Cyberbezpieczeństwo

Realizuj?c zadania wynikaj?ce z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpiecze?stwa, przekazujemy informacje pozwalaj?ce na zrozumienie zagro?e? wyst?puj?cych w cyberprzestrzeni oraz stosowanie skutecznych sposobów zabezpieczania si? przed tymi zagro?eniami.
Zgodnie z art. 2 pkt 4 ww. ustawy cyberbezpiecze?stwo to odporno?? systemów informacyjnych na dzia?ania naruszaj?ce poufno??, integralno??, dost?pno?? i autentyczno?? przetwarzanych danych lub zwi?zanych z nimi us?ug oferowanych przez te systemy.
Najpopularniejsze zagro?enia w cyberprzestrzeni to:
â€¢ ataki socjotechniczne (np. phishing - nazwa pochodzi od password ("has?o") oraz fishing ("w?dkowanie"). Istot? ataku jest próba pozyskania has?a u?ytkownika, które s?u?y do logowania si? na portalach spo?eczno?ciowych b?d? do serwisów. Po uzyskaniu dost?pu, przest?pca mo?e wykra?? dane osobowe i w tym celu dokonywa? oszustw);
â€¢ kradzie?e (wy?udzenia), modyfikacje lub niszczenie danych;
â€¢ kradzie?e to?samo?ci;
â€¢ ataki z u?yciem szkodliwego oprogramowania (wirusy, robaki, malware - to zbitka wyrazowa pochodz?ca od wyra?enia malicious software ("z?o?liwe oprogramowanie"). Wspóln? cech? programów uznawanych za malware jest fakt, ?e wykonuj? dzia?ania na komputerze bez jego zgody i wiedzy u?ytkownika, na korzy?? osoby postronnej. Dzia?ania tego typu obejmuj? np. do??czenie maszyny do sieci komputerów "zombie", które s?u?? do ataku na organizacje rz?dowe, zdobywanie wirtualnych walut lub kradzie? danych osobowych i informacji niezb?dnych do logowania do bankowo?ci elektronicznej.);
â€¢ blokowanie dost?pu do us?ug;
â€¢ spam (niechciane lub niepotrzebne wiadomo?ci elektroniczne mog?ce zawiera? odno?niki do szkodliwego oprogramowania).
Przyk?adowe sposoby zabezpieczenia si? przed zagro?eniami:
â€¢ aktualizowanie systemu operacyjnego i aplikacji bez zb?dnej zw?oki;
â€¢ instalacja i u?ytkowanie oprogramowania przeciw wirusom i spyware. Najlepiej stosowa? ochron? w czasie rzeczywistym;
â€¢ aktualizacja oprogramowania antywirusowego oraz bazy danych wirusów;
â€¢ sprawdzanie plików pobranych z Internetu za pomoc? programu antywirusowego;
â€¢ pami?tanie o uruchomieniu firewalla;
â€¢ nieotwieranie plików nieznanego pochodzenia;
â€¢ korzystanie ze stron banków, poczty elektronicznej czy portali spo?eczno?ciowych, które maj? wa?ny certyfikat bezpiecze?stwa;
â€¢ regularne skanowanie komputera i sprawdzanie procesów sieciowych;
â€¢ nieu?ywanie niesprawdzonych programów zabezpieczaj?cych;
â€¢ regularne wykonywanie kopii zapasowych wa?nych danych;
â€¢ nieodwiedzanie stron, które oferuj? niesamowite atrakcje (darmowe filmiki, muzyk?, albo ?atwy zarobek) - cz?sto na takich stronach znajduj? si? ukryte wirusy, trojany i inne zagro?enia;
â€¢ niezostawianie danych osobowych w niesprawdzonych serwisach i na stronach, je?eli nie ma si? absolutnej pewno?ci, ?e nie s? one widoczne dla osób trzecich oraz nie wysy?anie w wiadomo?ciach e-mail ?adnych poufnych danych w formie otwartego tekstu;
â€¢ pami?tanie. ?e ?aden bank czy Urz?d nie wysy?a e-maili do swoich klientów/interesantów z

pro?b? o podanie has?a lub loginu w celu ich weryfikacji.

Zrozumienie zagro?e? cyberbezpiecze?stwa i stosowanie sposobów zabezpieczania si? przed zagro?eniami to wiedza niezb?dna ka?demu u?ytkownikowi komputera, smartphona czy te? us?ug internetowych.
Zach?camy do regularnego zapoznawania si? z tre?ciami dotycz?cymi cyberbezpiecze?stwa zawartymi na m.in. na stronach: Ministerstwa Cyfryzacji czy pa?stwowego instytutu badawczego NASK.

Metryczka

Wytworzył:	Maria Wojcińska
Data wytworzenia:	17.05.2022
Opublikował w BIP:	Aneta Witkowska
Data opublikowania:	17.05.2022 11:03
Liczba wyświetleń:	139