Cyberbezpieczeństwo

Zgodnie 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 zmianami), przekazujemy Państwu informacje pozwalające na zrozumienie czym jest cyberbezpieczeństwo oraz jak się chronić przez zagrożeniami występujących w cyberprzestrzeni.

Czym jest „cyberbezpieczeństwo"?

Cyberbezpieczeństwo to dziedzina zajmująca się ochroną systemów komputerowych, sieci, urządzeń oraz danych przed nieautoryzowanym dostępem, atakami i innymi zagrożeniami w świecie cyfrowym. Jego celem jest zapewnienie poufności, integralności i dostępności informacji, a także minimalizowanie ryzyka cyberataków, które mogą prowadzić do kradzieży danych, strat finansowych czy zakłóceń w działaniu systemów. W praktyce cyberbezpieczeństwo obejmuje technologie, procedury i dobre praktyki, które wspólnie chronią użytkowników oraz organizacje przed zagrożeniami w cyberprzestrzeni.

Czym jest „cyberprzestrzeń"?

Cyberprzestrzeń to ogół środowisk i systemów cyfrowych, w których ludzie komunikują się, przechowują dane i korzystają z usług za pośrednictwem Internetu i innych sieci komputerowych. Obejmuje ona między innymi sieci społecznościowe, strony internetowe, aplikacje mobilne i inne platformy cyfrowe. Jest to wirtualna przestrzeń, w której odbywa się wymiana informacji oraz interakcje między ludźmi i urządzeniami.

Najczęściej występujące zagrożenia w cyberprzestrzeni to:

- ataki wykorzystujące inżynierię społeczną, tzw. **phishing**, czyli technika polegająca na tym, że przestępcy internetowi próbują Cię oszukać i spowodować, abyś podjął działanie zgodnie z ich zamierzeniami, najczęściej poprzez wysyłanie maili, smsów zawierających odnośnik do fałszywej strony internetowej, podając się przy tym za osobę lub instytucję godną zaufania;
- ataki z użyciem złośliwego oprogramowania, czyli tzw. **malware** (wirusy, robaki, trojany itp.), które może przejąć kontrolę nad Twoim komputerem, smartfonem, wykraść hasła oraz inne ważne informacje;
- ataki z żądaniem okupu, tzw. **ransomware**, polegające najczęściej na zaszyfrowaniu, bądź zablokowaniu dostępu do Twoich danych, po czym pojawia się monit z żądaniem zapłacenia okupu za odblokowanie/odszyfrowanie lub nieopublikowanie wykradzionych danych;
- **kradzieże tożsamości**, do których przestępcy używają wykradzionych lub wyłudzonych wcześniej danych, skutkujące np. zaciągnięciem w Twoim imieniu zobowiązań kredytowych;
- **blokowanie dostępu do usług**, czyli tzw. **atak DoS** (atak odmowy usługi) lub **DDoS** (rozproszony atak odmowy usługi), charakteryzujący się najczęściej zmasowanym zalewaniem danego urządzenia ruchem sieciowym, skutkującym zablokowaniem oferowanych usług;
- niechciane wiadomości elektroniczne, czyli tzw. **spam**.

Zalecane sposoby zabezpieczenia się przed zagrożeniami w cyberprzestrzeni:

- **Stosuj oprogramowanie antywirusowe**, które jest na bieżąco aktualizowane i które posiada ochronę w czasie rzeczywistym – dzięki takiemu oprogramowaniu możemy się ustrzec przed pobraniem i uaktywnieniem złośliwego oprogramowania;

- **Aktualizuj na bieżąco system operacyjny oraz zainstalowane oprogramowanie** – co pozwoli na zabezpieczenie Twojego urządzenia przed wykrytymi lukami / podatnościami

- w oprogramowaniu, które mogą wykorzystać cyberprzestępcy, aby przejąć dostęp do Twojego urządzenia;

- **Stosuj zasadę ograniczonego zaufania** w odniesieniu do odbieranych wiadomości e-mail, wiadomości SMS, czy też połączeń telefonicznych. Weryfikuj nadawcę wiadomości, zwracaj uwagę na podejrzaną treść wiadomości (błędy stylistyczne, literówki itp.), a także unikaj otwierania załączonych odnośników lub plików, bez upewnienia się, czy pochodzą z zaufanego źródła;

- **Weryfikuj zgodność certyfikatu bezpieczeństwa oraz adres odwiedzanych stron**, w szczególności na stronach banków, dostawców poczty elektronicznej, serwisach aukcyjnych i zakupowych, czy portali społecznościowych - sama informacja o bezpiecznym połączeniu nie oznacza, że połączyliśmy się z właściwą stroną. Zdecydowana większość fałszywych stron przygotowanych przez cyberprzestępców posiada ważny certyfikat, ważne abyś weryfikował na jaki adres i podmiot certyfikat został wystawiony. Korzystaj także z ustawionych przez siebie zakładek do często odwiedzanych stron lub wpisuj adres ręcznie w przeglądarce;

- **Miej zawsze aktywną zaporę sieciową**, tzw. **firewall** na swoim urządzeniu;

- **Zadbaj o swoje dane, wykonując ich kopię zapasową** na inny nośnik i/lub w usłudze chmurowej – będziesz miał możliwość odzyskania danych na wypadek awarii bądź celowego usunięcia danych przez cyberprzestępcę;

- **Unikaj korzystania z niezabezpieczonych hasłem, otwartych sieci WIFI** - podczas korzystania z takich sieci potencjalny atakujący może zobaczyć co wysyłasz i odbierasz z Internetu, jeśli komunikacja nie jest dodatkowo zabezpieczona, np. szyfrowaniem na poziomie aplikacji;

- **Nie wysyłaj pocztą elektroniczną poufnych danych bez ich uprzedniego zaszyfrowania** – używaj programów do szyfrowania plików zawierających poufne dane, hasło do odszyfrowania przekazuj innym kanałem, np. smsem lub telefonicznie;

- **Nie loguj się do banku, poczty elektronicznej oraz innych ważnych serwisów na urządzeniach niezaufanych** – potencjalny cyberprzestępca może użyć programu rejestrującego wprowadzane znaki na klawiaturze, tzw. **keylogger**, przechwytując ważne dane, w tym login i hasło do usługi, lub spróbować przejąć Twoją zalogowaną sesję, dzięki czemu będzie w stanie przejąć Twoje konto w danym serwisie lub usłudze;

- **Nie podawaj swoich danych osobowych w niezaufanych serwisach i stronach internetowych** – cyberprzestępcy mogą próbować wyłudzić Twoje dane, by je wykorzystać do późniejszego ataku;

- **Nigdy nie ujawniaj nikomu swoich haseł** – żadne instytucje (banki, urzędy, itp.) nigdy nie żądają w komunikacji z klientami wyjawienia hasła do logowania;

- **Nie pobieraj i nie instaluj oprogramowania z niezaufanych źródeł** – cyberprzestępcy bardzo często tworzą oprogramowanie lub modyfikują legalne i zaufane aplikacje, dodając do nich złośliwe oprogramowanie, dlatego zawsze pobieraj oprogramowanie bezpośrednio od zaufanego producenta / twórcy;
- **Zawsze skanuj programem antywirusowym pliki pobrane z Internetu bądź z urządzeń wymiennych** (pendrive, karty pamięci, dyski zewnętrzne itp.), zanim je otworzysz;
- **Staraj się używać unikalnych i silnych haseł**, w szczególności dotyczy to haseł do bankowości elektronicznej oraz poczty elektronicznej - korzystanie z menedżerów haseł może znacznie ułatwić to zadanie;

Szerszy zakres porad oraz informacji w zakresie cyberbezpieczeństwa możesz znaleźć, m.in.:

- w cyklicznym, darmowym zestawie porad bezpieczeństwa dla użytkowników komputerów na witrynie internetowej Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Naukową i Akademicką Sieć Komputerową (CSIRT NASK) pod adresem: https://www.cert.pl/ouch/
- w poradniku CSIRT NASK dotyczącym tworzenia bezpiecznych haseł pod adresem: https://cert.pl/bezpieczne-hasla/
- w publikacjach na witrynie internetowej CSIRT NASK pod adresem: https://www.cert.pl/publikacje/
- w publikacjach zespołu Dyżurnet.pl, składającego się z ekspertów Naukowej i Akademickiej Sieci Komputerowej, działającego jako punkt kontaktowy do zgłaszania nielegalnych treści w Internecie, pod adresem: https://dyzurnet.pl/publikacje
- w bazie wiedzy na witrynie internetowej Ministerstwa Cyfryzacji pod adresem: https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo.

Miejsca, gdzie można zgłosić incydenty dot. cyberbezpieczeństwa oraz podejrzane strony lub nielegalne treści:

- **Incydenty cyberbezpieczeństwa** można zgłaszać pod adresem: https://incydent.cert.pl
- **Nielegalne treści publikowane w Internecie** można zgłaszać pod adresem: https://dyzurnet.pl
- **Podejrzane domeny** (adresy stron internetowych), które mogą służyć do wyłudzeń danych i środków finansowych można zgłaszać pod adresem: https://incydent.cert.pl/phishing
- **Podejrzane wiadomości SMS** można przesyłać na numer **8080**, za pomocą opcji „Prześlij dalej” lub „Udostępnij”, jeśli wiadomość zawierała szkodliwą treść, otrzymasz odpowiednie ostrzeżenie od CERT Polska.