

CYBERBEZPIECZEŃSTWO i cyberhigiena

Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak skutecznie stosować sposoby zabezpieczenia się przed tymi zagrożeniami.

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 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20).

Najpopularniejsze zagrożenia w cyberprzestrzeni:

- Ataki z użyciem szkodliwego oprogramowania (malware, wirusy, robaki, trojany itp.).
- Ataki z użyciem oprogramowania, które szyfruje dane na komputerze ofiary i żąda okupu za ich odblokowanie.
- Kradzieże tożsamości.
- Kradzieże (wyłudzenia), modyfikacje bądź niszczenie danych.
- Blokowanie dostępu do usług.
- Spam (niechciane lub niepotrzebne wiadomości elektroniczne).
- Ataki socjotechniczne (np. phishing, czyli wyłudzenie informacji przez podszywanie się pod godną zaufania osobę lub instytucję).
- Sposoby zabezpieczenia się przed zagrożeniami:
 - aktualizowanie systemu operacyjnego i aplikacji bez zbędnej zwłoki;
 - instalacja i użytkowanie oprogramowania przeciw wirusom i spyware (najlepiej stosować ochronę w czasie rzeczywistym);
 - aktualizacja oprogramowania antywirusowego oraz bazy danych wirusów;
 - sprawdzanie plików pobranych z internetu za pomocą programu antywirusowego;
 - pamiętanie o uruchomieniu firewalla;
 - nieotwieranie plików nieznanego pochodzenia;
 - korzystanie ze stron banków, poczty elektronicznej czy portali społecznościowych, które mają ważny certyfikat bezpieczeństwa, chyba, że masz 100% pewność z innego źródła, że strona taka jest bezpieczna;
 - regularne skanowanie komputera i sprawdzanie procesów sieciowych. Jeśli się na tym nie znasz poproś o sprawdzenie kogoś, kto się zna. Czasami złośliwe oprogramowanie nawiązujące własne połączenia z Internetem, wysyłając twoje hasła i inne prywatne dane do sieci. Może również zainstalować się na komputerze mimo dobrej ochrony;
 - nieużywanie niesprawdzonych programów zabezpieczających czy też do publikowania własnych plików w internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony);
 - regularne wykonywanie kopii zapasowych ważnych danych;
 - niezostawianie danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie ma się absolutnej pewności, że nie są one widoczne dla osób trzecich oraz nie wysyłanie w wiadomościach e-mail żadnych poufnych danych w formie otwartego tekstu

przykładowo dane powinny być zabezpieczone hasłem i zaszyfrowane. Hasło najlepiej przekazać w sposób bezpieczny przy użyciu innego środka komunikacji;

- należy pamiętać, że Urząd nie wysyła e-maili do swoich klientów/interesantów z prośbą o podanie jakiegokolwiek hasła lub loginu w celu ich weryfikacji.

Przedstawiamy poniżej kilka ważnych informacji jak stosować się do standardów cyberbezpieczeństwa w naszym Urzędzie:

1. Jeśli korzystasz z Internetu na terenie Urzędu, nie podłączaj się pod żadne inne publiczne sieci WIFI¹. Urząd udostępnia darmowe WIFI o nazwie sieci/ SSID „RZEKUN”. Podłączenie się pod internet z nieznanego źródła może skutkować wyłudzeniem danych logowania i danych osobowych, a nawet przejęciem urządzenia przez hakera².

Pamiętaj, że każdy może udostępnić sieć WIFI o takiej samej nazwie jak nasz Urząd. Aby zweryfikować, czy jest to bezpieczna sieć połącz się z nią i wejdź na stronę <https://hotspot.rzekun.pl> a następnie sprawdź w przeglądarce internetowej prawidłowość certyfikatu tej strony. Jeżeli przeglądarka będzie zgłaszała problem, to nie korzystaj z tej sieci i zgłoś nieprawidłowości jakiegokolwiek pracownikowi Urzędu.

Nasza sieć wymaga zalogowania z wyjątkiem dostępu do strony internetowej Urzędu <https://www.rzekun.pl>. Procedurę uzyskania danych dostępowych sieci „RZEKUN” znajdziesz na terenie Urzędu.

2. Jeżeli na terenie Urzędu znajdziesz pamięć USB³ pozostawioną bez opieki, koniecznie zgłoś to i przekazaj zgubę pracownikowi Urzędu. Absolutnie nie podłączaj urządzenia do własnego sprzętu, gdyż może ono zainfekować Twoją własność złośliwymi wirusami⁴.
3. Nie zostawiaj swojego telefonu lub laptopa na terenie Urzędu bez opieki, w szczególności jeśli sprzęt nie jest zabezpieczony silnym hasłem. Jeśli zgubisz urządzenie to pamiętaj, żeby zaraz po odnalezieniu zabrać je do specjalisty, który oceni czy ktoś nie włamał się do Twojego sprzętu i nie zainstalował na nim wirusa, który ściągałby dane logowania w czasie normalnego użytkowania urządzenia.
4. Otrzymałeś e-maila bądź SMS-a od naszego Urzędu np. z prośbą o zmianę terminu wizyty dot. załatwienia sprawy, a wiadomość zawiera link? Nie klikaj w niego. Urząd nie wysyła e-maili i SMS'ów z linkami do stron innych niż własna (<https://www.rzekun.pl>) lub będących własnością instytucji publicznych. Wejście w link może być próbą wyłudzenia danych, a to z kolei doprowadzić nawet do wyczyszczenia/obrabowania konta bankowego.
5. Upewnij się, że przy korzystaniu z telefonu komórkowego do sprawdzenia ważnych informacji osobistych np. numeru PESEL nikt nie jest wystarczająco blisko, aby zrobić zdjęcie lub przeczytać wrażliwe dane znajdujące się na Twoim telefonie komórkowym. Udostępnienie takich informacji pracownikom Urzędu jest jak najbardziej zasadne przy

1 WIFI – sieć komórkowa udostępniająca dostęp do Internetu urządzeniom mobilnym, np. telefonom komórkowym

2 Haker – to osoba, która w nielegalny sposób pozyskuje dane osobowe i dane logowania w celu uzyskania korzyści majątkowej, zazwyczaj na szkodę ofiary.

3 Pamięć USB – to mały nośnik danych zakończony wejściem USB, który może być podłączony do komputera. Mogą się na nim znajdować zdjęcia, filmy, dokumenty, ale też i wirusy.

4 Wirusy – złośliwe oprogramowanie stworzone przez hakera, które ma na celu zaszkodzić użytkownikowi komputera. Może zbierać wrażliwe dane, przejąć kontrolę nad aparatem, dając wgląd osobom postronnym w prywatne życie użytkownika albo nawet sprawić, że komputer będzie niezdatny do użytku.

weryfikowaniu tożsamości, ale nigdy nie wiesz kto patrzy Ci przez ramię, ani co zrobi z Twoimi prywatnymi danymi. Jeżeli jesteś świadkiem dziwnego zachowania zgłoś to pracownikowi Urzędu.

6. Widzisz urządzenie, pozostawione bez opieki, które jest podłączone do gniazda w ścianie? Czy to telefon komórkowy, modem albo urządzenie, którego nie rozpoznajesz? Zareaguj i zgłoś tą sytuację pracownikowi Urzędu. Urządzenia mogą być celowo podłożone przez hakera, aby zakłócać lub przechwytywać sygnał wewnętrznej sieci Urzędu. To z kolei może się przyczynić do kradzieży danych osobowych lub naruszeniem integralności wewnętrznych systemów Urzędu, tym samym powodując poważną awarię.

Opracował: Informatyk Urzędu

Wydanie I, 26.02.2026 r.