

Cyberbezpieczeństwo

Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa publikujemy informacje na temat zagrożeń występujących w cyberprzestrzeni oraz porady jak zabezpieczyć się przed tymi zagrożeniami.

Definicja cyberbezpieczeństwa

Cyberbezpieczeństwo to zgodnie z obowiązującymi przepisami „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 (Dz.U. z 2020 r. poz. 1369, z późn.zm.).

Najpopularniejsze zagrożenia w cyberprzestrzeni:

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

Rodzaje zagrożeń cyberbezpieczeństwa:

- **Phishing** – Jest to metoda oszustwa, oznaczająca w tradycyjnym rozumieniu tego słowa podszywanie się (przede wszystkim z wykorzystaniem poczty elektronicznej i stron internetowych www.) pod inną osobę, instytucję lub znane marki, w celu wyłudzenia określonych informacji takich jak numery oraz hasła PIN kart płatniczych, hasła logowania do urzędów czy też płatności internetowej banków lub szczegółów karty kredytowej w celu wyłudzenia danych. Jest to rodzaj ataku oparty na tzw. inżynierii społecznej.
- **Atak DDoS** atak na system komputerowy lub usługę sieciową w celu uniemożliwienia świadczenia tej usługi (odmowy jej realizacji) polegający na zablokowaniu działania poprzez zajęcie wszystkich wolnych zasobów, przeprowadzany równocześnie z wielu komputerów. Ataki te nie uszkadzają danych, gdyż ich celem jest utrudnienie lub uniemożliwienie dostępu do nich, co może skutkować równie kosztownymi stratami co utrata danych. Ataki te są stanowią jeden z najprostszych sposobów paraliżowania infrastruktury sieciowej oraz aplikacji, jednakże wymagają użycia równocześnie kilku tysięcy urządzeń. Do przeprowadzenia ataku służą najczęściej komputery, nad którymi przejęto kontrolę przy użyciu specjalnego oprogramowania, i które na dany sygnał zaczynają jednocześnie atakować system ofiary, zasypując go fałszywymi próbami skorzystania z usług, jakie oferuje.
- **Złośliwe oprogramowanie (Malware)** - To określenie opisuje całą gamę szkodliwych programów i aplikacji, które po uzyskaniu dostępu do sieci podmiotu lub instytucji może poczynić wiele szkód. Złośliwe oprogramowanie może przyjąć formę wirusów, robaków, koni trojańskich i innych,

- **Atak Key Logger (ang. Key Logger Attack)** – Cyberprzestępcy używają programów, które mogą zapisywać naciśnięcie każdego klawisza na klawiaturze. Dzięki temu mogą poznać login i hasło użytkownika zainfekowanego komputera. Wystarczy raz zalogować się do danej usługi żeby dostarczyć przestępcom pełne dane.
- **Malvertising** – pozwala przestępcom na dotarcie do użytkowników przeglądających zaufane strony internetowe poprzez nośniki jakimi są udostępniane na stronach internetowych reklamy, a następnie na instalowanie bez wiedzy i zgody użytkownika złośliwego oprogramowania na urządzeniach użytkownika.
- **Ransomware** to rodzaj złośliwego oprogramowania, które infekując urządzenie lub komputer blokuje jego podstawowe funkcje i wymusza użytkownika do zapłacenia haraczu, w zamian za przywrócenie kontroli nad systemem operacyjnym i umożliwienia dostępu do danych zgromadzonych na komputerze. Zagrożenie może dostać się do komputera za pośrednictwem pobranego pliku, wykorzystując niespójności w strukturze ochrony lub nawet przez wiadomość tekstową.

Czym się różni od typowego złośliwego oprogramowania?

- Nie kradnie danych użytkownika, lecz je szyfruje.
- Wymusza płatność okupu, zazwyczaj w dolarach lub Bitcoinach.
- Jest relatywnie łatwy do stworzenia – istnieje wiele bardzo dobrze udokumentowanych cryptobibliotek.

Sposoby zabezpieczenia się przed zagrożeniami:

- Aktualizowanie systemu operacyjnego i aplikacji bez zbędnej zwłoki.
- Regularne wykonywanie kopii zapasowych ważnych danych na zewnętrzny nośnik. Taki nośnik podpinamy tylko jak wykonujemy kopię. W przypadku zaszyfrowania danych, będziesz mógł je przywrócić z kopii zapasowej.
- Higiena hasła - nie da się obronić przed atakami używając prostych haseł, takich jak „1234”. Odpowiednie, złożone hasło może ochronić konsumentów przed zagrożeniami cybernetycznymi.
- Oprogramowanie antywirusowe - subskrybuj dobrej jakości oprogramowanie antywirusowe oraz zaplanuj aktualizacje automatyczne systemu operacyjnego na Twoim urządzeniu.
- Nie otwieraj plików nieznanego pochodzenia. Zachowaj ostrożność podczas otwierania załączników plików. Na przykład, jeśli otrzymasz wiadomość e-mail z załącznikiem PDF z opisem „zaległa faktura”, nie otwieraj go jeśli zobaczysz, że pochodzi on z nietypowego e-maila, takiego jak jank4a361@gmail.com ! Otwórz dopiero jeżeli masz 100% pewności, że wiesz kto wysłał wiadomość.
- Nie korzystaj ze stron internetowych, które nie mają ważnego certyfikatu bezpieczeństwa, chyba że masz stuprocentową pewność, że strona taka jest bezpieczna.
- Staraj się nie odwiedzać zbyt często stron, które oferują darmowe atrakcje (filmiki, muzykę, aplikacje) - często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia.
- Nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach,

- Pamiętaj, że żadna instytucja nie wysyła e-maili do swoich klientów/interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.

Zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie sposobów zabezpieczania się przed zagrożeniami to wiedza niezbędna każdemu użytkownikowi komputera, smartphona czy też usług internetowych. Należy pamiętać, że najlepszym sposobem na ustrzeżenie się przed negatywnymi skutkami zagrożeń jest działalność zapobiegawcza.

Dodatkowe informacje można znaleźć:

- w publikacjach na witrynie internetowej CSIRT NASK – Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym pod adresem: <https://www.cert.pl/publikacje/>
- w poradach bezpieczeństwa dla użytkowników komputerów na witrynie internetowej CSIRT NASK pod adresem: <https://www.cert.pl/ouch/>
- w poradach CSIRT NASK dotyczących tworzenia silnych haseł pod adresem: <https://www.cert.pl/hasla/>
- w publikacjach Dyżurnet - zespołu ekspertów NASK - punktu kontaktowego do zgłaszania nielegalnych treści w Internecie pod adresem: <https://dyzurnet.pl/publikacje>
- w bazie wiedzy na witrynie internetowej Kancelarii Prezesa Rady Ministrów pod adresem: <https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo>
- na stronie internetowej kampanii STÓJ. POMYŚL. POŁĄCZ pod adresem: <https://stojpomyslpolacz.pl/stp/>.

Incydenty cyberbezpieczeństwa możecie Państwo zgłaszać pod adresem incydent.cert.pl

Podejrzane strony które mogą wyludzać dane osobowe, dane uwierzytelniające do kont bankowych lub serwisów społecznościowych, mogą Państwo zgłaszać za pomocą formularza dostępnego na incydent.cert.pl/phishing

W przypadku gdy źródłem podejrzanej strony jest wiadomość SMS, możecie Państwo ją przekazać CSIRT NASK na numer + 48 799 448 084 w sposób opisany poniżej:

Podejrzaną wiadomość SMS zawierającą link możecie Państwo przesłać na numer 799 448 084 wykorzystując funkcję "przekaż" albo "udostępnij" w swoim telefonie. Trafi ona bezpośrednio do analityków CERT NASK, którzy zdecydują o dopisaniu podejrzanej domeny do listy ostrzeżeń. Z jednego numeru można zgłosić maksymalnie 3 wiadomości w ciągu 4 godzin. Należy pamiętać że numer służy wyłącznie do zgłaszania prób wyludzeń internetowych (phishingu, fałszywych aplikacji) - nie przyjmowane tą drogą będą zgłoszenia dotyczące usług SMS premium. Podany numer służy tylko do przyjmowania SMS-ów - numer do telefonicznego zgłaszania incydentów znajduje się na stronie <https://incydent.cert.pl>