Cyberbezpieczeństwo - informacje ogólne

Realizując zadania, wynikające z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369, z późn.zm.), przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak skuteczne stosować sposoby zabezpieczenia się przed tymi zagrożeniami.

Cyberbezpieczeństwo, jest to odporność systemów informacyjnych na wszelkie działania naruszające ich dostępność, integralność, poufność oraz autentyczność. Jest to jeden z kluczowych czynników zapewniających bezpieczeństwo i ciągłość działania zarówno osób prywatnych, jak i przedsiębiorstw.

Najpopularniejsze zagrożenia w cyberprzestrzeni:

- ataki z użyciem szkodliwego oprogramowania (malware, ransomware, 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.

Zasady bezpiecznego poruszania się w cyberprzestrzeni

1. Zawsze korzystaj z oprogramowania antywirusowego stosującego ochronę w czasie rzeczywistym.
2. Pamiętaj o uruchomieniu firewalla.
3. Stosuj bezpieczne, unikalne hasła oraz pamiętaj o ich cyklicznej zmianie.
4. Regularnie, bez zbędnej zwłoki aktualizuj oprogramowanie antywirusowe oraz bazy danych wirusów.
5. Regularnie, bez zbędnej zwloki, aktualizuj system operacyjny oraz aplikacje.
6. Regularnie skanuj komputer w celu wykrycia niebezpiecznego oprogramowania oraz działających procesów mogących narazić cię na wykradzenie danych, 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. Nie otwieraj plików nieznanego pochodzenia- plików od nieznanych osób, firm lub instytucji, gdyż często są to sfabrykowane wiadomości w celu wyłudzenia danych lub zainstalowania niebezpiecznego oprogramowania.
8. 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.
9. Nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu bezpieczeństwa chyba, że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna.
10. Nie wysyłaj 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. Jeżeli już musisz to zrobić to staraj się zabezpieczyć plik przed odczytaniem przez osoby niepowołane.

11. Nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie są one widoczne dla osób trzecich,
12. Nie używaj niesprawdzonych programów zabezpieczających, czy też programów do publikowania własnych plików w Internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony).
13. Każdy pobrany plik z internetu sprawdzaj za pomocą skanera antywirusowego.
14. Staraj się nie odwiedzać stron, które oferują niesamowite atrakcje (pieniądze, darmowe filmiki, muzykę, albo łatwy zarobek przy rozsyłaniu spamu) – często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia.
15. Pracuj na najniższych możliwych uprawnieniach użytkownika.
16. Cyklicznie wykonuj kopie zapasowe danych, których utrata przyniosła by dla Ciebie duże straty.
17. Unikaj kontaktów z osobami podającymi się za przedstawicieli firm, instytucji, którzy żądają od nas podania danych autoryzacyjnych lub nakłaniają nas do instalowania aplikacji zdalnego dostępu, unikaj korzystania z otwartych sieci Wi-Fi.
18. Tam, gdzie to możliwe (konta społecznościowe, konto email, usługi e-administracji, usługi finansowe) stosuj dwuetapowego uwierzytelnienie za pomocą np. sms, pin, aplikacji generującej jednorazowe kody autoryzujące, tokenów, klucza fizycznego, faceID.
19. Czytaj regulaminy.

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.

Podsumowanie

Cyberbezpieczeństwo jest ważną kwestią dla każdego. Stosując się do podstawowych zasad cyberbezpieczeństwa, można znacząco zmniejszyć ryzyko ataku.

Zalecamy również śledzenie na bieżąco stron internetowych organizacji wyspecjalizowanych w zakresie cyberbezpieczeństwa, takich jak:

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

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