

Warszawa, 12 lutego 2024

Cyberbezpieczeństwo, dyrektywa Unii Europejskiej a nasze działania – informacja prasowa

Wobec rosnących zagrożeń w sferze cyfrowej, zarówno o charakterze politycznym, jak i kryminalnym, prawodawca unijny dynamicznie rozwija przepisy, które mają ułatwić stawienie czoła tym zagrożeniom. Jednym z ważniejszych aktów w obszarze cyberbezpieczeństwa jest dyrektywa z 2022 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (dyrektywa 2022/2555), nazywana w skrócie NIS2, która zastąpiła dyrektywę z 2016.

Celem nowej dyrektywy jest wzmocnienie i uszczelnienie systemu cyberbezpieczeństwa w państwach UE. Wzmocniony system cyberbezpieczeństwa w krajach unijnych oraz silniejsza współpraca między państwami członkowskimi nie zapewni poprawy bezpieczeństwa sprzętu, oprogramowania i aplikacji, jeżeli nie zostaną zachowane podstawowe zasady korzystania z narzędzi informatycznych. Prawodawca unijny nie pozostawia wątpliwości: wdrażanie tzw. cyberhigieny przyczyni się do zapewnienia ochrony przed cyberzagrożeniami.

Stąd w dyrektywie NIS 2 państwa członkowskie zostały zobowiązane do przyjęcia w ramach krajowej strategii cyberbezpieczeństwa m.in. wytycznych dotyczących dobrych praktyk i kontroli w zakresie cyberhigieny, która winna być zachowana przez cały sektor publiczny, w szczególności przez administrację. Dlatego, wysiłkiem ekspertów Federacji Przedsiębiorców Polskich, przygotowujemy „**Ogólne Zasady Cyberbezpieczeństwa Dla Instytucji Rządowych**”.

Zasady to zbiór rekomendacji konkretnych działań i zachowań skierowanych do instytucji publicznych i ich pracowników. Zaczynamy od podstaw, tj. wskazania osób odpowiedzialnych za zarządzanie cyberbezpieczeństwem w każdym urzędzie czy jednostce. Polityka i wytyczne dotyczące cyberbezpieczeństwa powinny zostać opracowane i opublikowane, aby wszyscy pracownicy mogli się z nimi zapoznać. Cyklicznie należy przeprowadzać audyty, a ochrona danych – w zgodzie z unijnymi przepisami – stanowi priorytet. Konieczne jest przeprowadzanie szkoleń dla podwyższenia świadomości pracowników, a dostawcy sprzętu i oprogramowania winni spełniać odpowiednie standardy.

Schodząc na poziom bliższy każdemu użytkownikowi sprzętu i oprogramowania, należy pamiętać o korzystaniu z długich haseł, wykorzystując przy ich tworzeniu cyfry i znaki specjalne, a same hasła regularnie zmieniać i nie stosować tego samego hasła w więcej niż jednym miejscu. Można sięgnąć po zweryfikowane programy typu „menedżer haseł”, aby ułatwić codzienne funkcjonowanie – wystarczy zapamiętać jedno hasło, a pozostałe są bezpiecznie przechowywane w tym narzędziu.

Konieczne należy chronić sprzęt, pocztę elektroniczną, stosować szyfrowanie danych, a używając sprzętu mobilnego każda instytucja powinna zarządzać tymi urządzeniami, chociażby wymuszając logowanie za pomocą hasła/kodu PIN, zapewnienie zainstalowania i aktualizacji oprogramowania antywirusowego, etc. Nie zapominamy o rzeczach banalnych jak bezpieczeństwo telefonów, tabletów czy komputerów – nie pozostawiamy ich bez opieki w trakcie podróży czy spotkania służbowego poza biurem, a także nie przyklejamy do sprzętu karteczki z hasłem do logowania.

Wśród licznych rekomendowanych działań zwracamy także uwagę na potrzebę zachowania szczególnej ostrożności przy korzystaniu z poczty elektronicznej, zwłaszcza podejrzliwości wobec załączników i linków w sytuacji, gdy nie do końca jesteśmy pewni nadawcy. Cyberprzestępcy nagminnie podszywają się pod instytucje publiczne, znane firmy, także kurierskie i finansowe, testując naszą czujność rzekomymi informacjami o przesyłce czekającej na odbiór albo o nieopłaconej fakturze. Jeśli nie jesteśmy pewni wiarygodności nadawcy, skontaktujmy się z osobą wyznaczoną do dbania o cyberbezpieczeństwo w naszej organizacji.

Kompletny materiał zawierający wszystkie rekomendacje eksperci FPP przedstawia już wkrótce.

Kontakt dla mediów:

Dominika Chirek

Dyrektor Komunikacji i PR

t: +48 665 553 288

m: dominika.chirek@federacjaprzedsiebiorcow.pl

Federacja Przedsiębiorców Polskich

news@federacjaprzedsiebiorcow.pl

www.federacjaprzedsiebiorcow.pl