Cyberbezpieczeństwo

Dla Mieszkańca

Co to jest cyberbezpieczeństwo?

Cyberbezpieczeństwo polega na zapewnieniu odporności systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

Cyberbezpieczeństwo dąży do zapewnienia ochrony przestrzeni przetwarzania informacji oraz zachodzących interakcji w sieciach teleinformatycznych w obszarze cyberprzestrzeni.

Celem cyberprzestępców zwykle jest kradzież naszych danych. W tym celu wykorzystywane są różne techniki oraz mechanizmy mające na celu nakłonienie nas do wykonania czynności, wskutek których ujawnione zostaną nasze hasła i stosowane zabezpieczenia. Wśród tych technik są to między innymi: zainfekowane załączniki, fałszywe strony internetowe i wiadomości e-mail łudząco przypominające prawdziwe.

Najpopularniejsze zagrożenia w cyberprzestrzeni:

- ataki z użyciem szkodliwego oprogramowania (malware, wirusy, robaki, itp.),
- kradzież tożsamości, 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),
- ataki, w których cyberprzestępca uczestniczy w komunikacji między osobami, bez ich wiedzy, w celu przechwycenia informacji lub środków pieniężnych, np. poprzez uzyskanie danych niezbędnych do logowania w systemie bankowości elektronicznej.

Pamiętaj, że twoja świadomość zagrożeń i zastosowanie środków bezpieczeństwa ma znaczenie dla zapewnienia ochrony Twoich danych – tożsamości, danych finansowych czy prywatności. Zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie zabezpieczeń przed zagrożeniami to wiedza niezbędna każdemu użytkownikowi komputera, telefonu komórkowego czy też usług internetowych.

Podstawowe sposoby zabezpieczenia się przed zagrożeniami:

- zainstaluj i używaj oprogramowania antywirusowego, stosuj ochronę w czasie rzeczywistym;
- aktualizuj system operacyjny i aplikacje bez zbędnej zwłoki;
- aktualizuj oprogramowanie antywirusowe oraz bazy danych wirusów (dowiedz się czy twój program do ochrony przed wirusami posiada taką funkcję i robi to automatycznie);
- nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu SSL;
- nie otwieraj plików nieznanego pochodzenia;
- nie używaj oprogramowania pochodzącego z niesprawdzonych źródeł (może być ono zainfekowane złośliwym kodem);
- 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;
- sprawdzaj pliki pobrane z Internetu za pomocą skanera antywirusowego;
- nie odwiedzaj 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 wysyłaj w e-mailach żadnych poufnych danych w formie otwartego tekstu – niech np. będą zabezpieczone hasłem i zaszyfrowane – hasła przekazuj w sposób bezpieczny najlepiej innym kanałem komunikacyjnym;
- nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że są one niewidoczne dla osób trzecich;
- wykonuj kopie zapasowe ważnych danych.

Warto również zapoznać się z informacjami poniżej:

- 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 Ministerstwa Cyfryzacji: https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo
- publikacje z zakresu cyberbezpieczeństwa: https://www.cert.pl/
- strona internetowa kampanii STÓJ. POMYŚL. POŁĄCZ. mającej na celu zwiększanie poziomu świadomości społecznej i promowanie bezpieczeństwa w cyberprzestrzeni: https://stojpomyslpolacz.pl/stp/

Dane kontaktowe
Urząd Miasta Opola

ul. Rynek 1A

45-015 Opole

77 45 11 800

urzad [at] um.opole.pl

www.opole.pl

Lokalizacja

Tagi
Cyberbezpieczeństwo