PREZENTACJA NA TEMAT

„Metody fizyczne przeciwdziałania zagrożeniom informacji i systemów teleinformatycznych organizacji”

ANASTASIIA TARNAVSKA 99817

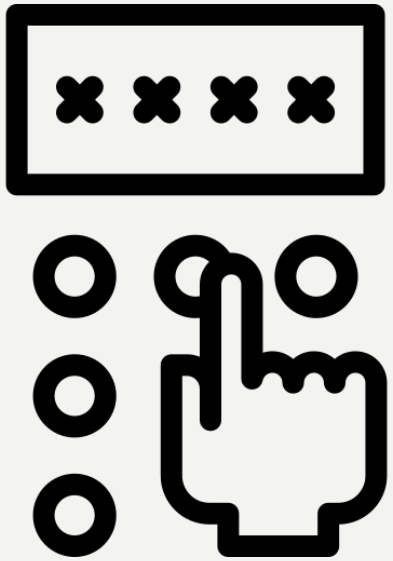
Kontrola dostępu fizycznego

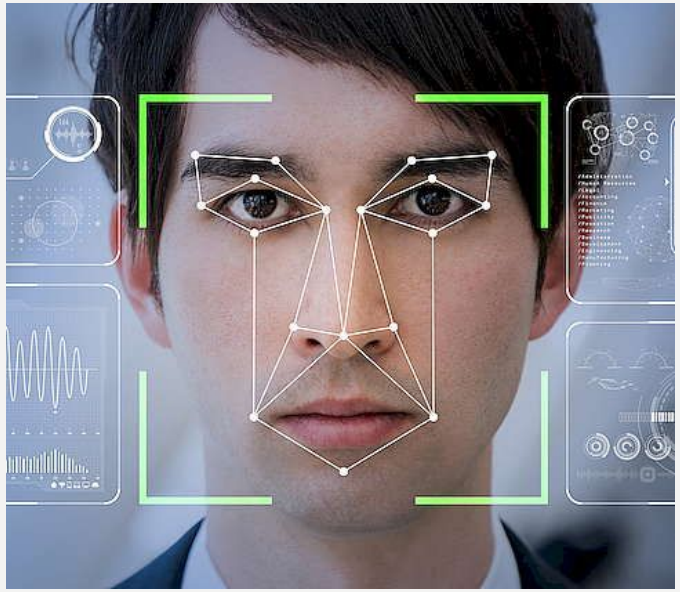
Kontrola dostępu fizycznego w firmie to proces zarządzania i monitorowania, kto ma dostęp do różnych obszarów i zasobów wewnątrz firmy. Jest to istotny element zapewnienia bezpieczeństwa pracowników, klientów, danych i mienia firmy. Są takie kluczowe koncepcji i praktyki związane z kontrolą dostępu fizycznego w firmie:

- Systemy kontroli dostępu
- Zarządzanie identyfikacją i autoryzacją
- Monitorowanie i rejestracja dostępu
- Zasady dostępu i polityka bezpieczeństwa
- Zgodność z przepisami prawnymi
- Regularne przeglądy i testy
- Szkolenie pracowników

Systemy kontroli dostępu

Firma może używać różnych systemów, takich jak karty dostępu, kody PIN, czytniki biometryczne (np. odciski palców lub rozpoznawanie twarzy) do kontrolowania dostępu do budynków, pomieszczeń lub komputerów





Zarządzanie identyfikacją i autoryzacją

Pracownicy i inni użytkownicy powinni być identyfikowani i autoryzowani do dostępu do określonych obszarów lub danych na podstawie ich roli i uprawnień w firmie.

Monitorowanie i rejestracja dostępu

Systemy kontroli dostępu powinny monitorować, kto, kiedy i gdzie próbuje uzyskać dostęp. Wszystkie próby dostępu, zarówno udane, jak i nieudane, powinny być rejestrowane w celu audytu i analizy.

Zasady dostępu i polityka bezpieczeństwa

Firma powinna opracować politykę bezpieczeństwa, która określa, kto ma dostęp do jakich zasobów, jakie są procedury dostępu i jakie sankcje obowiązują w przypadku naruszenia tych zasad.

Zgodność z przepisami prawnym

Firma powinna również zadbać o zgodność z przepisami prawnymi i regulacjami dotyczącymi prywatności danych i bezpieczeństwa, zwłaszcza jeśli przetwarza wrażliwe informacje.

W tym:

1. Ochrona danych osobowych
2. Przepisy sektorowe
3. Przepisy dotyczące budynków i infrastruktury
4. Przepisy dotyczące monitoringu i przechowywania nagrań
5. Odpowiedzialność za naruszenia bezpieczeństwa
6. Audyt i inspekcje
7. Sankcje za naruszenia

Regularne przeglądy i testy

Systemy kontroli dostępu powinny być regularnie przeglądane i testowane, aby upewnić się, że są skuteczne i zaktualizowane zgodnie z nowymi zagrożeniami.

Szkolenia pracowników

- ***Sensybilizacja pracowników:*** Szkolenie pracowników powinno zaczynać się od podstaw, a mianowicie od zrozumienia przez nich znaczenia bezpieczeństwa informacji. Pracownicy powinni zdawać sobie sprawę z potencjalnych zagrożeń i skutków, jakie mogą wyniknąć z naruszenia bezpieczeństwa.

- ***Polityki i procedury:*** Pracownicy powinni być zapoznani z politykami i procedurami dotyczącymi bezpieczeństwa informacji obowiązującymi w organizacji. To obejmuje zasady korzystania z systemów, zarządzania hasłami, przechowywania danych oraz zgłaszania incydentów bezpieczeństwa.

- ***Szkolenia w zakresie phishingu:*** Szkolenia na temat phishingu są istotne, ponieważ phishing jest jednym z najczęstszych sposobów ataków. Pracownicy powinni być w stanie rozpoznać podejrzane e-maile i strony internetowe oraz wiedzieć, jak na nie reagować.

- ***Szkolenia w zakresie zarządzania hasłami:*** Pracownicy powinni być informowani o zasadach tworzenia silnych haseł i regularnej ich zmiany.

- ***Szkolenia w zakresie zarządzania urządzeniami mobilnymi:*** Jeśli pracownicy korzystają z urządzeń mobilnych w celach służbowych, powinni być szkoleni w zakresie bezpiecznego korzystania z tych urządzeń i instalowania aplikacji tylko z wiarygodnych źródeł.

Zabezpieczenia przed uszkodzeniem:

Zastosowanie zabezpieczeń przed uszkodzeniem, takich jak gaśnice, systemy przeciwpożarowe i czujniki wycieku wody, aby chronić sprzęt przed pożarami, zalaniem i innymi awariami.

Zasilanie awaryjne:

Wykorzystywanie zasilaczy awaryjnych (UPS) i generatorów prądotwórczych, aby zapewnić ciągłość zasilania i ochronić przed awariami związanymi z przerwami w dostawie prądu.

Segregacja i oznaczanie:

Segregowanie i oznaczanie kabli i urządzeń, aby ułatwić identyfikację i zarządzanie infrastrukturą.

Zabezpieczenia przeciwwłamaniowe:

- **Bariery antywłamaniowe**: Wykorzystanie bariery antywłamaniowej, takiej jak metalowe kratki lub ekrany na oknach i drzwiach, aby utrudnić dostęp włamywaczom.

- **Oznaczenia włamania**: Oznaczanie sprzętu i urządzeń specjalnymi farbami lub etykietami, które trudno usunąć, aby utrudnić odsprzedaż skradzionego mienia.

- **Systemy śledzenia:** Użycie technologii do śledzenia skradzionego sprzętu, na przykład

System teleinformatyczny jest poddany bardzo dużej i różnorodnej gamie zagrożeń. W związku z coraz bardziej masowym wykorzystaniem systemów teleinformatycznych we wszystkich rodzajach działalności, problem występujących zagrożeń i sposobów przeciwdziałania im staje się jednym z kluczowych problemów związanych z elektronicznym przetwarzaniem danych.

Powszechność przetwarzania danych w systemach komputerowych powoduje zarówno zwiększenie skali zagrożeń jak i zmniejsza możliwość bezpośredniej kontroli poszczególnych etapów procesu przetwarzania. Integracja systemów powoduje, że np. wyniki uzyskiwane w jednym systemie są za pośrednictwem interfejsów przekazywane do następnego i błąd powstały czy wywołany w jednym systemie jest przenoszony dalej na zasadzie łańcuchowej. Możliwość bezpośredniej kontroli, a co za tym idzie eliminowania tego niekorzystnego zjawiska bez odpowiednich procedur i narzędzi jest bardzo ograniczona.

Bibliografia

https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-2261b4a4-7c1f-4239-a3b7-45000a07d698/c

http://widsystem.pl/sposoby-zapobiegania-zagrozeniom

http://www.iniejawna.pl/pomoce/przeciw_zagr.html

https://odo.wip.pl/analiza-ryzyka/analiza-ryzyka-w-twojej-organizacji-krok-po-kroku-2406.html

https://zpe.gov.pl/a/inne-zagrozenia-naturalne

https://www.flaticon.com