NASK

CyberBHP

Cyberbezpieczeństwo
w miejscu pracy - wskazówki dla pracodawcy

Cyberbezpieczeństwo to jeden z najważniejszych aspektów prawidłowego i bezpiecznego działania firmy, zwłaszcza w dobie powszechnej cyfryzacji i automatyzacji procesów biznesowych. Dbałość o bezpieczeństwo danych i systemów komputerowych w organizacji wymaga zaangażowania zarówno pracowników, jak i pracodawcy. **Regularne szkolenia, odpowiednie zabezpieczenia, świadomość ryzyka oraz reakcja na incydenty to kluczowe aspekty skutecznego systemu cyberbezpieczeństwa w firmie.** Często zdarza się, że to właśnie obowiązujące procedury i ludzka przezorność udaremniają bardzo dobrze przygotowane ataki socjotechniczne.

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

1. Polityka bezpieczeństwa. Wprowadź jasną i spójną politykę bezpieczeństwa w firmie, która określi zasady, procedury i narzędzia, jakie będą stosowane w firmie w celu zapobiegania cyberzagrożeniom. Zdefiniuj wytyczne dotyczące używania silnych haseł i innych metod uwierzytelniania (np. biometrii), przechowywania i ochrony danych, korzystania z zasobów sieciowych, zabezpieczania urządzeń przenośnych i innych aspektów związanych z cyberbezpieczeństwem.

2. Szkolenia i edukacja. Zapewnij regularne szkolenia z cyberbezpieczeństwa dla wszystkich pracowników, aby zwiększyć ich świadomość na temat cyberzagrożeń (tzw. security awareness), jak również nauczyć ich, jak rozpoznawać potencjalne ataki i jak działać w przypadku podejrzenia naruszenia bezpieczeństwa.

3. Hasła i uwierzytelnianie. Wymagaj, aby pracownicy korzystali z silnych i unikatowych haseł (jedno hasło = jedno konto), każdy z pracowników powinien korzystać z mechanizmu podwójnego uwierzytelnienia przy dostępie do swoich kont służbowych. Rekomendowane jest także stosowanie kluczy sprzętowych 2FA dla wszystkich działów firmowych i pracowników, którzy realizują newralgiczne działania związane m.in. z finansami firmowymi.

4. Aktualizacje i ochrona systemów. Upewnij się, że wszystkie systemy, oprogramowanie, aplikacje i urządzenia są regularnie aktualizowane. Zapewnienie najnowszych poprawek bezpieczeństwa jest kluczowe dla minimalizowania luk w zabezpieczeniach. Stosowanie odpowiednich narzędzi zabezpieczających przed cyberatakami, takich jak antywirusy, zapory sieciowe i programy do wykrywania i reagowania na incydenty stanowi podstawową warstwę ochrony.

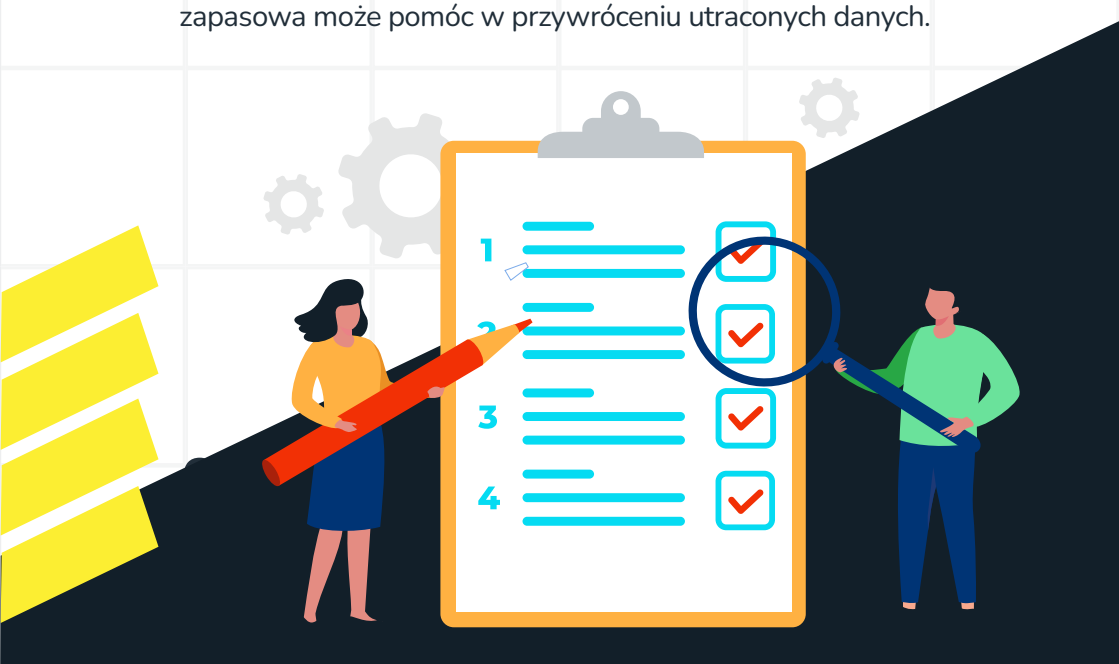
5. Monitorowanie systemów. zapewnij wdrożenie narzędzi monitorujących ruch sieciowy, które pozwolą na wykrywanie podejrzanych aktywności i wczesne reagowanie na potencjalne zagrożenia.

NASK

6. Zarządzanie uprawnieniami. Przeglądaj i aktualizuj regularnie uprawnienia dostępu pracowników do różnych systemów, aplikacji i danych. Nadawaj tylko niezbędne uprawnienia zgodnie z rolami i obowiązkami pracowników. Ogranicz dostęp do poufnych danych tylko dla tych, którzy go potrzebują do wykonywania swoich obowiązków. Przyznawaj uprawnienia na zasadzie najmniejszych przywilejów (ang. least privilege) - tylko tyle, ile jest niezbędne do wykonywania pracy.

7. Bezpieczne przechowywanie i zarządzanie danymi. Zadbaj o bezpieczne przechowywanie danych firmy oraz klientów i stosuj procedury zarządzania nimi, takie jak szyfrowanie, zabezpieczenie przed utratą oraz regularne kopie zapasowe.

8. Kopie zapasowe danych. Regularnie wykonuj kopie zapasowe danych i przechowuj je w bezpiecznym miejscu, na przykład zaszyfrowane w chmurze lub na zewnętrznym, odłączonym od sieci nośniku. Stosuj zasadę 3-2-1. Ważne pliki powinny być przechowywane w 3 kopiach, na co najmniej 2 różnych nośnikach, z czego 1 z nich powinien znajdować się poza siedzibą firmy. W przypadku awarii systemu lub ataku ransomware, kopia zapasowa może pomóc w przywróceniu utraconych danych.



dotyczącą bezpiecznego korzystania z takich urządzeń i dostępu do sieci. Wymagaj od pracowników instalacji oprogramowania ochronnego na tych urządzeniach.

10. Zabezpieczenie urządzeń przenośnych. Wprowadź politykę zabezpieczania urządzeń przenośnych używanych przez pracowników (np. smartfony, tablety, laptopy służbowe), poprzez zainstalowanie oprogramowania antywirusowego, aktualizacje systemów i regularne przeglądy. Wymagaj stosowania silnych haseł, szyfrowania i zdalnego usuwania danych w przypadku kradzieży lub zagubienia.

11. Reagowanie na incydenty. Opracuj plan reagowania na incydenty bezpieczeństwa, który określi, jakie działania należy podjąć w przypadku ataku lub naruszenia danych. Wszyscy pracownicy powinni być świadomi tego planu i wiedzieć, jak i do kogo zgłaszać incydenty. Szybka reakcja pomoże ograniczyć skutki ataku i zminimalizować straty.

12. Audyt bezpieczeństwa. Regularnie przeprowadzaj audyty bezpieczeństwa, aby ocenić poziom ryzyka, skuteczność zastosowanych środków bezpieczeństwa i identyfikować ewentualne zagrożenia i obszary do ulepszeń.

Wprowadzenie tych działań nie tylko pozwoli na ochronę firmy przed cyberprzestępcami, ale także przyniesie korzyści w postaci zwiększenia zaufania klientów, podniesienia efektywności pracy i poprawy wizerunku firmy.