Publikacje

Published: Friday, 08 October 2021 09:34
Written by Jacek Przepióra
Hits: 36227

Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak skuteczne stosować sposoby zabezpieczenia się przed tymi zagrożeniami. Do najpopularniejszych zagrożeń w cyberprzestrzeni, z którymi mogą się Państwo spotkać, należą: ataki z użyciem szkodliwego oprogramowania (malware, wirusy, robaki, itp.), kradzieże tożsamości, kradzieże (wyłudzenia), modyfikacje bądź niszczenie danych, blokowanie dostępu do usług, spam (niechciane lub niepotrzebne wiadomości elektroniczne), ataki socjotechniczne (np. phishing, czyli wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję).

Sposoby zabezpieczenia się przed zagrożeniami:

1. Zainstaluj i używaj oprogramowania przeciw wirusom i spyware. Najlepiej stosuj ochronę w czasie rzeczywistym.
2. Aktualizuj oprogramowanie oraz bazy danych wirusów (dowiedz się czy twój program do ochrony przed wirusami posiada taką funkcję i robi to automatycznie).
3. Nie otwieraj plików nieznanego pochodzenia.
4. Nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu, chyba, że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna.
5. Nie używaj niesprawdzonych programów zabezpieczających czy też do

publikowania własnych plików w Internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony).
6. Co jakiś czas skanuj komputer i sprawdzaj procesy sieciowe – jeśli się na tym nie znasz poproś o sprawdzenie kogoś, kto się zna. Czasami złośliwe oprogramowanie nawiązujące własne połączenia z Internetem, wysyłające twoje hasła i inne prywatne dane do sieci może się zainstalować na komputerze mimo dobrej ochrony – należy je wykryć i zlikwidować.
7. Sprawdzaj pliki pobrane z Internetu za pomocą skanera.
8. Staraj się nie odwiedzać zbyt często 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.
9. Nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie są one widoczne dla osób trzecich.
10. Nie wysyłaj w e-mailach żadnych poufnych danych w formie otwartego tekstu.
11. Aktualizuj system operacyjny i aplikacje bez zbędnej zwłoki.
12. Pamiętaj o uruchomieniu firewalla.
13. Wykonuj kopie zapasowe ważnych danych.
14. Pamiętaj, że żaden bank czy Urząd nie wysyła e-maili do swoich klientów/interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.

Zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami to wiedza niezbędna każdemu użytkownikowi komputera, smartphona czy też usług internetowych.

1. STÓJ. POMYŚL. POŁĄCZ. jest polską wersją międzynarodowej kampanii **STOP. THINK. CONNECT.™**, mającej na celu zwiększanie poziomu świadomości społecznej i promowanie bezpieczeństwa w cyberprzestrzeni. ZAPOZNAJ SIĘ Z DOBRYMI PRAKTYKAMI opublikowanymi na stronach kampanii oraz z dostępnymi na niej MATERIAŁAMI DO POBRANIA.
2. OUCH! To cykliczny, darmowy zestaw porad bezpieczeństwa dla użytkowników komputerów. Każde wydanie zawiera krótkie, przystępne przedstawienie wybranego zagadnienia z bezpieczeństwa komputerowego wraz z listą wskazówek jak można chronić siebie, swoich najbliższych i swoją organizację.
3. Zobacz wszystkie polskie wydania OUCH! na stronie CERT Polska.
4. Zespół CERT POLSKA działa w strukturach **NASK (Naukowej i Akademickiej Sieci Komputerowej)** – państwowego instytutu badawczego prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne. **CERT Polska** jest zespołem specjalistów zwalczających zagrożenia w sieciach komputerowych.

Publikacje

Published: Friday, 08 October 2021 09:34
Written by Jacek Przepióra
Hits: 36227

5. Zapoznaj się z rocznymi raportami z działalności CERT POLSKA zawierającymi zebrane dane o zagrożeniach dla polskich użytkowników Internetu, w tym również opisy najciekawszych nowych zagrożeń i podatności.