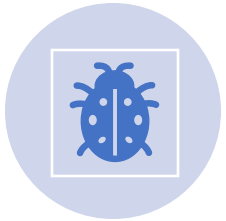
Cyberbezpieczeństwo

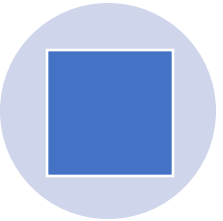
Realizując zadania, wynikające z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369, z późn.zm.), przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak skuteczne stosować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

Najpopularniejsze zagrożenia w cyberprzestrzeni:



ataki z użyciem szkodliwego oprogramowania (malware, wirusy, robaki, itp.)

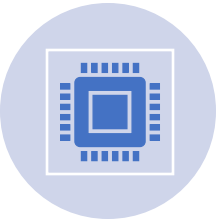
kradzieże tożsamości, wyłudzenia pieniędzy



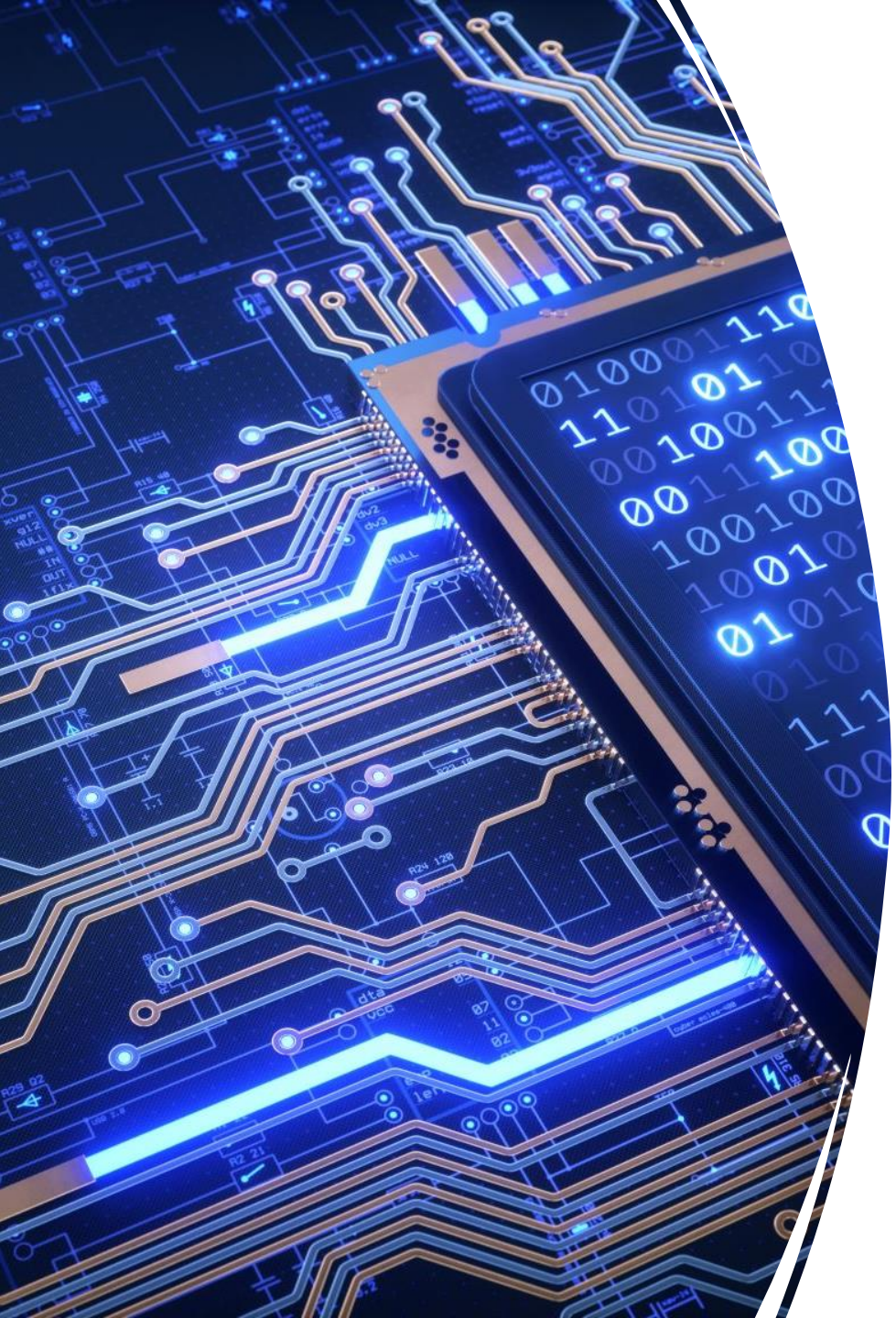
modyfikacje bądź niszczenie danych (np. szyfrowanie)

blokowanie dostępu do usług (np. stron internetowych, poczty, programów)

spam (niechciane lub niepotrzebne wiadomości elektroniczne)



ataki socjotechniczne (np.: phishing, czyli wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję)

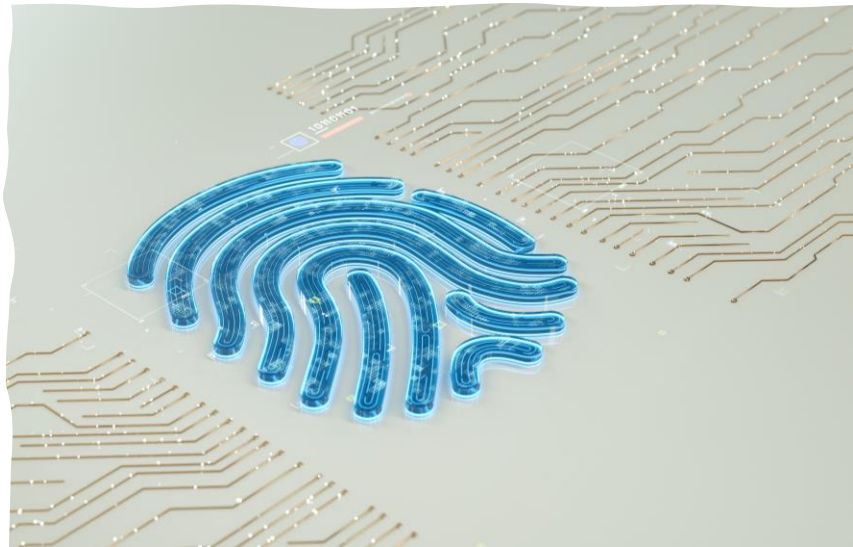


Sposoby zabezpieczenia się przed zagrożeniami:

- Używaj oprogramowania przeciw wirusom. Stosuj ochronę w czasie rzeczywistym.
- Aktualizuj oprogramowanie antywirusowe oraz bazy danych wirusów - sprawdź czy robi się to automatycznie.
- Aktualizuj system operacyjny i programy bez zbędnej zwłoki.
- Nie otwieraj plików nieznanego pochodzenia.
- Nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu, chyba, że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna.
- Nie instaluj programów z niezaufanych źródeł, mogą one mieć wbudowane dodatkowe niebezpieczne funkcje.
- Sprawdzaj procesy sieciowe – jeśli wiesz jak, poproś o kogoś, kto ci pomoże. Czasami złośliwe oprogramowanie samodzielnie nawiązujące połączenia z Internetem, wysyłające twoje hasła i inne prywatne dane do sieci może się zainstalować na komputerze mimo dobrej ochrony.

Sposoby zabezpieczenia się przed zagrożeniami:

- Sprawdzaj pliki pobrane z Internetu za pomocą programu antywirusowego.
- Nie ufaj stronom, które oferują niesamowite okazje (darmowe filmiki, muzykę, albo łatwy zarobek przy rozsyłaniu spamu) – 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 są one widoczne dla osób trzecich.
- Nie wysyłaj w e-mailach żadnych poufnych danych w formie otwartego tekstu – niech np.: będą zabezpieczone hasłem i zaszyfrowane – hasło przekazuj w sposób bezpieczny.
- Pamiętaj o uruchomieniu firewalla.
- Co jakiś czas skanuj komputer programem antywirusowym ręcznie.
- Wykonuj kopie zapasowe ważnych danych.
- **Pamiętaj, że żaden bank czy Urząd nie wysyła e-maili z prośbą o podanie hasła lub loginu w celu ich weryfikacji**.



Dodatkowe informacje:

- zestaw porad bezpieczeństwa dla użytkowników komputerów prowadzony przez Zespół CERT: 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/