NASK

CyberBHP

Cyberhigiena to podstawa!

Nie musisz być ekspertem, żeby zwiększyć bezpieczeństwo cyfrowe swojej firmy. Liczy się nie tylko specjalistyczna wiedza czy wyszukane narzędzia i programy, ale przede wszystkim codzienne stosowanie podstawowych zasad cyberhigieny i zdrowych cyfrowych nawyków.

Cyberbezpieczeństwo w mikro-, małych i średnich przedsiębiorstwach (MŚP)

Poczta, wiadomości, załączniki, linki

Nie otwieraj załączników ani nie klikaj w linki, które otrzymasz w wiadomościach e-mail, jeśli nie masz pewności, co się w nich znajduje.

Korzystaj z rozwiązań, które ograniczą liczbę wiadomości typu spam.

Zawsze zwracaj uwagę na nadawcę wiadomości – weryfikuj adres e-mail.

Szczególnie ostrożnie sprawdzaj wiadomości, które wywierają presję, grożą i zmuszają do natychmiastowego działania – takie jak informacja o niezapłaconej fakturze, mandacie, zaległości w płatnościach itp.

Zanim otworzysz załącznik lub dokonasz płatności, zweryfikuj, czy wiadomość jest prawdziwa – w razie wątpliwości skontaktuj się z nadawcą (np. poprzez rozmowę telefoniczną).

Podobne zasady stosuj również wobec wiadomości SMS oraz otrzymywanych za pośrednictwem komunikatorów.

NASK

Oprogramowanie i sprzęt

Korzystaj tylko z legalnego oprogramowania – kupuj je bezpośrednio u producenta lub pobieraj tylko ze sprawdzonych i oficjalnych stron oraz sklepów.

Pamiętaj o aktualizowaniu swojego sprzętu, oprogramowania i aplikacji, z których korzystasz. Włącz automatyczne aktualizacje.

Zawsze blokuj lub wyłączaj sprzęt, gdy od niego odchodzisz lub przestajesz z niego korzystać.

Nie używaj sprzętu służbowego do celów prywatnych i prywatnego do celów służbowych. Jeżeli masz jeden komputer, stwórz dwa odrębne konta dla każdej z ról.

Korzystaj z programów antywirusowych.

Hasła

Silne i bezpieczne hasło powinno być długie (co najmniej 12 znaków, ale rekomendowane są dłuższe), a przy tym łatwe do zapamiętania. Dobrym rozwiązaniem może być np. cytat z piosenki, przysłowie, tytuł filmu/serialu – fraza, która będzie zmodyfikowana w sposób znany tylko Tobie (np. WlazlKostekNaMostekIStuka!).

Silne hasło nie wymaga cyklicznych, częstych modyfikacji. Należy je jednak zmienić, jeśli zaistniało podejrzenie, że wyciekło.

Hasła powinny być unikatowe – jedna usługa, jedno hasło.

Stosuj uwierzytelnianie dwuskładnikowe w usługach, z których korzystasz. Rozważ korzystanie z kluczy bezpieczeństwa (U2F) lub używaj przeznaczonych do tego aplikacji.

NASK

Ważne!

Zapoznaj się z polityką bezpieczeństwa i procedurami, jakie obowiązują w Twojej firmie.
Jeśli zdarzy się incydent bezpieczeństwa, postępuj zgodnie z nimi.

Bierz udział w szkoleniach i kursach, które zwiększają wiedzę z zakresu cyberbezpieczeństwa.

Śledź strony i profile instytucji, które zajmują się cyberbezpieczeństwem. Dzięki temu będziesz na bieżąco dowiadywać się o różnych zagrożeniach i kampaniach skierowanych przeciwko użytkownikom internetu.

NASK

Finansowane ze środków Kancelarii Prezesa Rady Ministrów.
Publikacja wyraża jedynie poglądy autorów i nie może być utożsamiana z oficjalnym stanowiskiem Kancelarii Prezesa Rady Ministrów.