich potencjalnych luk. Pozwala to zidentyfikować podatności i opracować plan naprawczy w celu ich zamknięcia. Ważne jest również uzyskanie akceptacji decydentów i innych interesariuszy w odniesieniu do planu działania oraz zapewnienia zgodności" – mówi Krzysztof Budziński z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania BItdefender.

Personel zarządzania ryzykiem będzie musiał to robić sprawnie ze względu na ograniczenia budżetowe i szybką, zdecentralizowaną oś czasu NIS2. Na szczęście dyrektywa ściśle podąża za istniejącymi ramami cyberbezpieczeństwa, których organizacje już przestrzegają – w tym ISO 27001. Przestrzeganie tych już zdefiniowanych zasad i procesów to dobry sposób na przyspieszenie oceny i zgodności w krótkim okresie.

Długoterminowa zgodność z przepisami NIS2 będzie wymagać ciągłego

monitorowania i raportowania. Ważne będzie obserwowanie zmian w konkretnych przepisach i przyjęcie skutecznego, niezakłócającego zarządzania zmianą. Regularne audyty wewnętrzne mogą stanowić dobrą podstawę zgodności, ale zatrudnienie strony trzeciej do przeprowadzenia audytu zewnętrznego prawdopodobnie przyniesie bardziej kompletne lub „uczciwe” wyniki.

Przeprowadzanie ćwiczeń red-team może również pomóc zapewnić gotowość w scenariuszach z życia wziętych. Użytkownicy mogą również pomóc w przestrzeganiu przepisów, uczestnicząc w szkoleniach, które pomagają ustanowić silną kulturę cyberbezpieczeństwa w organizacji i zgłaszać niezgodności za pośrednictwem ustalonych kanałów informacji zwrotnej.

Nadążanie za zgodnością z NIS2

Ponieważ zbliża się termin 17 października, a w krótkim czasie mnóstwo przepisów staje się prawem, ważne jest, aby nie dać się przytłoczyć ani nie poddać się panice. Prawdopodobnie robisz już wszystko, co musisz zrobić, aby spełnić wymagania NIS2, o ile wiesz, w jaki sposób różne przepisy w każdym państwie członkowskim UE wpływają na Twoją organizację i masz dobrą ocenę swoich zasobów cyfrowych oraz potencjalnych luk. Następnie możesz postępować zgodnie z już ustalonymi ramami cyberbezpieczeństwa, aby spełnić wymagania NIS2 i nadążać za wszelkimi zmianami regulacyjnymi, gdy się pojawią. Posiadanie planu wdrożonego teraz w dużym stopniu przyczyni się do spełnienia i utrzymania zgodności z prawem.

Źródło:https://bitdefender.pl/podstawowe-kroki-w-celu-zapewnienia-zgodnosci-z-rozproszonym-systemem-nis2/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 11.10.2024
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.