Cyberbezpieczeństwo – informacje dla użytkowników

Zgodnie z art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa cyberbezpieczeństwo oznacza odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

Na podstawie art. 9 ust. 1 pkt 2 ustawy o krajowym systemie cyberbezpieczeństwa podmiot kluczowy lub podmiot ważny zapewnia użytkownikowi usługi dostęp do wiedzy pozwalającej na zrozumienie cyberzagrożeń oraz stosowanie skutecznych sposobów ochrony przed nimi, w zakresie związanym ze świadczonymi usługami. Obowiązek ten może być realizowany w szczególności przez udostępnianie informacji na stronie internetowej.

Poniżej przedstawiamy podstawowe informacje o najczęstszych zagrożeniach oraz zasady bezpiecznego korzystania z Internetu i usług cyfrowych.

Najczęstsze cyberzagrożenia

- **Phishing** – próba wyłudzenia danych, np. loginu, hasła, kodu BLIK lub danych karty płatniczej, przez wiadomość e-mail, SMS, komunikator albo fałszywą stronę internetową podszywającą się pod bank, urząd, firmę kurierską lub inną zaufaną instytucję.
- **Smishing** – phishing prowadzony za pomocą wiadomości SMS.
- **Vishing** – oszustwo telefoniczne, w którym przestępca podszywa się np. pod pracownika banku, urzędu, Policji lub członka rodziny.
- **Qrishing** – oszustwo wykorzystujące fałszywy kod QR, prowadzący np. do podrobionej strony logowania, fałszywej płatności lub złośliwego oprogramowania.
- **Spear phishing** – ukierunkowany atak przygotowany pod konkretną osobę lub organizację, często z wykorzystaniem danych dostępnych w Internecie.
- **Malware** – złośliwe oprogramowanie, w tym wirusy, trojany, programy szpiegujące, ransomware i inne narzędzia służące m.in. do kradzieży danych, przejęcia urządzenia albo zaszyfrowania plików.
- **Ransomware** – rodzaj złośliwego oprogramowania, które blokuje dostęp do danych lub systemu i żąda okupu za ich odblokowanie.
- **Kradzież tożsamości** – wykorzystanie cudzych danych osobowych, kont, dokumentów lub wizerunku bez uprawnienia.
- **Ataki socjotechniczne** – manipulowanie emocjami, pośpiechem lub zaufaniem użytkownika, aby skłonić go do ujawnienia informacji, wykonania przelewu albo zainstalowania oprogramowania.
- **Deepfake** – fałszywe nagranie audio lub wideo, często wykorzystujące wizerunek lub głos znanej osoby. Może służyć do oszustw inwestycyjnych, wyłudzeń danych lub podszywania się pod bliskich i współpracowników.
- **Baiting** – pozostawienie lub przesłanie nośnika albo pliku, który ma zachęcić do jego otwarcia, a następnie zainfekować urządzenie.
- **Ataki na dostępność usług** – działania prowadzące do przeciążenia lub zablokowania strony internetowej, systemu lub usługi.

Jak chronić siebie i dane

- Aktualizuj system operacyjny, przeglądarkę, aplikacje, oprogramowanie antywirusowe i urządzenia sieciowe. Włącz automatyczne aktualizacje, jeśli są dostępne.
- Korzystaj wyłącznie z legalnego oprogramowania oraz pobieraj aplikacje z oficjalnych sklepów i stron producentów.
- Używaj oprogramowania chroniącego przed złośliwym oprogramowaniem oraz włącz zaporę sieciową, jeśli jest dostępna.
- Stosuj silne, długie i niepowtarzalne hasła lub frazy hasłowe. Nie używaj jednego hasła w kilku usługach.
- Rozważ korzystanie z menedżera haseł; ułatwia on tworzenie i bezpieczne przechowywanie unikalnych haseł.
- Włącz uwierzytelnianie wieloskładnikowe (MFA), zwłaszcza dla poczty elektronicznej, bankowości, mediów społecznościowych i kont służbowych.
- Nie przekazuj nikomu haseł, kodów jednorazowych, kodów BLIK, kodów autoryzacyjnych ani danych karty płatniczej. Bank, urząd ani inna wiarygodna instytucja nie powinny żądać takich danych przez e-mail, SMS lub telefon.
- Przed kliknięciem w link sprawdź adres strony oraz nadawcę wiadomości. Uważaj na literówki w nazwach domen, nietypowe adresy e-mail i komunikaty wywołujące presję czasu.
- Nie otwieraj podejrzanych załączników ani plików z nieznanego źródła. Szczególną ostrożność zachowaj wobec plików z rozszerzeniami `.exe`, `.js`, `.zip`, `.rar`, `.iso` i dokumentów wymagających włączenia makr.
- Nie skanuj kodów QR z nieznanych źródeł bez uprzedniego sprawdzenia, dokąd prowadzą. Przed podaniem danych upewnij się, że adres strony jest prawidłowy.
- Zawsze samodzielnie wejdź na stronę banku, urzędu lub usługodawcy, wpisując jej adres w przeglądarce albo korzystając z oficjalnej aplikacji.
- Ogranicz ilość danych publikowanych w mediach społecznościowych. Weryfikuj ustawienia prywatności oraz nie akceptuj zaproszeń od nieznanych osób.
- Nie udostępniaj zdjęć dokumentów, kart płatniczych, biletów, kart pokładowych ani innych materiałów zawierających dane osobowe.
- Regularnie wykonuj kopie zapasowe ważnych danych. Przechowuj co najmniej jedną kopię poza urządzeniem, z którego korzystasz na co dzień.
- Zabezpiecz domową sieć Wi-Fi: zmień domyślne hasło administratora routera, stosuj silne hasło do sieci i aktualizuj oprogramowanie routera.
- Zachowaj ostrożność w publicznych sieciach Wi-Fi. Nie loguj się w nich do bankowości elektronicznej ani usług zawierających szczególnie wrażliwe dane, jeżeli nie jest to konieczne.
- Zabezpiecz telefon i komputer blokadą ekranu, kodem PIN, hasłem lub biometrią. Ustaw automatyczne blokowanie urządzenia.
- W przypadku wątpliwości przerwij działanie: nie klikaj, nie odpowiadaj, nie instaluj aplikacji i nie podawaj danych. Zweryfikuj informację innym kanałem kontaktu.

Gdy podejrzewasz oszustwo

- Podejrzanego SMS-a z linkiem prześlij dalej na bezpłatny numer **8080**.
- Podejrzany e-mail, stronę internetową, próbę phishingu lub inny incydent zgłoś przez formularz: incydent.cert.pl.

- Jeżeli podałeś dane do logowania, niezwłocznie zmień hasło, wyloguj aktywne sesje oraz włącz uwierzytelnianie wieloskładnikowe.
- Jeżeli przekazałeś dane bankowe, kod BLIK albo dane karty, natychmiast skontaktuj się ze swoim bankiem, korzystając z numeru podanego na oficjalnej stronie banku lub na karcie płatniczej.
- Zachowaj dowody zdarzenia: wiadomości, adresy stron, numery telefonów i zrzuty ekranu. Mogą być potrzebne przy zgłoszeniu do banku, CERT Polska lub organów ścigania.

Więcej informacji i zgłoszenia

- CERT Polska – aktualności i ostrzeżenia
- CERT Polska – poradniki OUCH!
- Zgłoszenie incydentu do CSIRT NASK / CERT Polska
- Baza wiedzy o cyberbezpieczeństwie – Ministerstwo Cyfryzacji
- Ministerstwo Cyfryzacji
- Urząd Ochrony Danych Osobowych – „Bądźmy bezpieczni w sieci”
- CSIRT GOV