Cyberbezpieczeństwo

Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak przeciwdziałać tymi zagrożeniom.

Cyberbezpieczeństwo, zgodnie z art. 2 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa, to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy".

Najpopularniejsze zagrożenia w cyberprzestrzeni to:

- **Phishing** - atak za pośrednictwem przede wszystkim poczty e-mail polegający na nakłonieniu odbiorcy wiadomości e-mail do ujawnienia poufnych informacji lub pobrania złośliwego oprogramowania.
- **Malware** - oprogramowanie, które wykonuje złośliwe zadanie na urządzeniu docelowym lub w sieci, np. uszkadza dane lub przejmuje system.
- **Ransomware** - atak polegający na zaszyfrowaniu danych w systemie docelowym i żądaniu okupu w zamian za umożliwienie użytkownikowi ponownego dostępu do danych.
- **Atak DoS lub DDoS** - atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów. DDoS atakuje z wielu miejsc równocześnie.
- **Ataki IoT w Internecie rzeczy** - atak polegający na przejmowaniu kontroli nad urządzeniami w sieci Internet: inteligentnymi domami, budynkami, sieciami energetycznymi, urządzeniami gospodarstwa domowego - przemysłu etc.).
- **Data Breaches (naruszenie danych)** - atak tego typu polega na kradzieży danych. Motywy naruszeń danych obejmują przestępstwa: (tj. kradzieży tożsamości, chęci zawstydzenia instytucji, szpiegostwo i inne).
- **Spam** – niechciane lub niepotrzebne wiadomości elektroniczne

Sposoby zabezpieczenia się przed zagrożeniami:

- Zainstalowanie i używanie oprogramowania antywirusowego. Stosowanie ochrony w czasie rzeczywistym
- Aktualizacja systemu operacyjnego, aplikacji użytkowych i programów antywirusowych. Brak aktualizacji zwiększa podatność na cyberzagrożenia
- Uruchomienie firewalla
- Korzystanie z różnych haseł do różnych usług elektronicznych
- Zaleca się aby hasło miało co najmniej 12 znaków i było budowane w oparciu o całe zdanie
- Tam gdzie to możliwe stosować dwuetapowe uwierzytelnianie za pomocą, np. sms, pin, tokenów, klucza fizycznego
- Regularne tworzenie kopii zapasowych ważnych danych

- Nie otwieranie stron zawierających darmowe filmy lub pliki muzyczne
- Należy pamiętać, że żaden bank czy urząd nie wysyła e-maili z prośbą o podanie hasła lub loginu w celu ich weryfikacji
- Podając poufne dane należy sprawdzić czy strona internetowa posiada certyfikat SSL, który zabezpiecza dane podczas przesyłania
- Nie otwieranie plików nieznanego pochodzenia
- Nie wysyłanie w wiadomościach e-mail żadnych poufnych informacji w formie otwartego tekstu. Dane powinny być zabezpieczone hasłem i zaszyfrowane. Hasło najlepiej przekazać przy użyciu innego środka komunikacji
- Zwracanie uwagi na komunikaty pojawiające się na ekranie.

Anonimowe zgłaszanie incydentów:

Dyżurnet.pl to zespół ekspertów Naukowej i Akademickiej Sieci Komputerowej, działający jako punkt kontaktowy do zgłaszania nielegalnych treści w Internecie, szczególnie związanych z seksualnym wykorzystywaniem dzieci. Zgłoszenia o potencjalnie nielegalnych treściach można przekazać za pomocą formularza, na adres mailowy lub za pomocą infolinii 0 801 615 005. Zgłoś incydent

Przydatne strony:

www.cert.pl – publikacje na temat cyberbezpieczeństwa

www.cert.pl\ouch - zestaw porad bezpieczeństwa dla użytkowników komputerów