PORADNIK CYBERBEZPIECZEŃSTWA

Realizując zadanie wynikające z art. 22 ust. 1 pkt. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 z późn. zm.) przekazujemy Państwu informacje pozwalające zrozumieć zagrożenia występujące w cyberprzestrzeni oraz porady jak zabezpieczać się przed tymi zagrożeniami.

Czym jest cyberbezpieczeństwo?

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 wskazanej ustawy).

Cyberbezpieczeństwo to proces, którego celem jest ochrona danych i systemów przed zagrożeniami, jakie niosą za sobą cyberataki. Wdrożenie odpowiednich procedur w tym zakresie pozwala minimalizować skutki działań cyberprzestępców.

Czym jest cyfrowy ślad?

Cyfrowy ślad generuje każda nasza czynność w Internecie. Składają się na niego dwa rodzaje informacji:

- Dane o użytkowniku na podstawie adresu sieciowego – tzw. adresu IP — który jest generowany dla każdego urządzenia łączącego się z siecią. Adres IP może pomóc w ustaleniu lokalizacji, w której znajduje się urządzenie. Ponadto, na jego podstawie można ustalić m.in. wersję wykorzystywanego systemu operacyjnego, zestaw zainstalowanych czcionek i przeglądarek internetowych;
- Dane dotyczące ruchu w sieci, czyli ile czasu w niej spędzamy. Cały ruch na naszych urządzeniach jest zapisany na serwerze dostawcy usług telekomunikacyjnych. Przeglądarki zapamiętują odwiedzane strony, zaś wyszukiwarki — pytania, które zadajemy. Dzięki tzw. ciasteczkom (pliki „cookies") serwery stron mogą śledzić naszą aktywność w sieci. Pamiętaj, że masz możliwość samodzielnego zarządzania (w tym usuwania i blokowania) „cookies". Umożliwiają to np. przeglądarki internetowe, z których korzystasz.

Najpopularniejsze zagrożenia w cyberprzestrzeni:

- ataki socjotechniczne (przykładowo phishing, czyli metoda polegająca na wyłudzaniu poufnych informacji przez podszycie się pod godną zaufania osobę lub instytucję);
- kradzieże (wyłudzenia), modyfikacje lub niszczenie danych;
- kradzieże tożsamości;
- ataki z użyciem szkodliwego oprogramowania (malware, wirusy, robaki, itp.);
- blokowanie dostępu do usług;
- spam (niechciane lub niepotrzebne wiadomości elektroniczne mogące zawierać odnośniki do szkodliwego oprogramowania).

Zagrożenia ze strony cyberprzestępców mogą spowodować m.in. utratę wrażliwych danych, straty finansowe w wyniku kradzieży, duże koszty związane z odzyskaniem skradzionych danych, utrata dobrej reputacji.

Przykładowe sposoby zabezpieczenia się przed zagrożeniami:

- dbanie o prywatność, informacje o sobie należy udostępniać w sposób rozsądny i tylko w takim zakresie, w jakim jest to konieczne;
- stosowanie zasady ograniczonego zaufania do odbieranych wiadomości e-mail, SMS, stron internetowych nakłaniających do podania danych osobowych;
- zachowanie szczególnej ostrożności w przypadku podejrzanych linków wysyłanych przez e-mail, SMS lub wiadomości z popularnych komunikatorów internetowych i mediów społecznościowych;
- regularne aktualizowanie systemu operacyjnego i aplikacji;
- instalowanie, użytkowanie i aktualizowanie oprogramowania antywirusowego;
- korzystanie z zapór sieciowych (firewall);
- nieotwieranie plików nieznanego pochodzenia;
- regularne skanowanie komputera za pomocą programów antywirusowych;
- używanie legalnego oprogramowania pochodzącego z wiarygodnych źródeł;
- regularne wykonywanie kopii zapasowych ważnych danych;
- korzystanie z silnych haseł i dwuskładnikowej weryfikacji podczas logowania;
- korzystanie z różnych haseł do różnych usług elektronicznych;
- korzystanie z szyfrowanych protokołów transmisji danych;
- szyfrowanie poufnych danych wysyłanych pocztą elektroniczną;

- szyfrowanie dysków twardych komputerów;
- korzystanie ze stron banków, dostawców poczty elektronicznej czy portali społecznościowych, które mają ważny certyfikat bezpieczeństwa;
- unikanie z korzystania otwartych sieci Wi-Fi;
- praca na najniższych możliwych uprawnieniach użytkownika.

Dodatkowe informacje na temat cyberbezpieczeństwa:

- Jak chronić się przed cyberatakami? Praktyczne wskazówki: https://www.gov.pl/attachment/5a702c24-aaaa 4da0-9502-ea1c940a31d6
- ABC cyberbezpieczeństwa – darmowy poradnik NASK zawierający 157 ułożonych alfabetycznie pigułek wiedzy dotyczących z jednej strony wirtualnych zagrożeń, a z drugiej – dobrych praktyk i cyfrowych nawyków: https://abccyberbezpieczenstwa.pl/
- Zestaw porad bezpieczeństwa dla użytkowników komputerów prowadzony na stronie internetowej CSIRT NASK: https://www.cert.pl/ouch/
- Baza wiedzy nt. Cyberbezpieczeństwa na stronie Ministerstwa Cyfryzacji: https://www.gov.pl/web/baza wiedzy/cyberbezpieczenstwo
- Publikacje z zakresu cyberbezpieczeństwa na stronie CERT Polska: https://www.cert.pl/