agileo.it
Dbamy o Twoje Bezpieczeństwo

Cyberbezpieczeństwo - Praktyczne Aspekty Bezpieczeństwa

z uwzględnieniem specyfiki JST

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Plan Szkolenia

agileo.it
Dbamy o Twoje Bezpieczeństwo

1. Wprowadzenie do cyberbezpieczeństwa
2. Typy zagrożeń w cyberprzestrzeni
3. Regulacje i przepisy prawa
4. Zasady bezpieczeństwa i praktyki
5. Reagowanie na incydenty i planowanie awaryjne
6. Q&A

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

NOTATKI: .....
.....
.....
.....
.....
.....

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

agileo.it

Wprowadzenie do cyberbezpieczeństwa

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

Czym jest cyberbezpieczeństwo

Ochrona danych i urządzeń
Cyberbezpieczeństwo koncentruje się na ochronie komputerów, serwerów, urządzeń mobilnych i systemów przed potężnymi
zagrożeniami. Ważne jest zabezpieczenie danych przed atakami.

Edukacja w zakresie cyberbezpieczeństwa
W obliczu stale zmieniających się zagrożeń, edukacja w zakresie cyberbezpieczeństwa jest kluczowa dla ochrony danych. Ciągłe aktualizowanie wiedzy jest niezbędne.

Zagrożenia cyfrowe
W dziedzinie cyberbezpieczeństwa istnieje wiele zagrożeń, takich jak malware, phishing czy ataki DDoS. Zrozumienie tych zagrożeń jest kluczowe.

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

NOTATKI: .....

.....

.....

.....

.....

.....

Dlaczego cyberbezpieczeństwo jest ważne?

Kluczowa rola cyberbezpieczeństwa

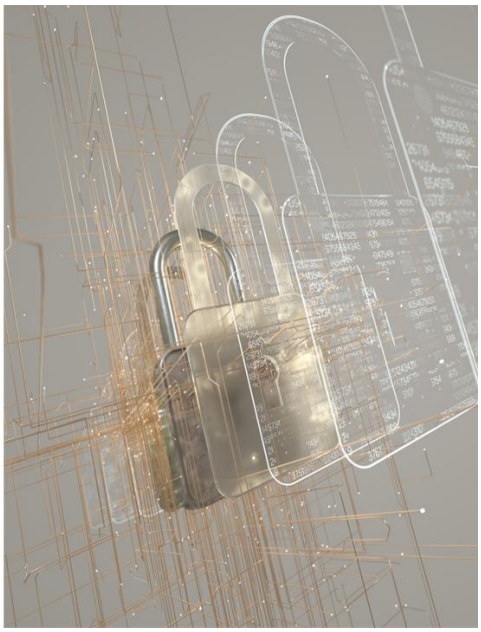
Cyberbezpieczeństwo jest niezbędne w erze cyfrowej, aby chronić dane przechowywane online oraz zapewnić bezpieczeństwo użytkowników.

Skutki naruszenia bezpieczeństwa

Naruszenia bezpieczeństwa mogą prowadzić do katastrofalnych skutków, takich jak utrata danych i usunięcie reputacji organizacji.

Ochrona danych osobowych

Właściwe cyberbezpieczeństwo chroni dane osobowe przed kradzieżą i nieautoryzowanym dostępem, co jest kluczowe w dzisiejszym świecie.



AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

Kluczowe zagadnienia związane z cyberbezpieczeństwem

Zarządzanie ryzykiem

Zarządzanie ryzykiem w cyberbezpieczeństwie polega na identyfikacji i ocenie zagrożeń oraz wdrażaniu odpowiednich środków ochrony.

Zgodność z regulacjami

Zgodność z regulacjami jest kluczowa dla ochrony danych i wymaga przestrzegania przepisów prawnych dotyczących bezpieczeństwa informacji.

Edukacja użytkowników

Edukacja użytkowników w zakresie zagrożeń cybernetycznych i zasad ochrony informacji jest niezbędna do zapobiegania atakom.

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

NOTATKI: .....

.....

.....

.....

.....

.....

agileo.it

Typy zagrożeń w cyberprzestrzeni

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

Przegląd statystyk oraz trendów w cyberbezpieczeństwie

Wzrost liczby cyberataków

Statystyki wskazują na znaczący wzrost liczby cyberataków w ostatnich latach, co wymaga pilnej uwagi.

Złożoność zagrożeń

Złożoność cyberzagrożeń rośnie, co czyni je trudniejszymi do wykrycia i obrony przed nimi.

Śledzenie trendów

Śledzenie trendów w cyberbezpieczeństwie pomaga w identyfikacji nowych zagrożeń i przygotowaniu się na nie.

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

NOTATKI: .....

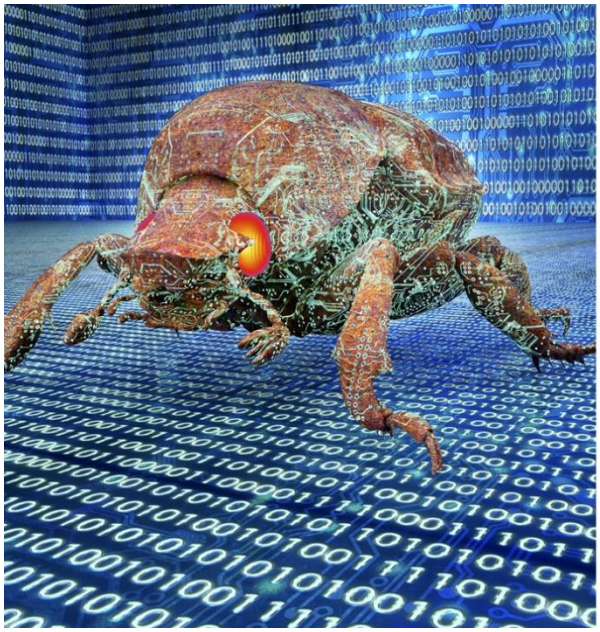
.....

.....

.....

.....

.....



Malware (wirusy, trojany, robaki itp.)

Definicja malware

Malware to ogólna kategoria złośliwego oprogramowania, które ma na celu zakłócanie systemów komputerowych oraz ich funkcjonowania.

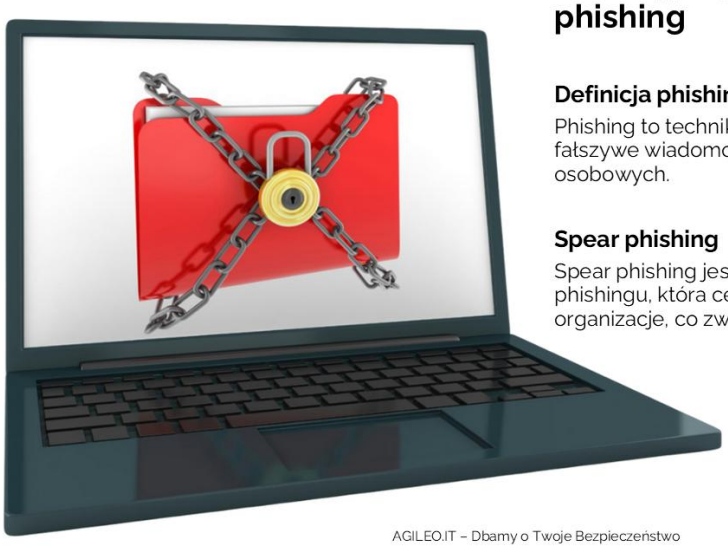
Rodzaje malware

Do typowych form malware należą wirusy, trojany, robaki oraz inne złośliwe programy, które mogą zagrażać danym użytkowników.

Skutki działania malware

Malware może powodować poważne uszkodzenia danych oraz prowadzić do utraty informacji i zasobów w systemach komputerowych.

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo



Ataki typu phishing i spear phishing

Definicja phishingu

Phishing to technika oszustwa, która wykorzystuje fałszywe wiadomości e-mail do wyłudzenia danych osobowych.

Spear phishing

Spear phishing jest bardziej ukierunkowaną formą phishingu, która celuje w konkretne osoby lub organizacje, co zwiększa jej skuteczność.

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

NOTATKI: .....

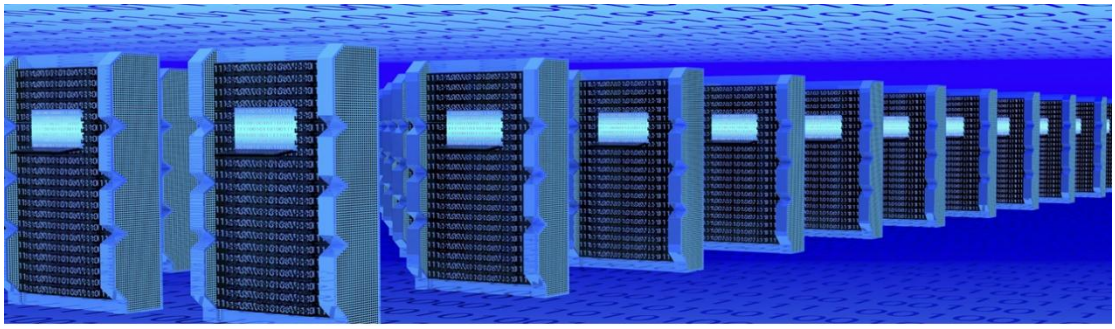
.....

.....

.....

.....

.....



Ataki DDoS

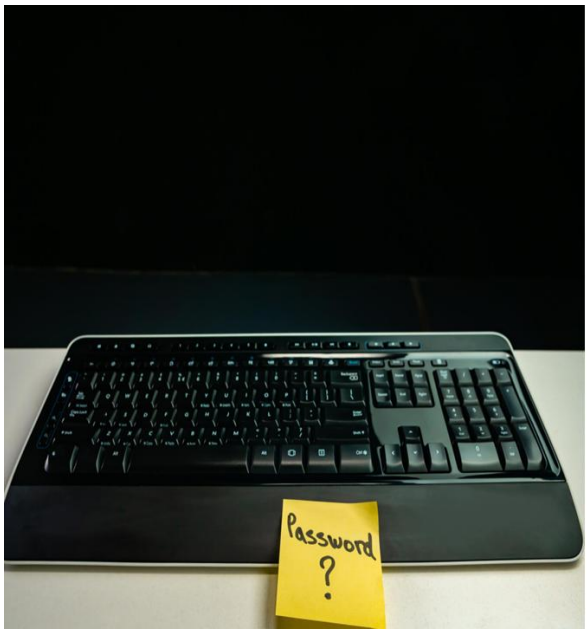
Definicja ataków DDoS

Ataki DDoS polegają na przeciążeniu systemu przez masowe wysyłanie żądań z różnych źródeł.

Cele ataków DDoS

Celem ataków DDoS jest zablokowanie dostępu do usług lub aplikacji, co uniemożliwia ich użytkowanie.

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo



Ataki ransomware

Definicja ransomware

Ransomware to złośliwe oprogramowanie, które blokuje dostęp do systemu komputerowego i żąda okupu za jego odblokowanie.

Ryzyko utraty danych

Ataki ransomware są niebezpieczne, ponieważ mogą prowadzić do poważnej utraty danych, co może mieć konsekwencje finansowe i reputacyjne.

Jak działa ransomware

Ransomware infiltruje system, szyfrując pliki i uniemożliwiając użytkownikom dostęp do nich, aż do zapłacenia okupu.

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

NOTATKI: .....

.....

.....

.....

.....

.....

Zagrożenia związane z sieciami społecznościowymi

Oszustwa internetowe

Sieci społecznościowe mogą być polem do działania dla oszustów, którzy wykorzystują fałszywe konta i oferty, aby wyłudzić pieniądze od użytkowników.

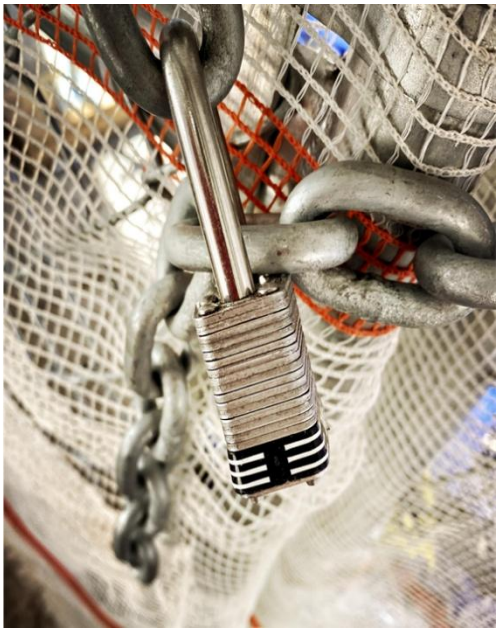
Phishing

Phishing jest powszechnym zagrożeniem w sieciach społecznościowych, gdzie oszuści próbują zdobyć dane osobowe użytkowników za pomocą fałszywych linków i wiadomości.

Utrata prywatności

Użytkownicy sieci społecznościowych mogą nieświadomie ujawniać swoje dane osobowe, co może prowadzić do utraty prywatności i niechcianych konsekwencji.

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo



agileo.it

Wymogi prawne i regulacyjne

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

NOTATKI: .....

.....

.....

.....

.....

Regulacje prawne

- Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC)
- Krajowe Ramy Interoperacyjności (KRI)
- Rozporządzenie o Ochronie Danych Osobowych (RODO)
- Dyrektywa NIS2 – nowe wymagania dla cyberbezpieczeństwa

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

Kluczowe obowiązki wynikające z NIS2

- Wdrożenie środków technicznych i organizacyjnych
- Zarządzanie ryzykiem cybernetycznym
- Kompleksowe zarządzanie incydentami
- Zapewnienie odporności i ciągłości działania
- Wyznaczenie osoby/osób do kontaktu z CSIRT

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

NOTATKI: .....

.....

.....

.....

.....

agileo.it

Normy i standardy

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

Normy międzynarodowe ISO/IEC

- ISO/IEC 27001 – zarządzanie bezpieczeństwem informacji
- ISO/IEC 22301 – ciągłość działania
- ISO/IEC 27002 – katalog zabezpieczeń
- ISO/IEC 27005 – zarządzanie ryzykiem informacyjnym
- ISO 31000 – zarządzanie ryzykiem
- ISO 20000 – środowisko IT

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

NOTATKI: .....

.....

.....

.....

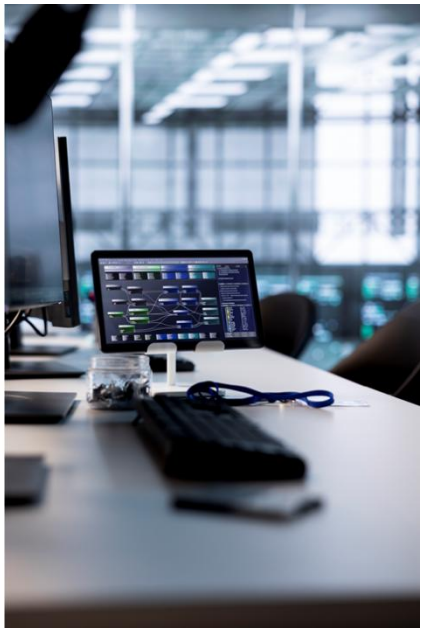
. .....

.....

Wybrane światowe standardy bezpieczeństwa IT

- NIST Cybersecurity Framework (baza dla NSC)
- COBIT – doskonalenie polityk IT
- ITIL – zarządzanie usługami IT
- SANS – polityka szyfrowania

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo



Wymogi normy ISO/IEC 27001 – SZBI

- Zrozumienie kontekstu organizacji
- Przywództwo i zaangażowanie kierownictwa
- Planowanie
- Wsparcie
- Działania operacyjne
- Ocena efektów działania
- Doskonalenie

Załącznik A – Kontrole bezpieczeństwa – wdrożenie odpowiednich środków bezpieczeństwa spośród 93 kontroli pogrupowanych w 4 obszarach, zależnie od wyników oceny ryzyka

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

NOTATKI: .....

.....

.....

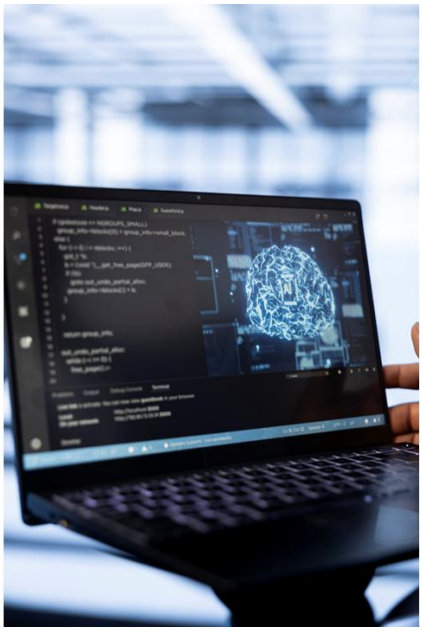
.....

.....

Wymogi normy ISO/IEC 22301 – SZCD

- Wymogi normy ISO/IEC 22301 - SZCD
- Ustanowienie polityki ciągłości działania
- Przeprowadzenie analizy wpływu na działalność (BIA)
- Ocena ryzyka
- Opracowanie strategii ciągłości działania
- Wdrożenie planów ciągłości działania
- Monitorowanie, przegląd i doskonalenie systemu BCM
- Komunikacja z interesariuszami

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo



agileo.it

Zasady bezpieczeństwa i praktyki

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

NOTATKI: .....

.....

.....

.....

.....

Zarządzanie hasłami i uwierzytelnianie wieloskładnikowe

Znaczenie zarządzania hasłami

Bezpieczne zarządzanie hasłami jest kluczowe dla ochrony danych i zapobiegania nieautoryzowanemu dostępowi do systemów.

Uwierzytelnianie wieloskładnikowe

Uwierzytelnianie wieloskładnikowe zwiększa bezpieczeństwo, wymagając różnych metod potwierdzenia tożsamości użytkownika.

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

Zasady bezpieczeństwa e-mail

Unikaj podejrzanych linków

Otwieranie podejrzanych linków może prowadzić do złośliwego oprogramowania i ataków phishingowych. Zachowaj ostrożność podczas korzystania z e-maili.

Filtry antywirusowe

Stosowanie filtrów antywirusowych jest kluczowe dla ochrony przed złośliwym oprogramowaniem. Regularne aktualizacje pomagają w wykrywaniu zagrożeń.

Bezpieczne załączniki

Nie otwieraj załączników z nieznanych źródeł. Może to być sposób na wprowadzenie złośliwego oprogramowania do systemu.

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

NOTATKI: .....

.....

.....

.....

. .....

.....

Bezpieczeństwo w sieciach bezprzewodowych

Celem ataków

Sieci bezprzewodowe są często narażone na różnego rodzaju ataki cybernetyczne, co stanowi poważne ryzyko dla użytkowników.

Szyfrowanie danych

Stosowanie szyfrowania danych jest kluczowe dla ochrony informacji przesyłanych przez sieci bezprzewodowe.

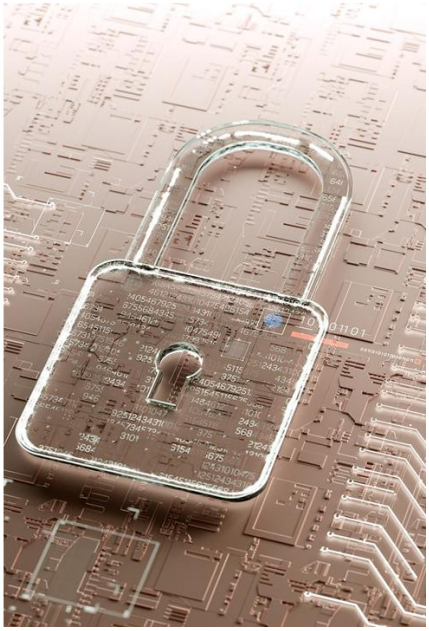
Silne hasła

Używanie silnych haseł jest niezbędne do zabezpieczenia dostępu do sieci bezprzewodowych przed nieautoryzowanym dostępem.

Aktualizacja oprogramowania

Regularne aktualizowanie oprogramowania routerów pomaga w poprawie bezpieczeństwa sieci i eliminacji znanych luk.

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo



Bezpieczne przeglądanie internetu

Unikanie podejrzanych stron

Ważne jest, aby unikać podejrzanych i nieznanych stron internetowych, aby chronić swoje dane osobowe.

Zabezpieczone połączenia

Korzystanie z zabezpieczonych połączeń, takich jak HTTPS, pomaga zapewnić bezpieczeństwo danych podczas przeglądania.

Regularne aktualizacje przeglądarek

Regularne aktualizowanie przeglądarek internetowych jest kluczowe dla ochrony przed nowymi zagrożeniami i lukami w zabezpieczeniach.

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

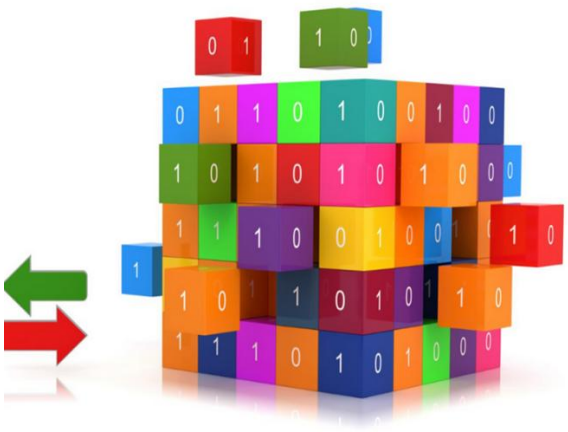
NOTATKI: .....

.....

.....

.....

.....



Backup i odzyskiwanie danych

Znaczenie kopii zapasowych
Regularne tworzenie kopii zapasowych danych jest kluczowe dla ich ochrony przed utratą. Kiedy dane są zabezpieczone, ryzyko ich zagubienia jest znacznie mniejsze.

Odzyskiwanie danych
Dobrze zarządzany proces odzyskiwania danych jest niezbędny w przypadku ich utraty. Skuteczne odzyskiwanie może zminimalizować straty związane z utratą danych.

Konsekwencje utraty danych
Utrata danych może prowadzić do poważnych konsekwencji, w tym finansowych i reputacyjnych. Dlatego tak ważne jest posiadanie planu awaryjnego.

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

agileo.it

Reagowanie na incydenty i planowanie awaryjne

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

NOTATKI: .....

.....

.....

.....

.....

Jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem

Zidentyfikowanie incydentu

Pierwszym krokiem w zarządzaniu incydentem jest jego identyfikacja. Ważne jest, aby dostrzegać anomalie i potencjalne zagrożenia

Zgłaszanie incydentów

Po identyfikacji,zgłoszenie incydentu jest kluczowe. Umożliwia to podjęcie odpowiednich działań prze zespół reagowania.

Informacje potrzebne do zgłoszenia

Zgłaszając incydent, ważne jest, aby dostarczyć kluczowe informacje, takie jak czas, miejsce i charakter incydentu.

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

Zasady reagowania na incydenty

Jasne zasady

Skuteczne reagowanie na incydenty wymaga ustanowienia jasnych zasad, które określają procedury działania w sytuacjach kryzysowych.

Plan działania

Niezbędne jest posiadanie szczegółowego planu działania na wypadek różnych rodzajów incydentów, aby zapewnić szybkie reagowanie.

Przywracanie normalności

Celem skutecznego reagowania jest szybkie przywrócenie normalnego funkcjonowania organizacji po incydencie.

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

NOTATKI: .....

.....

.....

.....

.....

.....

Planowanie awaryjne i kontynuacja działalności

Zrozumienie zakłóceń

Planowanie awaryjne polega na identyfiakcji potencjalnych zakłóceń, które mogą wpłynąć na działalność firmy. Zrozumienie tych zagrożeń jest kluczowe dla skutecznej strategii.

Strategia kontynuacji działalności

Właściwa strategia kontunuacji działalności pomaga w minimalizowaniu skutków zakłóceń oraz zapewnia szybkie przywrócenie operacji po incydencie.

Szkolenie i symulacje

Regularne szkolenia i symulacje pomogą pracownikom przygotować się na sytuacje awaryjne i skutecznie wdrażać plany awaryjne

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

Przegląd realnych przypadków naruszeń bezpieczeństwa i lekcje z nich wyniesione

Zrozumienie zagrożeń

Analiza przypadków naruszeń bezpieczeństwa umożliwia identyfikację i lepsze zrozumienie potencjalnych zagrożeń dla systemów.

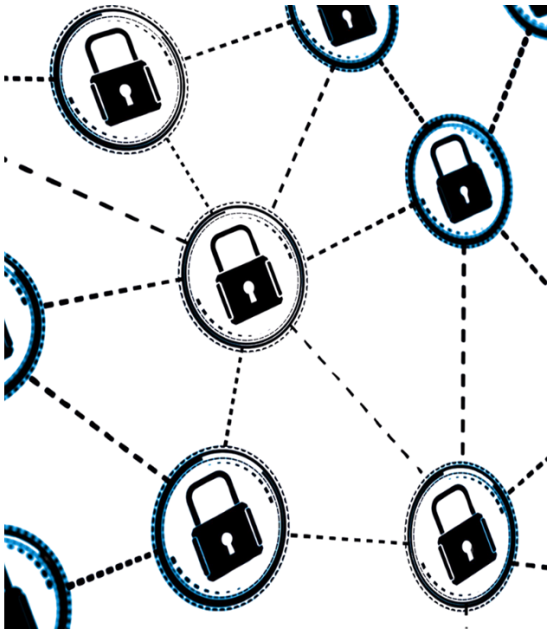
Lekcje z incydentów

Incydenty bezpieczeństwa dostarczają cennych lekcji, które pozwalają na udoskonalenie procedur i strategii ochrony.

Udoskonalenie procedur

Wnioski z analizy przypadków naruszeń pomagają w tworzeniu skuteczniejszych systemów bezpieczeństwa i procedur ochronnych.

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo



NOTATKI: .....

.....

.....

.....

.....

.....

agileo.it

Konkluzja

Znaczenie cyberbezpieczeństwa	**Świadomość zagrożeń**	**Zasady bezpieczeństwa**
Cyberbezpieczeństwo jest kluczowe w każdej organizacji, chroniąc dane i zasoby przed zagrożeniami	**Zrozumienie zagrożeń związanych z cyberprzestrzenią jest kluczowe dla skutecznej ochrony organizacji**	**Znajomość zasad bezpieczeństwa może znacznie zmniejszyć ryzyko wystąpienia incydentów cybernetycznych**

AGILEO.IT – Dbamy o Twoje Bezpieczeństwo

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

agileo.it

Dbamy o Twoje Bezpieczeństwo

Q&A

Porozmawiajmy jeszcze trochę o cyberbezpieczeństwie

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

NOTATKI: .....

.....

.....

.....

.....

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa