Informacja prasowa

Warszawa, 2.12.2024

50% więcej ataków na urządzenia mobilne[1]. Czy nadchodzące regulacje zmienią zasady gry dotyczące bezpieczeństwa cyfrowego?

W 2023 roku liczba cyberataków na urządzenia mobilne osiągnęła prawie 33,8 mln przypadków, co stanowi wzrost o 50% w porównaniu z rokiem poprzednim.[2] W obliczu rosnących zagrożeń pojawią się nowe regulacje, które będą miały wpływ na kwestie bezpieczeństwa.

Odpowiadając na rosnące zainteresowanie Dyrektywą NIS 2, bolttech Poland podjął współpracę z ekspertką w tej dziedzinie – Agnieszką Wachowską, radczynią prawną i Co-Managing Partner w kancelarii Traple Konarski Podrecki i Wspólnicy. Celem tego działania jest dostarczanie klientom szczegółowego przeglądu kluczowych założeń dyrektywy oraz omówienie jej potencjalnego wpływu na przedsiębiorstwa zarządzające urządzeniami w firmie.

Dyrektywa NIS 2 – podstawowe informacje

NIS 2 (ang. Network and Information Systems Directive 2 – kontynuacja NIS 1) to dyrektywa w sprawie sieci i systemów informatycznych obejmująca zbiór przepisów dotyczących cyberbezpieczeństwa ustanowionych przez Unię Europejską. Jej głównym założeniem jest ochrona podstawowych usług i infrastruktury cyfrowej przed zagrożeniami cybernetycznymi. NIS 2 wprowadza nowe środki, które mają zapewnić, że organizacje działające w Unii Europejskiej (UE) lub współpracujące z Unią Europejską (UE) mają wysoki wspólny poziom bezpieczeństwa sieci i infrastruktury.

Dyrektywa będzie obowiązywała średnie i duże przedsiębiorstwa, które zatrudniają co najmniej 50 pracowników i których roczny obrót przekracza 10 mln euro. Obejmuje zarówno podmioty kluczowe, takie jak energetyka, bankowość czy infrastruktura cyfrowa, jak i ważne, w tym dostawców usług cyfrowych, branżę spożywczą oraz produkcję. NIS 2 wskazuje również na konieczność stosowania nowych regulacji przez mikro i małe przedsiębiorstwa, jeśli ich działalność uznana zostanie za kluczową dla gospodarki lub społeczeństwa.

Dyrektywa NIS 2 nakłada na firmy szereg obowiązków, między innymi:

- obowiązek raportowania incydentów cyberbezpieczeństwa w ciągu 24 godzin od ich wykrycia,
- wprowadzenie procedur zarządzania ryzykiem oraz systematyczne testowanie bezpieczeństwa sieci i systemów,
- zarządzanie urządzeniami mobilnymi w celu minimalizacji zagrożeń, takich jak adware, ransomware czy phishing.

Jak wskazuje Agnieszka Wachowska, radczyni prawna i Co-Managing Partner w kancelarii Traple Konarski Podrecki i Wspólnicy: *Dyrektywa NIS 2 podnosi poprzeczkę w zakresie wymogów dotyczących ochrony infrastruktury IT. Firmy muszą wdrożyć odpowiednie i proporcjonalne środki techniczne oraz organizacyjne, aby skutecznie zarządzać ryzykiem dla swoich systemów. Warto zaznaczyć, że*

[1] https://www.kaspersky.com/about/press-releases/attacks-on-mobile-devices-significantly-increase-in-2023, Luty 2024
[2] J.w.

obowiązek zarządzania ryzykiem dotyczy także urządzeń mobilnych, które uznawane są za jedno z najsłabszych ogniw w systemach IT.

Wzrost ataków na urządzenia mobilne wymaga nowych rozwiązań

Celem cyberprzestępców najczęściej są urządzenia mobilne i w 2023 roku liczba cyberataków na nie wzrosła o 50%. Zagrożenia takie jak malware, phishing czy złośliwe aplikacje mogą prowadzić do poważnych konsekwencji dla firm, w tym wycieków danych czy przestojów operacyjnych. Co więcej, cyberprzestępcy coraz częściej stosują techniki inżynierii społecznej, aby wykradać dane użytkowników, takie jak numery telefonów i pełne imiona.[3]

Unijni ustawodawcy dostrzegają zagrożenia związane z urządzeniami mobilnymi i uwzględniają je w przepisach NIS 2 – są one traktowane na równi z innymi systemami informatycznymi. Firmy będą musiały wdrożyć rozwiązania, które umożliwią zabezpieczenie urządzeń końcowych przed kradzieżą, cyberatakami oraz innymi zagrożeniami, co będzie nieodłącznym elementem budowy odpornej infrastruktury cyfrowej – dodaje Agnieszka Wachowska.

Kompleksowe wsparcie w przygotowaniu firm do zgodności z Dyrektywą NIS 2

Aby skutecznie przygotować się do wymagań Dyrektywy NIS 2, firmy muszą podjąć kroki w celu podniesienia poziomu bezpieczeństwa swojej infrastruktury IT. bolttech Poland oferuje wszechstronne rozwiązania, które pomagają firmom dostosować się do nowych regulacji w zakresie zarządzania urządzeniami mobilnymi, co jest jednym z kluczowych elementów w kontekście zapewnienia cyberbezpieczeństwa. Naszym celem jest stworzenie bezpiecznego i zgodnego z regulacjami środowiska, co nie tylko zwiększa odporność na cyberzagrożenia, ale także poprawia efektywność operacyjną – przekonuje Mariusz Pik, ekspert ds. wdrożeń z bolttech Poland.

W obliczu rosnących zagrożeń cybernetycznych, odpowiednie przygotowanie do Dyrektywy NIS 2 staje się strategicznym krokiem w budowaniu przewagi konkurencyjnej. Więcej informacji na ten temat można znaleźć w webinarze, przygotowanym przez bolttech Poland z udziałem Agnieszki Wachowskiej, radczyni prawnej i Co-Managing Partner w kancelarii Traple Konarski Podrecki i Wspólnicy. Materiał dostępny jest na: *https://nis2.bolttechdlafirm.pl/.*

***

Informacje o bolttech

bolttech to międzynarodowa firma insurtech, której misją jest zbudowanie globalnego, opartego na technologii ekosystemu ubezpieczeń. bolttech obsługuje klientów na ponad 30 rynkach w Stanach Zjednoczonych, Azji i Europie.

Bazując na kompetencjach cyfrowych i kompleksowej analizie danych, bolttech łączy ubezpieczycieli, dystrybutorów i klientów, aby ułatwić kupowanie i sprzedawanie ubezpieczeń i produktów ochronnych. Więcej informacji można znaleźć na stronie www.bolttech.io.

Informacje o ekspercie

Agnieszka Wachowska – Radczyni prawna, Co-Managing Partner kancelarii Traple Konarski Podrecki i Wspólnicy. Ekspert z kilkunastoletnim doświadczeniem w obsłudze projektów związanych z IT. Specjalizuje się w problematyce prawnej branży IT i nowych technologii. Od początku kariery prawniczej doradza w zakresie zagadnień związanych z prawem IT, zamówieniami publicznymi na dostawy i usługi IT, a także w obszarze cyberbezpieczeństwa i prawa autorskiego.

[3] https://www.kaspersky.com/about/press-releases/attacks-on-mobile-devices-significantly-increase-in-2023, Luty 2024

Kontakt dla mediów:
Aneta Szerszeniewska
aneta.szerszeniewska@38pr.pl
tel. +48 509453 985