CYBERBEZPIECZEŃSTWO

Powiatowy Inspektorat Weterynarii w Myszkowie
ul. Pułaskiego 42,
42-300 Myszków

Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa Powiatowy Inspektorat Weterynarii publikuje informacje na temat zagrożeń występujących w cyberprzestrzeni oraz kilka prostych porad jak uniknąć zagrożeń w sieci Internet.

Cyberbezpieczeństwo to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy”.

1. **Zagrożenia w cyberprzestrzeni:**

- Malware - oprogramowanie, które wykonuje złośliwe zadanie na urządzeniu docelowym lub w sieci, np. uszkadza dane lub przejmuje system.
- Phishing - atak za pośrednictwem poczty e-mail polegający na nakłonieniu odbiorcy wiadomości e-mail do ujawnienia poufnych informacji lub pobrania złośliwego oprogramowania.
- Spear Phishing - bardziej wyrafinowana forma phishingu, w której napastnik podszywa się pod osobę bliską osoby atakowanej.
- Atak typu “Man in the Middle” (MitM) - atak ten wymaga, aby napastnik znalazł się między dwiema stronami, które się komunikują i był w stanie przechwytywać wysyłane informacje.
- Trojan - (koń trojański) - oprogramowanie, które podszywa się pod przydatne lub ciekawe dla użytkownika aplikacje, implementując szkodliwe, ukryte przed użytkownikiem różne funkcje (oprogramowanie szantażujące - ransomware, szpiegujące - spyware etc.).
- Ransomware - atak polegający na zaszyfrowaniu danych w systemie docelowym i zażądaniu 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).
- Malware w aplikacjach telefonów. Urządzenia mobilne są szczególnie podatne na ataki złośliwego oprogramowania.

1. **Dobre praktyki zabezpieczenia przez atakami:**

- Hasła - Odpowiednie, złożone hasło może ochronić konsumentów przed zagrożeniami cybernetycznymi.
- Oprogramowanie antywirusowe - zainstaluj i używaj oprogramowania przeciw wirusom i spyware. Najlepiej stosuj ochronę w czasie rzeczywistym, aktualizuj oprogramowanie antywirusowe oraz bazy danych wirusów.
- Aktualizuj system operacyjny i aplikacje bez zbędnej zwłoki,
- Pliki nieznanego pochodzenia. Zachowaj ostrożność podczas otwierania załączników plików.
- Nie korzystaj ze stron internetowych, które nie mają ważnego certyfikatu bezpieczeństwa.
- Unikaj stron, które oferują darmowe atrakcje.
- Nie udostępniaj danych osobowych w niesprawdzonych serwisach internetowych.
- Pamiętaj nigdy nie podawaj haseł dostępowych do kont bankowych itp. w podejrzanych serwisach które tego żądają.
- Nie otwieraj plików nieznanego pochodzenia.
- Co jakiś czas skanuj komputer i sprawdzaj procesy sieciowe - jeśli się na tym nie znasz poproś o sprawdzenie kogoś, kto się zna.

- Wykonuj kopie zapasowe ważnych danych.

1. **Odnośniki do stron dotyczących cyberbezpieczeństwa:**

- Publikacje z zakresu cyberbezpieczeństwa: https://www.cert.pl
- Zestaw porad bezpieczeństwa dla użytkowników komputerów prowadzony na witrynie internetowej CSIRT NASK – Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym: https://www.cert.pl/ouch
- Poradniki na witrynie internetowej Serwis Rzeczypospolitej Polskiej https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo