Cyberbezpieczeństwo – podstawowe informacje i zasady

Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa publikujemy informacje na temat zagrożeń występujących w cyberprzestrzeni oraz porady jak zabezpieczyć 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" (art. 2 pkt 4, Dz.U.2020.1369 t.j. z dnia 2020.08.11).

Najpopularniejsze zagrożenia w cyberprzestrzeni:

- Malware - oprogramowanie, które wykonuje złośliwe zadanie na urządzeniu docelowym lub w sieci, np. uszkadza dane lub przejmuje system.
- Phishing - atak za pośrednictwem poczty e-mail polegający na nakłonieniu odbiorcy wiadomości e-mail do ujawnienia poufnych informacji lub pobrania złośliwego oprogramowania.
- Spear Phishing - bardziej wyrafinowana forma phishingu, w której napastnik podszywa się pod osobę bliską osoby atakowanej.
- Atak typu "Man in the Middle" (MitM) - atak ten wymaga, aby napastnik znalazł się między dwiema stronami, które się komunikują i był w stanie przechwytywać wysyłane informacje.
- Trojan – (koń trojański) - oprogramowanie, które podszywa się pod przydatne lub ciekawe dla użytkownika aplikacje, implementując szkodliwe, ukryte przed użytkownikiem różne funkcje (oprogramowanie szantażujące – ransomware, szpiegujące – spyware etc.).
- Ransomware - atak polegający na zaszyfrowaniu danych w systemie docelowym i zażądaniu okupu w zamian za umożliwienie użytkownikowi ponownego dostępu do danych.
- Atak DoS lub DDoS - atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów. DDoS atakuje z wielu miejsc równocześnie.
- Ataki IoT w Internecie rzeczy - atak polegający na przejmowaniu kontroli nad urządzeniami w sieci Internet: inteligentnymi domami, budynkami, sieciami energetycznymi, urządzeniami gospodarstwa domowego - przemysłu etc.).
- Data Breaches (naruszenie danych) - atak tego typu polega na kradzieży danych. Motywy naruszeń danych obejmują przestępstwa: (tj. kradzieży tożsamości, chęci zawstydzenia instytucji, szpiegostwo i inne).
- Malware w aplikacjach telefonów. Urządzenia mobilne są szczególnie podatne na ataki złośliwego oprogramowania.

Sposoby zabezpieczenia się przed zagrożeniami:

- Higiena hasła – nie da się obronić przed atakami używając prostych haseł, takich jak „1234". Odpowiednie, złożone hasło może ochronić konsumentów przed zagrożeniami cybernetycznymi.
- Oprogramowanie antywirusowe - subskrybuj dobrej jakości oprogramowanie antywirusowe oraz zaplanuj aktualizacje automatyczne systemu operacyjnego na Twoim urządzeniu.
- Nie otwieraj plików nieznanego pochodzenia. Zachowaj ostrożność podczas otwierania załączników plików. Na przykład, jeśli otrzymasz wiadomość e-mail z załącznikiem PDF z opisem „zaległa faktura", nie otwieraj go jeśli zobaczysz, że pochodzi on z nietypowego e-maila, takiego jak ann23452642@gmail.com ! Otwórz dopiero jeżeli masz 100% pewności, że wiesz kto wysłał wiadomość.
- Nie korzystaj ze stron internetowych, które nie mają ważnego certyfikatu bezpieczeństwa, chyba że masz stuprocentową pewność, że strona taka jest bezpieczna.
- Staraj się nie odwiedzać zbyt często stron, które oferują darmowe atrakcje (filmiki, muzykę, aplikacje) – często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia.
- Nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie będą one widoczne dla osób trzecich.
- Pamiętaj, że żadna instytucja nie wysyła e-maili do swoich klientów/interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.

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

Podmioty zajmujące się cyberbezpieczeństwem:
Ministerstwo Cyfryzacji,

- CERT Polska, https://cert.pl/
- CSIRT GOV, https://csirt.gov.pl/
- CSIRT NASK, https://www.nask.pl/pl/dzialalnosc/csirt-nask/3424,CSIRT-NASK.html

Firmy zajmujące się cyberbezpieczeństwem:

- Niebezpiecznik.pl, https://niebezpiecznik.pl/
- CyberDefence24, https://cyberdefence24.pl/
- Cyberrescue, https://pl.cyberrescue.me/