Realizując obowiązek wynikający z ustawy z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560)* udostępniamy poniżej kilka najistotniejszych informacji pozwalających przyswoić sobie podstawowe zagadnienia związane z cyberbezpieczeństwem.

CYBERBEZPIECZEŃSTWO – „odporność systemów informacyjnych na wszelkie 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).

SYSTEM INFORMACYJNY – system teleinformatyczny (zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego) wraz z przetwarzanymi w nim danymi w postaci elektronicznej.

POUFNOŚĆ DANYCH – cecha „polegająca na tym, że informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, przedmiotom lub procesom".[1]

INTEGRALNOŚĆ DANYCH – cecha „polegająca na zapewnieniu dokładności i kompletności aktywów"[2], to znaczy zagwarantowaniu, że dane nie będą przypadkowe lub celowo zmieniane lub uszkadzane.

DOSTĘPNOŚĆ – cecha polegająca na tym, że dane są dostępne osobom upoważnionym w danym momencie (czasie).

AUTENTYCZNOŚĆ – „właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana"[3].

NAJBARDZIEJ ROZPOWSZECHNIONE RODZAJE CYBERATAKÓW

PHISHING – atak cybernetyczny polegający na podszywaniu się atakującego pod inny podmiot lub osobę i nakłanianiu atakowanego do wykonania pożądanej przez atakującego czynności. Atakowany jest przy tym przekonany, że postępuje zgodnie z oczekiwaniami podmiotu lub osoby legalnie działającego.

MALWARE („złośliwe oprogramowanie") – oprogramowanie, które stworzono w celu naruszenia prawidłowego działania komputera, systemów komputerowych, czy urządzeń mobilnych bez wiedzy użytkownika. Do „złośliwego oprogramowania" zalicza się miedzy innymi: wirusy, tzw. robaki, konie trojańskie, oprogramowanie szpiegujące. Jest ono wykorzystywane do kradzieży danych, haseł, pieniędzy lub do blokowania dostępu do urządzeń w celu wymuszenia okupu.

DDoS – „rozproszona odmowa usługi" – zmasowane, zautomatyzowane i fałszywe próby skorzystania z usługi dostępnej on-line z wielu komputerów jednocześnie. Skutkiem ataku jest znaczące spowolnienie lub całkowite zablokowanie funkcjonowanie usługi.

Więcej informacji, które przybliżą i pozwolą zrozumieć Państwu zagrożenia związane z cyberbezpieczeństwem, a także będą zawierały wskazówki w zakresie stosowania skutecznych sposobów zabezpieczania się przed tymi zagrożeniami znajdziecie Państwo na stronach internetowych:

https://www.cert.pl/ouch/.

https://www.cert.pl/publikacje/.

https://stojpomyslpolacz.pl/stp/dobre-praktyki

---

[1] D. Lisiak-Felicka, M. Szmit, *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016, s. 34;
[2] *Ibidem;*
[3] *Ibidem;*