Cyberbezpieczeństwo

Cyberbezpieczeństwo oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami (art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06.2019, str. 15, z późn. zm.))

Zagrożenia w cyberprzestrzeni (przykłady)

- **Phishing** – to atak wykorzystujący socjotechnikę mający na celu nakłonienie do podjęcia określonych działań przez osobę będącą celem ataku (podanie danych, zainstalowanie określonej aplikacji, kliknięcie w link itp.). Przestępcy podszywają się pod znane i budzące zaufanie instytucje lub osoby, także pod osoby najbliższe ofierze ataku i poprzez silne oddziaływanie na emocje (np. informacja o niespodziewanej wygranej lub o próbie zaciągnięcia kredytu na konto ofiary) i wywieranie presji czasu (np. nagrodę można odebrać tylko przez określony czas lub natychmiast należy podać dane lub zainstalować daną aplikację i podjąć w niej określone czynności aby zablokować procedurę udzielania kredytu) próbują zrealizować swoje cele. Do phishingu są wykorzystywane wiadomości e-mail, wiadomości SMS, komunikatory internetowe lub połączenia telefoniczne.
- **Ransomware** – to atak polegający na zaszyfrowaniu danych na urządzeniu i żądaniu okupu za ich odszyfrowanie. Często w tego rodzaju atakach przed zaszyfrowaniem danych przestępcy je pobierają.
- **Malware** – to wszelkiego rodzaju złośliwe oprogramowanie, za pomocą którego przestępcy np. przejmują dostęp nad urządzeniem, wykradają dane lub uszkadzają oprogramowanie. Malware może zostać zainstalowany przy pobieraniu przez użytkownika treści z Internetu, poprzez otwarcie załącznika w poczcie elektronicznej czy z zewnętrznego nośnika pamięci.
- **Deepfake**– to rodzaj oszustwa polegającego na tworzeniu, z wykorzystaniem sztucznej inteligencji, treści audio lub wideo, których zadaniem jest nakłonienie użytkownika Internetu do podjęcia określonych działań lub kształtowania jego poglądów. Oszustwo to polega na podszywaniu się pod znaną lub budzącą zaufanie osobę (np. polityka, sportowca lub artystę) i zachęcaniu np. do „inwestowania" w dany sposób lub przekazywaniu fałszywych informacji w innym celu (np. dezinformacji). Ponadto w komunikatorach internetowych przeprowadzane są oszustwa polegające na podszywanie się pod głos osoby bliskiej, w których oszuści przesyłają spreparowane wiadomości głosowe.
- **Fałszywa CAPTCHA** – CAPTCHA to wykorzystywany na stronach internetowych test służący do odróżnienia ludzi od botów polegający np. na wybraniu kafelków, na których znajduje się rower, auto, przejście dla pieszych itp. Przestępcy podszywając się pod CAPTCHA zamieszczają fałszywą instrukcję potwierdzenia, że nie jest się robotem, która wymaga wykonania określonych kombinacji na klawiaturze. TO PUŁAPKA – taka kombinacja powoduje uruchomienie złośliwego kodu służącego przejęciu kontroli nad urządzeniem lub wykradnięciu danych.
- **Ataki typu „Man in the Middle"** – ataki polegające na przechwytywaniu przez przestępców informacji wymienianych przez użytkowników, którzy o tym nie wiedzą i myślą, że komunikują się bezpośrednio ze sobą. Do takiego ataku może dojść np. poprzez połącznie się z otwartą siecią Wi-Fi do której dostał się przestępca.
- **Ataki DoS lub DDoS** – to ataki, których celem jest zakłócenie działania serwera lub sieci poprzez ich przeciążenie co odbywa się w drodze wysyłania bardzo dużej liczby żądań. W wyniku takiego ataku usługa lub strona internetowa może być czasowo niedostępna.
- **Ataki dotyczące IoT** – to ataki, które ukierunkowane są na przejęcie kontroli nad „inteligentnymi" urządzeniami podłączonymi do sieci np. kamery, głośniki.

Co zrobić, aby zwiększyć swoje bezpieczeństwo?

- pamiętaj o aktualizowaniu oprogramowania sprzętu oraz programów/aplikacji z których korzystasz – nie odkładaj tego na później,
- pamiętaj o instalowaniu programów/aplikacji wyłącznie z zaufanego źródła,
- pamiętaj o ustawieniu silnego hasła, nie ustawiaj tego samego hasła w różnych serwisach, nie zapisuj go w pamięci przeglądarki, nikomu go nie zdradzaj – rozważ wykorzystywanie menadżera haseł,
- jeżeli jest to możliwe ustaw do logowania metodę uwierzytelniania dwuskładnikowego,
- nie loguj się do swoich kont na niezaufanym sprzęcie,
- nie podejmuj decyzji pod wpływem emocji – uważaj np. na informacje o niespodziewanej wygranej, otrzymaniu pokaźnego spadku po krewnym, o istnieniu którego nie wiedziałeś, wypadku osoby bliskiej i powiązanej z nim konieczności przekazania pieniędzy czy informacje z „banku", że z twojego konta bankowego robione są operacje na wysokie kwoty i należy podać dane do uwierzytelnienia (login i hasło) aby zatrzymać ich wykonywanie,
- w przypadku otrzymania wiadomości w komunikatorze internetowym (w tym głosowej) od znajomego z prośbą o podanie kodu BLIK (który twierdzi np. że zablokowano mu kartę płatniczą, lub zgubił portfel a musi pilnie dokonać płatności np. kupić bilet, zapłacić za taksówkę) skontaktuj się z tą osobą w inny sposób np. zadzwoń do niej w celu potwierdzenia, że prośba pochodzi właśnie od tej osoby. Otrzymanie wiadomości, o których mowa wyżej może bowiem świadczyć, że konto Twojego znajomego zostało przejęte przez oszusta,
- zachowaj czujność w stosunku do treści audio i wideo, w których znane osoby zachęcają do podjęcia określonych czynności np. inwestowania czy kupowania określony produktów, zwróć uwagę czy treści te wyglądają naturalnie – czy zgadza się mimika twarzy, sposób poruszania, sposób wypowiedzi – UWAGA techniki generowania głosu i obrazu ulegają stałem doskonaleniu – nie wierz we wszystko co zobaczysz lub usłyszysz,
- uważaj na otwarte sieci Wi-Fi udostępniane w kawiarniach, restauracjach itp., używaj VPN,
- dokładnie sprawdzaj adres e-mail, z którego wysłano do ciebie wiadomość – np. czy nie ma w nim „literówek" lub czy litery nie zostały zastąpione innymi literami, cyframi lub znakami np. „l" na „I", „O" na „0",
- nie otwieraj załączników ani linków, które otrzymałeś na swoją pocztę elektroniczną lub w wiadomości SMS, jeżeli treść wiadomości lub jej nadawca wzbudza twoje podejrzenia,
- zachowaj czujność, jeżeli dane usługa lub serwis wymaga podania szeregu danych osobowych, których podanie nie znajduje uzasadnienia w charakterze danej usługi lub serwisu,
- korzystaj z opcji dostosowywania ustawień prywatności jakie oferują strony lub portale internetowe oraz aplikacje,

- pamiętaj o wykonywaniu regularnych kopii zapasowych swoich danych,
- korzystaj z programów antywirusowych.

Incydenty dotyczące cyberbezpieczeństwa można zgłosić do CERT Polska (więcej informacji: Incydent? Nie działaj w pojedynkę – zgłoś go do CERT Polska):

- za pośrednictwem formularza dostępnego na https://incydent.cert.pl/,
- wysyłając SMSa na numer 8080 lub
- za pośrednictwem aplikacji mObywatel.

W przypadku podejrzenia popełnienia przestępstwa należy je zgłosić w najbliższej jednostce Policji lub prokuratury.

Więcej informacji na temat cyberbezpieczeństwa można znaleźć na:

- CERT Polska
- OUCH! | CERT Polska
- Aktualności - Baza wiedzy - Portal Gov.pl