Cyberbezpieczeństwo

Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz kroki jakie należy podjąć, aby móc sprawnie przeciwdziałać tym zagrożeniom.

1. Co to jest cyberbezpieczeństwo?

Cyberbezpieczeństwo to zastosowanie technologii, procesów i kontroli w celu ochrony systemów, sieci, programów, urządzeń i danych przed atakami cybernetycznymi.

Celem cyberbezpieczeństwa jest zmniejszenie ryzyka cyberataków i ochrona przed nieuprawnionym wykorzystaniem systemów, sieci i technologii. Jest to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

2. Przykłady cyberzagrożeń

Poniżej znajdą Państwo opis najczęściej występujących rodzajów cyberzagrożeń:

a) **ATAKI SOCJOTECHNICZNE** - ataki na Użytkownika mające na celu wykorzystanie technik służących do osiągniecia określonych celów poprzez manipulację. Najczęściej podczas ataku socjotechnicznego sprawca podszywa się pod zaufaną osobę, dział, organizację itp. przekonując Użytkownika do podjęcia konkretnie ukierunkowanych działań.

Tego rodzaju ataki występują najczęściej w kilku postaciach, poniżej podajemy kilka przykładów:

- **Phishing** - metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji, zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań.

- **Pharming** - polega na modyfikacji zawartości adresu www w celu przekierowania użytkownika na fałszywą stronę, mimo wpisania prawidłowego adresu strony.

- **Vishing** – tzw. Phishing głosowy czyli wykorzystywanie telefonu do przeprowadzania ataków phishingowych.

- **Smishing** - atak socjotechniczny podobny do phishingu polegający na rozsyłaniu SMS-ów, które mają skłonić ofiarę do podjęcia określonego działania.

b) MALWARE to złośliwe oprogramowanie, którego celem jest powodowanie szkód na komputerach użytkowników. Oprogramowanie wykorzystuje słabości systemów informatycznych i może prowadzić do kradzieży danych osobowych. Mianem malware określa się także wirusy, robaki, programy szpiegujące i inne. Rozpowszechnianie złośliwego oprogramowania odbywa się najczęściej poprzez złośliwe strony internetowe, które odwiedzają użytkownicy. Malware może być także umieszczany na dyskach zewnętrznych i innych nośnikach danych.

Tego rodzaju ataki występują najczęściej w kilku postaciach, poniżej podajemy kilka przykładów:

- **Adware –** jest to typ złośliwego oprogramowania malware , które wyświetla w nachalny sposób niechciane reklamy.

- **Ransomeware** - oprogramowanie, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych, a następnie żąda od ofiary okupu za przywrócenie stanu pierwotnego.

- **Spyware –** tzw. oprogramowanie szpiegujące – szkodliwe oprogramowanie, którego celem jest gromadzenie informacji o użytkowniku, a także ich przesyłanie bez jego wiedzy innym osobom. Programy te mogą również wyświetlać reklamy lub rozsyłać niechcianą pocztę elektroniczną.

3. Sposoby zabezpieczania się przed zagrożeniami

Aby uchronić organizację lub nas samych należy przede wszystkim:

- ✓ zainstalować i używać oprogramowania przeciw wirusom i spyware (najlepiej stosować ochronę w czasie rzeczywistym);
- ✓ aktualizować oprogramowanie antywirusowe oraz bazy danych wirusów;
- ✓ aktualizować system operacyjny i aplikacje bez zbędnej zwłoki;
- ✓ nie otwierać plików z nieznanego pochodzenia;
- ✓ nie korzystać ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu bezpieczeństwa;
- ✓ nie używać niesprawdzonych programów zabezpieczających (np. programu antywirusowego, który pochodzi od niezaufanego dostawcy) czy też do publikowania własnych plików w Internecie;
- ✓ sprawdzać pliki pobrane z Internetu za pomocą skanera (np. program antywirusowy);
- ✓ nie odwiedzać stron, które oferują niesamowite atrakcje (darmowe filmiki, muzykę, albo łatwy zarobek przy rozsyłaniu spamu) – często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia;
- ✓ nie zostawiać danych osobowych w niesprawdzonych serwisach i na stronach;

- ✓ nie wysyłać w e-mailach żadnych poufnych danych w formie otwartego tekstu – niech np. będą zabezpieczone hasłem i zaszyfrowane – hasło przekazujemy w sposób bezpieczny inną formą komunikacji (np. poprzez sms);
- ✓ wykonywać regularnie kopie zapasowe;
- ✓ ograniczyć korzystanie z ogólnodostępnych sieci WI-FI;
- ✓ używać silnych i zróżnicowanych haseł oraz starać się je systematycznie zmieniać;
- ✓ sprawdzać uprawnienia pobieranych aplikacji;

Więcej informacji znajdą Państwo na stronach:

https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo

https://www.cert.pl/publikacje/