CYBERBEZPIECZEŃSTWO

Zgodnie z art. 22 ust. 1 pkt 4 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej jako „Ustawa") przekazujemy Państwu niezbędne informacje w przedmiocie zagadnienia jakim jest cyberbezpieczeństwo.

Cyberbezpieczeństwo to nic innego jak odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Definicja cyberbezpieczeństwa wprost wynika z art. 2 pkt 4 Ustawy.

Ataki cybernetyczne podejmowane są w różnych celach, ale najczęściej podejmowane są w celu kradzieży tożsamości, w tym kradzieży danych osobowych, by umożliwić podejmowanie nieuprawnionego działania w Twoim imieniu mającego na celu np. kradzież zgromadzonych przez Ciebie środków finansowych, ujawnienie informacji Ciebie dotyczących osobom nieuprawnionym czy zablokowanie Ci dostępu do jakiegoś rodzaju usług. By przeciwdziałać wystąpieniu zagrożenia w obszarze bezpieczeństwa informacji musisz w szczególności mieć na uwadze następujące zasady:

1. Pamiętaj, aby zawsze mieć aktualny system operacyjny w swoim komputerze (w tym w laptopie).
2. Stosuj szyfrowanie (zabezpieczenie kryptograficzne) wobec urządzeń przenośnych typu np. laptop, pendrive itp.
3. Pamiętaj również o szyfrowaniu pamięci wewnętrznej telefonu. Koniecznie Ustaw PIN lub/oraz znak graficzny do odblokowywania telefonu. Jeżeli jest dostępna funkcja biometryki (odcisk palca, skan twarzy) warto z niej skorzystać.
4. Chroń swoje urządzenia używając programów antywirusowych.
5. Uważaj na wiadomości sms, e-mail, telefony, które nakłaniają Cię do podania danych osobowych czy kliknięcia w link w celu skorzystania z jakiejś usługi.
6. Nie instaluj aplikacji z nieznanych i niezaufanych źródeł.
7. Stosuj do systemów bazodanowych, z których korzystasz (w tym systemów bankowych, aplikacji mobilnych) hasła o wysokim poziomie skomplikowania (najlepiej co najmniej 12 znaków, wielka, mała litera, cyfra i znak specjalny).
8. Stosuj uwierzytelnianie dwuskładnikowe (np. za pośrednictwem np. pin, sms, klucza fizycznego, tokena).
9. Zmieniaj cyklicznie hasła (np. co 90 dni).
10. Używaj tzw. menedżerów haseł służących do ich przechowywania (w szczególności, jeśli masz problem z zapamiętaniem hasła o dużym poziomie skomplikowania).
11. Nie udostępniaj swoich haseł innym osobom/podmiotom.
12. Nie korzystaj z tzw. „otwartych" sieci Wi-Fi.
13. W przypadku znalezienia jakiegoś magnetycznego/półprzewodnikowego nośnika danych (np. pendrive, dysk twardy, karta pamięci) lub optycznego nośnika danych (np. płyta CD, DVD, BluRay) pod żadnym pozorem nie podłączaj takich urządzeń do swoich urządzeń (komputer, komórka, tablet).

Zachęcamy Cię do śledzenia na bieżąco stron internetowych wyspecjalizowanych w zakresie cyberbezpieczeństwa organizacji takich jak:

- https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo
- https://www.cert.pl/publikacje/
- https://akademia.nask.pl/publikacje/