Informacje dotyczące cyberbezpieczeństwa

Realizując zadania wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady, jak skutecznie stosować sposoby zabezpieczenia się przed tymi zagrożeniami.

Cyberbezpieczeństwo – zgodnie z obowiązującymi przepisami 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:

- 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:

- instalacja i używanie oprogramowania przeciw wirusom i spyware (najlepiej stosować ochronę w czasie rzeczywistym),
- aktualizacja oprogramowania antywirusowego oraz bazy danych wirusów,
- aktualizacja systemu operacyjnego i aplikacji bez zbędnej zwłoki,
- nieotwieranie plików nieznanego pochodzenia,
- niekorzystanie ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu bezpieczeństwa,
- nieużywanie niesprawdzonych programów zabezpieczających, jak i niepublikowanie własnych plików w Internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony),
- regularne skanowanie komputera i sprawdzanie procesów sieciowych – 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,
- sprawdzanie plików pobranych z Internetu za pomocą skanera antywirusowego,
- nieodwiedzanie stron, które oferują niesamowite atrakcje (darmowe filmiki, muzykę lub łatwy zarobek przy rozsyłaniu spamu) – często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia,
- niezostawianie danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że są one niewidoczne dla osób trzecich,
- niewysyłanie w e-mailach żadnych poufnych danych w formie otwartego tekstu – niech np. będą zabezpieczone hasłem i zaszyfrowane – hasło przekazuj w sposób bezpieczny, innym kanałem komunikacji,
- pamiętanie o uruchomieniu zapory sieciowej (firewall),
- pracowanie na najniższych możliwych uprawnieniach użytkownika,
- wykonywanie kopii zapasowej ważnych danych,
- pamiętanie, że żaden bank ani urząd nie wysyła e-maili do swoich klientów/interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji,
- unikanie kontaktów z osobami podającymi się za przedstawicieli firm, instytucji, którzy żądają od nas podania danych autoryzacyjnych lub nakłaniają nas do instalowania aplikacji zdalnego dostępu,
- unikanie korzystania z otwartych sieci Wi-Fi,
- tam, gdzie to możliwe (konta społecznościowe, konto e-mail, usługi e-administracji, usługi finansowe), stosowanie dwuetapowego uwierzytelnienia za pomocą np. SMS, PIN, aplikacji generującej jednorazowe kody autoryzujące, tokenów, klucza fizycznego, face ID.

Powyższe informacje nie stanowią zamkniętego katalogu zagrożeń oraz porad, jak ich uniknąć.

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

Wszelkie porady bezpieczeństwa dla użytkowników komputerów dostępne są na:

• witrynie internetowej polskich wydań Ouch!;

• stronach serwisu Rzeczypospolitej Polskiej: Baza wiedzy – cyberbezpieczeństwo;

• portalu CERT Polska;

• stronie internetowej kampanii Stój. Pomyśl. Połącz;

• stronie OSE IT Szkoła w poradniku „ABC cyberbezpieczeństwa” (PDF, 1,3 MB).

Zgłaszanie incydentów bezpieczeństwa na stronie https://incydent.cert.pl.

Metryka strony

Udostępniający: **Samorząd Powiatu Bielskiego**
Wytwarzający/odpowiadający: Bogdan Komarzewski
Data wytworzenia: **2023-04-06**
Wprowadzający: **Wojciech Charyton**
Data modyfikacji: **2023-04-06**
Opublikował: **Wojciech Charyton**
Data publikacji: **2023-04-06**