Krajowy system cyberbezpieczeństwa

Wraz z wejściem w życie ustawy o krajowym systemie bezpieczeństwa na NASK-PIB został nałożony istotny obowiązek pełnienia obowiązku jednego z trzech CSIRT poziomu krajowego. CSIRT NASK przyjmuje, analizuje i podejmuje działania i koordynuje reakcje na incydenty dotyczące bezpieczeństwa cywilnej cyberprzestrzeni RP zgłaszane przez operatorów usług kluczowych, dostawców usług cyfrowych, samorząd terytorialny i osoby prywatne oraz na incydenty związane z nielegalnymi treściami publikowanymi w Internecie i zagrażającymi bezpieczeństwu dzieci oraz odpowiada za monitorowanie zagrożeń internetowych i stanu cyberbezpieczeństwa na poziomie sektorowym i krajowym.

Działania i kierunki „Cyberbezpieczeństwa"

Cyberbezpieczeństwo jest jednym z celów strategicznych w obszarze bezpieczeństwa naszego państwa i zapewnia ochronę kluczowym sektorom gospodarki, obywatelom oraz przedsiębiorcom. To obszar wymagający stałego rozwoju i rozbudowy. Dzięki realizacji założeń Krajowych Ram Polityki Cyberbezpieczeństwa jak również strategii krajowych oraz wewnętrznych NASK zapewnia wysoki poziom bezpieczeństwa polskiej cyberprzestrzeni. Bierze aktywny udział w różnego rodzaju inicjatywach zarówno na poziomie krajowym (np. kampanie edukacyjno-informacyjne w ramach Programu Polska Cyfrowa) jak i zagranicznym (np.

Aspekt cyberbezpieczeństwa	**Znaczenie**
Ochrona poufnych danych	Zapobiega kradzieży i niewłaściwemu wykorzystaniu danych osobowych i firmowych.
Zapobieganie przerwom w działalności	Utrzymuje ciągłość działania organizacji, chroniąc przed atakami zakłócającymi operacje.
Ochrona klientów i partnerów biznesowych	Zabezpiecza dane osób trzecich, co jest kluczowe dla utrzymania dobrych relacji biznesowych.
Budowanie zaufania i reputacji	Wzmacnia postrzeganie organizacji jako bezpiecznej i godnej zaufania.
Zmniejszenie ryzyka strat finansowych	Ogranicza potencjalne straty związane z atakami cybernetycznymi i naruszeniem danych.
Zgodność z przepisami i regulacjami	Zapewnia, że organizacja przestrzega obowiązujących przepisów prawnych dotyczących ochrony danych.

Jak zadbać o podstawy cyberbezpieczeństwa w sieci?

Aby zadbać o cyberbezpieczeństwo w sieci, należy przede wszystkim:

- Instalować i regularnie aktualizować oprogramowanie antywirusowe oraz zapory sieciowe (ang. firewall)
- Upewnić się, że wszystkie aplikacje i systemy operacyjne posiadają najnowsze poprawki bezpieczeństwa
- Tworzyć kopie zapasowe ważnych danych
- Ustawiać silne hasła, regularnie je zmieniać oraz włączyć uwierzytelnianie wieloskładnikowe, jeśli to możliwe
- Ograniczyć uprawnienia użytkowników do niezbędnego minimum
- Szyfrować poufne dane
- Uważnie weryfikować nieznane wiadomości e-mail oraz załączniki
- Korzystać z zaufanych sieci Wi-Fi

Jak rozpoznać cyberatak?

Oto kilka symptomów, które mogą wskazywać na cyberatak:

- Nietypowa aktywność na kontach użytkowników
- Nowe, nieznane pliki wykonywalne na komputerach
- Zwiększony ruch w sieci lub zużycie przepustowości
- Problemy z dostępem do zasobów sieciowych
- Zmiany w konfiguracji oprogramowania i sprzętu
- Pojawienie się podejrzanych procesów lub usług
- Spowolnienie działania aplikacji i systemów IT
- Alarmy generowane przez systemy wykrywania włamań
- Niepowodzenia logowań lub inne błędy uwierzytelniania

W przypadku zaobserwowania takich objawów, należy niezwłocznie podjąć działania zaradcze i zgłosić incydent zespołowi bezpieczeństwa IT.

Cyberataki – rodzaje

1. Złośliwe oprogramowanie

Malware (ang. „malicious software"), to termin określający każdy rodzaj złośliwego oprogramowania, którego celem jest uszkodzenie lub wykorzystanie dowolnego urządzenia, aplikacji, usługi lub elementów sieci. Cyberprzestępcy zazwyczaj wykorzystują malware do pozyskiwania danych, którymi mogą posłużyć się wobec ofiar w celu:

- kradzieży, zaszyfrowania lub usunięcia poufnych informacji,
- przejęcia lub zmiany podstawowych funkcji systemu,
- monitorowania ich aktywności,
- łatwiejszego spamowania użytkowników lub zainstalowania na ich systemie oprogramowania, które wymuszona wizualizację wybranych reklam,
- wyłudzania pieniędzy.

Ataki hakerskie przy użyciu malware'u są najczęściej rozpowszechniane przez:

- załączniki poczty elektronicznej,
- fałszywe reklamy,
- zainfekowane aplikacje lub strony internetowe,
- linki w smsach i mmsy multimedialne.

Aby uniknąć zakażenia złośliwym oprogramowaniem, zapoznaj się z listą najpopularniejszych rodzajów cyberataków przeprowadzanych przy jego użyciu.

- **Robaki**
- **Koń trojański**
- **Ransomware**
- **Adware**
- **Spyware**
- **Freeware**
- **Shareware**
- **Keylogger**
- **ScareWare**

Zapoznaj się z ważnymi informacjami:

- Publikacje z zakresu cyberbezpieczeństwa: https://www.cert.pl/
- Ministerstwo Cyfryzacji: https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo
- Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego: https://www.cert.pl/ouch/

Zgłaszanie incydentów bezpieczeństwa: https://incydent.cert.pl/#!/lang=pl