CYBERBEZPIECZEŃSTWO W FIRMIE INFORMATYCZNEJ

Aleksandra Rokita

Czym jest cyberbezpieczeństwo?

Cyberbezpieczeństwo, znane także jako bezpieczeństwo informatyczne lub bezpieczeństwo cybernetyczne, odnosi się do praktyk, technologii, procedur i środków mających na celu ochronę systemów komputerowych, sieci, danych oraz infrastruktury przed atakami, nieautoryzowanym dostępem, kradzieżą danych, złośliwym oprogramowaniem i innymi zagrożeniami.

W obliczu ciągłego rozwoju technologii i coraz bardziej złożonych zagrożeń ze strony cyberprzestępców, cyberbezpieczeństwo staje się kluczowym obszarem dla przedsiębiorstw, instytucji publicznych i jednostek indywidualnych. Efektywne środki cyberbezpieczeństwa wymagają ciągłego monitorowania, dostosowywania i doskonalenia, aby skutecznie chronić przed różnorodnymi zagrożeniami.

Jakie są cele cyberbezpieczeństwa?

Poufność:
Zapewnienie, że tylko uprawnione osoby lub systemy mają dostęp do określonych informacji.

Integralność:
Gwarancja, że dane nie zostały zmienione nielegalnie ani nieautoryzowanie, zachowanie ich integralności.

Dostępność:
Zapewnienie, że systemy i dane są dostępne, gdy są potrzebne, i że są odporne na ataki.

Autoryzacja:
Przyznawanie uprawnień dostępu użytkownikom lub systemom.Potwierdzanie tożsamości użytkowników i systemów, aby zapobiegać nieautoryzowanemu dostępowi.

Świadomość cyberbezpieczeństwa:
Edukacja i szkolenia pracowników oraz użytkowników w zakresie zagrożeń i praktyk bezpieczeństwa online.

Jak dbać o cyberbezpieczeństwo w firmie?

Odpowiednie dbanie o cyberbezpieczeństwo w firmie jest kluczowe dla ochrony poufności, integralności i dostępności informacji oraz uniknięcia poważnych skutków związanych z atakami lub naruszeniem bezpieczeństwa. Oto kilka kluczowych kroków, które firma może podjąć, aby zadbać o cyberbezpieczeństwo.

Polityka bezpieczeństwa informatycznego

Opracuj i wdroż formalną politykę bezpieczeństwa informatycznego, która obejmuje zasady dotyczące dostępu do systemów, zarządzania hasłami, korzystania z urządzeń mobilnych, a także środki zarządzania ryzykiem.

Szkolenia dla Pracowników

Przeprowadzaj regularne szkolenia w zakresie cyberbezpieczeństwa dla pracowników, zwracając uwagę na identyfikację zagrożeń, rozpoznawanie phishingu, bezpieczne korzystanie z urządzeń i sieci. Zachęcaj pracowników do zgłaszania potencjalnych zagrożeń oraz utrzymuj otwartą komunikację w kwestiach bezpieczeństwa.

Instalacja i regularna aktualizacja oprogramowania

Instaluj oprogramowania antywirusowe na wszystkich urządzeniach w firmie. Zapewniaj regularne aktualizacje oprogramowania, w tym systemów operacyjnych, aplikacji i oprogramowania zabezpieczającego, aby wykorzystywać najnowsze łatki bezpieczeństwa.

Ochrona danych

Regularnie twórz kopie zapasowe danych i przechowuj je w bezpiecznym miejscu. W razie ataku lub awarii systemu, można przywrócić dane z kopii zapasowej. Ogranicz dostęp do danych tylko do osób, które wymagają takich uprawnień w ramach ich obowiązków służbowych. Regularnie przeglądaj i aktualizuj te uprawnienia.

Co jeszcze możesz zrobić aby poprawić bezpieczeństwo swojej firmy?

-Monitorowanie Działań

-Ustalanie Polityki Hasłowej

-Zabezpieczenia Fizyczne

-Zarządzanie Ryzykiem

-Szyfrowanie danych

-Regularne audyty bezpieczeństwa

Jakie pytania zadać na temat cyberbezpieczeństwa w firmie, w której chciałbyś pracować?

1.Jakie środki bezpieczeństwa są obecnie wdrożone w firmie?

Pytanie to pozwala zrozumieć aktualny stan bezpieczeństwa w firmie.

2. Czy firma posiada politykę bezpieczeństwa informatycznego?

Dowiesz się, czy firma ma formalne wytyczne i procedury związane z bezpieczeństwem informatycznym.

3. Jakie dane są przechowywane i przetwarzane przez firmę, a także w jakim celu?

To pytanie pozwala zidentyfikować, jakie informacje są istotne dla bezpieczeństwa i jak są one chronione.

4. Jakie środki zabezpieczające są wdrożone w przypadku ataków hakerskich lub awarii systemów?

Sprawdzenie, czy firma ma plan reagowania na incydenty bezpieczeństwa.

Komu powierzyć bezpieczeństwo?

Istnieje wiele firm na całym świecie, które specjalizują się w dziedzinie cyberbezpieczeństwa. Przed wyborem dostawcy usług bezpieczeństwa warto przeprowadzić analizę i dostosować wybór do konkretnych potrzeb i charakteru działalności firmy.

Oto wykaz niektórych znanych firm zajmujących się usługami z zakresu cyberbezpieczeństwa.

McAfee

McAfee to globalny dostawca rozwiązań bezpieczeństwa informatycznego oferujący oprogramowanie antywirusowe, zabezpieczające przed zagrożeniami oraz rozwiązania dla przedsiębiorstw.

Cisco Systems:

Cisco to globalny dostawca sprzętu sieciowego, ale także oferuje rozwiązania z zakresu bezpieczeństwa sieciowego i cyberbezpieczeństwa.

Symantec

Symantec to jedna z największych firm świadczących usługi bezpieczeństwa informatycznego, w tym oprogramowanie antywirusowe, zabezpieczające przed zagrożeniami i usługi związane z zarządzaniem zagrożeniami.

Dziękuję za uwagę.

Aleksandra Rokita
173697
L05 2EF-DI