Sigma Sp. z o.o.
ul. Wojska Polskiego 5/309, 19-400 Olecko
NIP8471613976 | REGON281608399 | KRS0000517689
**tel.** +48 58 880 88 80 | e-mail: hello@sigma.pl

**Zapewnienie dostępu do wiedzy**
Art. 22 ust. 1 pkt 4 UoKSC
wersja 1.0

# 1. Zagrożenia cyberbezpieczeństwa urządzenia końcowego i skuteczne sposoby zabezpieczania się przed tymi zagrożeniami.

## 1.1. Komputer.

Komputer to z definicji urządzenie elektroniczne automatycznie przetwarzające dane zapisane cyfrowo, służące do szybkiego wykonywania obliczeń, przechowywania, porządkowania i wyszukiwania danych oraz sterowania pracą innych urządzeń. W praktyce to jedno z podstawowych urządzeń pozwalających na wykonywanie codziennych zadań służbowych i prywatnych w cyfrowym świecie, np. na odczytywanie niniejszej strony internetowej. Komputer jako urządzenie zbudowane z podzespołów odpowiedzialnych za przetwarzanie informacji (np. procesor) oraz ich przechowywanie (np. dysk twardy, RAM) może pracować w trybie offline (bez dostępu do sieci internet) oraz online (z dostępem do sieci internet). Wyposażony jest najczęściej w dodatkowe urządzenia wejścia (np. mysz, klawiatura) oraz wyjścia (np. monitor, głośniki), które komunikują się z nim za pomocą portów (np. USB, HDMI, Ethernet). Dane, z których korzysta komputer, mogą być przechowywane również na zewnętrznych nośnikach pamięci (np. przenośny dysk twardy, przenośna pamięć masowa USB – tzw. pendrive).

Większość użytkowników komputera potrzebuje do jego obsługi systemu operacyjnego, np. Windows, Linux.

**Zagrożenia:** złośliwe oprogramowanie, które przypadkowo (np. poprzez swoją niedoskonałość) lub celowo (oprogramowanie, którego celem jest wyrządzenie szkody lub szkód w stosunku do komputera, oprogramowania komputerowego lub użytkownika komputera nazywane jest ogólnie jako malware) działa wbrew oczekiwaniom użytkownika. Istnieje wiele rodzajów złośliwego oprogramowania, np. wirusy, robaki, konie trojańskie, backdoory, oprogramowanie szpiegujące, rejestratory klawiszy, rootkity, exploity oraz jedne z najgroźniejszych – ransomware (oprogramowanie blokujące dostęp do danych znajdujących się na komputerze, żądające okupu za przywrócenie możliwości ich odczytu).

Najczęstszym wektorem ataku złośliwego oprogramowania na urządzenie typu komputer to porty komunikacyjne (port USB – np. poprzez umieszczenie w nim przenośnej pamięci masowej oraz port Ethernet – np. poprzez lokalną sieć komputerową lub sieć internet).

Celem niniejszej strony internetowej nie jest działanie w sposób szkodliwy w stosunku do komputera, oprogramowania komputerowego lub użytkownika komputera, natomiast korzystanie z niniejszego serwisu z komputera, który wcześniej uległ infekcji złośliwym oprogramowaniem, może wpływać na niewłaściwe działanie usługi, w tym nielegalne gromadzenie danych o zachowaniach użytkownika przez cyberprzestępców.

**Sposoby zabezpieczania:** oprogramowanie antywirusowe z aktualną bazą sygnatur (sygnatury to swoiste i niepowtarzalne „odciski palca" złośliwych programów, a także inne wpisy pozwalające na wykrywanie złośliwego kodu w celu jego unieszkodliwienia poprzez usunięcie lub umieszczenie w tzw. kwarantannie).

Należy nadmienić w tym miejscu, iż bezpłatne programy antywirusowe mogą zawierać w swoich regulaminach (które zwykle akceptowane są przez użytkowników bez uprzedniego przeczytania ze zrozumieniem) klauzule zezwalające na zbieranie i gromadzenie danych o aktywnościach powiązanych z komputerem objętym ochroną antywirusową. Dodatkowo warto zwrócić uwagę, iż licencje zdecydowanej większości bezpłatnych programów

antywirusowych nie zezwalają na użytkowanie ich w trybie komercyjnym (tzn. przez przedsiębiorstwa oraz inne podmioty niebędące Konsumentami).

Dodatkową i bardzo ważną warstwą zabezpieczenia komputera jest aktualność oprogramowania pracującego w jego środowisku, w tym aktualność systemu operacyjnego. Bardzo często nieaktualne oprogramowanie posiada tzw. podatności pozwalające na przedostanie się złośliwego oprogramowania na komputer ofiary w sposób trudny do wykrycia, w tym bez aktywacji alertu po stronie oprogramowania antywirusowego.

Dodatkową prewencyjną metodą zabezpieczenia komputerów przed infekcją złośliwym oprogramowaniem jest ograniczenie wektorów ataków, np. poprzez techniczne lub organizacyjne wyłączenie możliwości wykorzystywania portów USB do umieszczania w nich przenośnych pamięci masowych.

## 1.2. Urządzenie mobilne (smartfon, tablet).

Urządzenia mobilne to przenośne komputery, które różnią się od klasycznych komputerów gabarytami, przeznaczeniem, architekturą podzespołów oraz systemem operacyjnym, np. Android, iOS, iPadOS. Podstawowe interfejsy komunikacyjne w urządzeniach mobilnych to interfejs przewodowy (np. USB-C odpowiedzialny za ładowanie i transmisję danych) oraz bezprzewodowy (np. LTE, Wi-Fi, Bluetooth).

**Zagrożenia:** potencjalnie pożądane aplikacje zawierające w sobie złośliwy kod (np. adware wyświetlające reklamy) i inne złośliwe oprogramowanie.

Najczęstszym wektorem ataku złośliwego oprogramowania na urządzenie typu smartfon lub tablet to interfejsy komunikacyjne (interfejs USB-C – np. poprzez tzw. Juice Jacking, czyli umieszczenie w nim publicznie dostępnej, zainfekowanej ładowarki oraz interfejs bezprzewodowy – np. poprzez lokalną sieć komputerową, otwarty Bluetooth lub sieć internet).

**Sposoby zabezpieczania:** oprogramowanie antywirusowe z aktualną bazą sygnatur ma rację bytu wyłącznie dla urządzeń typu Android z dozwoloną opcją instalacji aplikacji spoza sklepu Google Play. Oznacza to, że urządzenia mobilne, które mają wyłączoną możliwość instalowania aplikacji spoza oficjalnych źródeł (np. sklep Google Play, AppStore) są zabezpieczone w zakresie instalowanych aplikacji oraz ich aktualizacji (przechodzą one skanowanie antywirusowe wcześniej).

Należy nadmienić w tym miejscu, iż bezpłatne programy antywirusowe mogą zawierać w swoich regulaminach (które zwykle akceptowane są przez użytkowników bez uprzedniego przeczytania ze zrozumieniem) klauzule zezwalające na zbieranie i gromadzenie danych o aktywnościach powiązanych z komputerem objętym ochroną antywirusową. Dodatkowo warto zwrócić uwagę, iż licencje zdecydowanej większości bezpłatnych programów antywirusowych nie zezwalają na użytkowanie ich w trybie komercyjnym (tzn. przez przedsiębiorstwa oraz inne podmioty niebędące Konsumentami).

# 2. Zagrożenia cyberbezpieczeństwa przeglądarki internetowej i skuteczne sposoby zabezpieczania się przed tymi zagrożeniami.

## 2.1. Komunikacja przeglądarki z serwerem strony www.

Przeglądarka internetowa (np. Chrome, Edge, Firefox, Opera, Brave, Vivaldi) służy do komunikacji z serwerem strony www dzięki czemu możliwe jest przeglądanie stron www dostępnych w sieci internet, a także tych dostępnych w ograniczonym środowisku (np. w ramach tzw. intranetu w środowisku służbowym lub w trybie offline po pobraniu strony na swój komputer). Jednym z najważniejszych miejsc w przeglądarce jest pasek adresu, służący do wprowadzania i odczytywania adresu strony www, na której znajdujemy się w danym momencie. Adres strony www nazywany jest skrótem URL. Dla przykładu obecnie znajdujemy się na stronie, której adres URL to **https://bip.gwprzeworno.finn.pl**. Prosimy ze względów bezpieczeństwa o zweryfikowanie czy wskazany adres URL jest zgodny z adresem URL widocznym w pasku adresu oraz czy adres URL widoczny w pasku adresu jest faktycznym celem odwiedzin.

Domyślnie przeglądarki komunikują się z serwerami stron www za pomocą portów określonych numerami 80 (połączenie ze stroną nie jest szyfrowane) lub 443 (połączenie ze stroną jest szyfrowane z wykorzystaniem certyfikatu SSL). To, czy przeglądarka wykorzystuje szyfrowane połączenie z witryną można sprawdzić najczęściej po lewej stronie paska adresu – bezpieczne połączenie szyfrowane ze stroną www komunikowane jest zwykle ikoną „kłódki". Analogicznie połączenie nieszyfrowane będzie zwykle komunikowane przez przeglądarkę ikoną przekreślonej kłódki, a nawet komunikatami o „niezabezpieczonej stronie" lub informacją, że „strona nie jest bezpieczna". Dodatkową wskazówką jest litera „s" w pasku adresu URL, gdzie https oznacza połączenie szyfrowane, a http oznacza połączenie nieszyfrowane.

**Zagrożenia:** fałszywa strona internetowa podszywająca się pod właściwą stronę www. Bardzo często spreparowana strona internetowa łudząco przypomina oryginalną stronę www.

Jednym z najwiekszych zagrożeń w cyberprzestrzeni jest tzw. phishing. Ta przebiegła metoda opierająca się o psychologiczne mechanizmy zwane socjotechnikami, wykorzystywana jest przez cyberprzestępców do wyłudzania informacji (np. loginów i haseł) lub nakłaniania użytkowników do zachowań pozwalającym im osiągnąć założony cel.

Innym zagrożeniem cyberbezpieczeństwa w komunikacji przeglądarki z serwerem strony www są ataki o nazwie Man in The Middle (z ang. człowiek po środku, dalej MiTM). W celu przeprowadzenia takiego ataku cyberprzestępca musi sprawić, by pakiety danych służące do komunikacji pomiędzy przeglądarką internetową a serwerem strony www zaczęły przechodzić przez jego urządzenie (np. komputer, serwer). Jest to możliwe poprzez skompromitowanie dowolnego urządzenia na drodze tej komunikacji (np. routera wi-fi, z którego korzysta komputer, na którym zainstalowana jest przegladarka internetowa lub serwera strony www).

**Sposoby zabezpieczania:** weryfikacja adresu URL odwiedzanej strony internetowej (cyberprzestępcy mogą zakupić domenę internetową łudząco przypominającą oryginalną stronę www). W celu uwierzytelnienia prawidlowosci adresu URL odwiedzanej strony, można wykorzystać jedną z poniższych metod:

1) kontakt z nami drogą telefoniczną pod nr +48 74 810 20 52 lub odwiedzenie naszej organizacji osobiście;
2) wyszukanie naszego adresu URL za pomocą co najmniej dwóch rocznych wyszukiwarek (np. Google, Bing), jednak należy mieć na uwadze, iż znane są przypadki wykupowania reklam przez cyberprzestępców w celu umieszczenia spreparowanej strony www w górnych wynikach wyszukiwania (w takim przypadku wynik wyszukiwania oznaczony jest słowem „Reklama" lub „Ad") – informujemy, że nasza organizacja nie kupuje tego typu reklam;
3) weryfikacja właściciela odwiedzanej witryny w bazie WHOIS, np. pod adresem https://dns.pl/whois/.

W celu zabezpieczenia przeglądarki przed atakami typu MiTM, należy zwrócić szczególną uwagę na to, czy komunikacja z serwerem strony www jest szyfrowana. Ataki typu MiTM wykorzystują nieuwagę użytkowników próbując wyłączyć szyfrowanie w komunikacji przeglądarki z serwerem strony www. Cyberprzestępcy najczęściej nie będą w stanie przechwycić informacji, gdy szyfrowanie komunikacji jest aktywne.

Informujemy, iż nasza strona internetowa wykorzystuje szyfrowanie SSL.

## 2.2. Wprowadzanie danych na stronie www (formularze, panele logowania).

Cyberbezpieczeństwo wprowadzanych danych na stronie www (np. w dostępnych na stronie formularzach i panelach logowania) związane jest przede wszystkim z bezpieczeństwem komunikacji (szyfrowanie), opisanym w punkcie poprzednim.

**Zagrożenia:** przechwycenie danych wprowadzanych na stronie www przez cyberprzestępców (np. z wykorzystaniem ataków typu MiTM lub poprzez spreparowaną stronę www).

**Sposoby zabezpieczania:** weryfikacja bezpieczeństwa komunikacji poprzez sprawdzenie poprawności adresu URL oraz – jeśli adres jest poprawny w 100% – weryfikacja poprawności szyfrowania (https, ikona kłódki).