Informacja o zagrożeniach związanych z cyberbezpieczeństwem

W związku z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2023, poz. 913) przekazujemy informację o zagrożeniach oraz sposobach zabezpieczeń stosowanych w celu minimalizacji ryzyk związanych z funkcjonowaniem w środowisku internetowym.

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) ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Do najpopularniejszych zagrożeń związanych z funkcjonowaniem w sieci internetowej możemy zaliczyć:

- ataki z użyciem szkodliwego oprogramowania (malware, wirusy, itp.),
- kradzieże tożsamości,
- modyfikacje bądź niszczenie danych,
- blokowanie dostępu do usług,
- podszywanie się pod inne usługi,
- spam (niechciane lub niepotrzebne wiadomości elektroniczne),
- ataki socjotechniczne (np. phishing, czyli wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję).

Postępowanie w celu minimalizacji ryzyka związanego z użytkowaniem sieci komputerowej, komputera, telefonu:

- używanie oprogramowania antywirusowego,
- regularne aktualizowanie oprogramowania antywirusowego,
- skanowanie komputera, pamięci przenośnych USB oprogramowaniem antywirusowym,
- aktualizowanie systemów operacyjnych oraz zainstalowane oprogramowanie,
- nie pobieranie i nie otwieranie plików, dokumentów nieznanego pochodzenia,
- nie pobieranie załączników poczty elektronicznej od nieznanych nadawców, zawsze należy weryfikować adres, z którego przyszedł e-mail,
- zachowanie szczególnej ostrożności podczas odbierania telefonów od osób podszywających się pod urzędy, policję, członków rodziny, proszących o pilne przesłanie pieniędzy,
- zachowanie szczególnej ostrożności podczas odbierania telefonów oraz e-maile informujących o zwrotach podatku, informacjach o spadku – najprawdopodobniej są to próby wyłudzenia,
- nie otwieranie plików nieznanego pochodzenia,
- nie korzystanie ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu SSL,
- nigdy nie podawaj hasła lub loginu do swojego konta bankowego, konsultant banku nigdy nie poprosi o takie dane w celu weryfikacji,
- nie wysyłaj e-maili zawierających poufne informacje (takie dane zawsze zabezpieczaj hasłem),
- nie wpisuj swoich danych na nieznanych serwisach (nie podawaj numerów kart kredytowych, numeru pesel),

- wykonuj kopie zapasowe ważnych danych i przechowuj je w innym miejscu niż na komputerze, z którego zostały wykonane, aby w przypadku infekcji nie utracić zgromadzonych plików.
- regularnie zapoznawaj się z zestawem porad publikowanych przez ekspertów z Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym: https://www.cert.pl/ouch/

Przeglądaj poradniki:

- Strona internetowa Ministerstwa Cyfryzacji: 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/