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@esigma.pl

Zapewnienie dostępu do wiedzy

Art. 22 ust. 1 pkt 4 UoKSC

wersja 1.3

Spis treści

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://gminaterespol.pl/. Prosimy ze względów bezpieczeństwa o bardzo dokładne 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 pozwalających im osiągać 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 prawidłowości adresu URL odwiedzanej strony, można wykorzystać jedną z poniższych metod:

1) kontakt z nami drogą telefoniczną pod nr 83 411 20 00 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).

2.3. Wersja przeglądarki internetowej.

Producenci przeglądarek internetowych stale rozwijają swoje oprogramowanie – zarówno w aspekcie funkcjonalnym, jak i w zakresie cyberbezpieczeństwa. Każda aktualizacja przeglądarki jest ważna, ponieważ niektóre z nich zawierają tzw. „łatki bezpieczeństwa", czyli usprawnienia kodu aplikacji przeglądarek będące odpowiedzią na wykryte podatności, pozwalające na ich kompromitację.

Zagrożenia: kompromitacja przeglądarki spowodowana nieaktualnym oprogramowaniem (pozwalająca np. na kradzież haseł, wyświetlanie spreparowanych stron – w tym reklamowych, śledzenie użytkownika itp.).

Sposoby zabezpieczania: weryfikacja aktualnej wersji przeglądarki oraz włączenie automatycznych aktualizacji przeglądarki.

2.4. Wtyczki i rozszerzenia do przeglądarek internetowych.

Przeglądarki internetowe mogą być wyposażone w dodatkowe funkcjonalności (dodatkowy kod aplikacji) dzięki zastosowaniu tzw. wtyczek lub rozszerzeń. Podobnie jak wszystkie aplikacje, rozszerzenia do przeglądarek również mogą zawierać własne podatności. Oznacza to, że pomimo aktualnej wersji przeglądarki, może być ona podatna na ataki z wykorzystaniem podatności występujących w rozszerzeniach do niej doinstalowanych.

Zagrożenia: kompromitacja przeglądarki spowodowana podatnościami występującymi w rozszerzeniach do przeglądarek internetowych (pozwalająca np. na kradzież haseł, wyświetlanie spreparowanych stron – w tym reklamowych, śledzenie użytkownika itp.).

Sposoby zabezpieczania: unikanie instalowania rozszerzeń do przeglądarek lub rozważne ich używanie (np. w ograniczonej ilości i w momencie ich faktycznego wykorzystywania oraz poprzez selekcję wtyczek, zwracając uwagę na reputację dostawcy, a także częstotliwość wydawania aktualizacji).

2.5. Obsługa hiperłączy i przycisków na stronie www.

Hiperłącze (link), które można spotkać na niemal każdej stronie internetowej, to z definicji odwołanie do innej strony internetowej lub podstrony w ramach obecnie przeglądanej strony internetowej (pod pojęciem odwołania kryje się najczęściej inny adres URL niż aktualnie przeglądany). Uaktywnienie hiperłącza może nastąpić poprzez

kliknięcie lub najechanie kursorem na element, który nazywany jest czasem kotwicą. Powoduje to wyświetlenie docelowej informacji.

Przykładowe hiperłącze prowadzące do podstrony w ramach obecnie przeglądanej strony www: Polityka prywatności (warto zwrócić uwagę na faktyczny adres URL kryjący się pod tym hiperłączem poprzez najechanie kursorem – adres URL powinien pojawić się na dole przeglądarki).

Przykładowe hiperłącze prowadzące do zewnętrznej strony: sigma (ponownie warto zwrócić uwagę na faktyczny adres URL kryjący się pod tym hiperłączem poprzez najechanie kursorem – adres URL powinien pojawić się na dole przeglądarki).

[PRZYCISK] to również hiperłącze, ale przedstawione w nieco innej formie, którą tworzyć może sam tekst, tekst z obrazem, tekst z specjalnym kodem interpretowanym przez przeglądarkę jako kształt (np. prostokąt z ostrymi lub zaokrąglonymi rogami) lub sam obraz. Zaprezentowany dla przykładu przycisk nie prowadzi do żadnej strony, pomimo że posiada odwołanie – zastosowany znak # zmusza przeglądarkę do pozostania na niniejszej stronie (ponownie warto zwrócić uwagę na faktyczny adres URL kryjący się pod tym hiperłączem poprzez najechanie kursorem – adres URL powinien pojawić się na dole przeglądarki).

Zagrożenia: kompromitacja adresu URL i umieszczenie fałszywego odwołania, które może prowadzić do spreparowanej strony www, będącej częścią tzw. kampanii phishingowej (próba wyłudzenia/kradzieży informacji w celu zainfekowania komputera lub doprowadzenie do kradzieży środków finansowych znajdujący się na kontach użytkowników) oraz może doprowadzić do infekcji podatnej przeglądarki internetowej (np. poprzez wykonanie szybkich „przeskoków" przez kilka lub więcej stron internetowych próbujących wstrzyknąć złośliwy kod)

Sposoby zabezpieczania: weryfikacja poprawności linków przed ich kliknięciem (zwracając uwagę na faktyczny adres URL kryjący się pod hiperłączem).

2.6. Tokeny, trackery (narzędzia śledzące firm trzecich), cookies (tzw. ciasteczka) i tryb prywatny (incognito).

Tokeny do specjalne klucze składające się z ciągu znaków, doklejane do adresów URL np. po zalogowaniu się do panelu użytkownika. Pozwalają one aplikacjom wierzyć (uwierzytelniać), że poruszający się po aplikacji użytkownik jest stale tą samą osobą. Najczęściej token nie jest jedynym elementem uwierzytelniającym użytkownika podczas wykorzystywania aplikacji. Dodatkowymi elementami mogą być np. fingerprint (odcisk palca) przeglądarki, adres IP użytkownika odwiedzającego stronę www, a nawet zachowanie (np. w celu blokowania zewnętrznych skryptów, tzw. botów).

Fingerprint przeglądarki składa się najczęściej z takich danych jak: system operacyjny użytkownika, typ przeglądarki oraz jej wersja, język, w którym strona jest wyświetlana. Jeżeli przeglądarka ma włączoną obsługę JavaScript (większość przeglądarek posiada domyślnie włączoną obsługę JavaScript), strona www może być wyposażona w skrypt zbierający dodatkowe informacje, np.: strefę czasową, listę zainstalowanych dodatków w przeglądarce, rozdzielczość ekranu, na którym strona www jest przeglądana, wykorzystywaną kartę graficzną, zakres oraz szybkość tworzenia grafiki w przeglądarce.

Trackery pozwalają pewnym firmom śledzić aktywność użytkowników na zewnętrznych stronach.

Zagrożenia: kompromitacja przeglądarki spowodowana podatnościami występującymi w rozszerzeniach do przeglądarek internetowych (pozwalająca np. na kradzież haseł, wyświetlanie spreparowanych stron – w tym reklamowych, śledzenie użytkownika itp.).

Sposoby zabezpieczania: unikanie instalowania rozszerzeń do przeglądarek lub rozważne ich używanie (np. w ograniczonej ilości i w momencie ich faktycznego wykorzystywania oraz poprzez selekcję wtyczek, zwracając uwagę na reputację dostawcy, a także częstotliwość wydawania aktualizacji).

2.7. Dodatkowe narzędzia pozwalające na zrozumienie zagrożeń cyberbezpieczeństwa.

Warto wiedzieć, że istnieją dodatkowe narzędzia, pozwalające na weryfikację konkretnych stron internetowych, a także własnych kont w różnych serwisach internetowych.

VirusTotal to serwis, w którym istnieje możliwość weryfikacji podejrzanych plików [FILE] oraz stron internetowych [URL] - https://www.virustotal.com/

Baza WHOIS w ramach Krajowego Rejestru Domen NASK pozwala na weryfikację właściciela strony internetowej poprzez wpisanie adresu domeny .pl (np. domena.pl) - https://dns.pl/whois

Have I Been Pwned to serwis pozwalający na sprawdzenie czy posiadany przez nas adres e-mail lub numer telefonu nie był przedmiotem wycieku danych (np. w zakresie wykorzystywanego hasła) - jest to szczególnie ważne, jeżeli ktoś używa tego samego hasła w wielu serwisach - https://haveibeenpwned.com/

3. Zagrożenia cyberbezpieczeństwa w zakresie komunikacji elektronicznej i skuteczne sposoby zabezpieczania się przed tymi zagrożeniami.

3.1. Komunikacja z wykorzystaniem wiadomości e-mail oraz phishing.

W ramach komunikacji elektronicznej z naszym podmiotem dostępna jest droga mailowa (poczta elektroniczna). Usługa e-mail pozwala zarówno na wysyłanie, jak i odbieranie poczty elektronicznej. Sam adres e-mail składa się z identyfikatora, znaku „@„ (tzw. „małpa”) oraz domeny, w ramach której utrzymywany jest adres e-mail.

Przykładowy adres e-mail to *identyfikator@domena.pl*.

Phishing to przebiegła metoda wykorzystywana przez cyberprzestępców w celu nakłaniania ofiar do ujawnienia informacji poufnych, takich jak loginy, hasła lub numery kart bankowych, kont bankowych itp. Robią to poprzez wysyłanie fałszywych e-maili lub przekierowywanie na fałszywe strony.

Zagrożenia: istnieją możliwości podszycia się pod dowolny (w tym nasz) adres e-mail w komunikacji elektronicznej (np. poprzez wykorzystanie łudząco podobnego adresu e-mail lub poprzez wykorzystanie dowolnej nazwy lub dowolnego imienia i nazwiska) w celu przeprowadzenia ataku typu phishing.

Sposoby zabezpieczania: zachowanie zasady ograniczonego zaufania w komunikacji drogą elektroniczną, dokładna weryfikacja nazwy nadawcy w komunikacji elektronicznej, a w przypadku pojawienia się wątpliwości, kontakt telefoniczny lub osobisty w celu uwierzytelnienia otrzymanej wiadomości; nie klikanie w odnośniki w wiadomościach e-mail, nie instalowanie żadnego sugerowanego oprogramowania i nie ujawnianie żadnych danych

osobowych, identyfikatorów, haseł itp. - żadna instytucja nigdy nie powinna prosić o podanie w wiadomości e-mail danych osobowych.

Przykładowo urzędy administracji publicznej, szpitale itp. nigdy nie proszą przy pomocy SMS czy maili o dopłatę do szczepionki, uregulowanie należności podatkowych lub dopłatę do mandatu.

3.2. Komunikacja z wykorzystaniem tradycyjnej telefonii, wiadomości SMS oraz spoofing.

W ramach komunikacji elektronicznej z naszym podmiotem dostępna jest droga telefoniczna.

Zagrożenia: istnieją metody podszywania się pod dowolny numer telefoniczny, w tym numer naszego podmiotu (spoofing rozmowy telefonicznej oraz wiadomości SMS); możliwe jest również podszywanie się pod dowolną osobę, przez dowolną osobę, z dowolnego numeru telefonu.

Sposoby zabezpieczania: zachowanie zasady ograniczonego zaufania w komunikacji drogą elektroniczną, a w przypadku pojawienia się wątpliwości, kontakt telefoniczny lub osobisty w celu uwierzytelnienia otrzymanego telefonu, nie instalowanie żadnego sugerowanego oprogramowania i nie ujawnianie żadnych danych osobowych, identyfikatorów, haseł itp.

4. Zagrożenia cyberbezpieczeństwa w zakresie zarządzania hasłami i skuteczne sposoby zabezpieczania się przed tymi zagrożeniami.

4.1. Pojęcie mocnego hasła.

W celu rozstrzygnięcia kwestii mocnego hasła, warto zajrzeć do standardów opisanych w wytycznych jednej z amerykańskich agencji federalnych – NIST (National Institute of Standards and Technology) a dokładniej zawartych w dokumencie – „NIST 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management” (oficjalny link: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf).

- Hasło powinno zawierać od 8 do 64 znaków.
- Zaleca się, by hasło składało się z drukowalnych znaków ASCII (95 znaków drukowalnych: !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~), a także – o ile jest to możliwe - znaków UNICODE (standard kodowania obejmujący litery większości używanych na świecie pism, a także symboli, emoji i kodów formatowania).
- Hasła nie należy zmieniać – powinno być stałe i niezmienne aż do skompromitowania.
- Hasło powinno przed zastosowaniem być zweryfikowane jako nieskompromitowane (np. tu: https://haveibeenpwned.com/Passwords).
- Należy pomijać wskazówki – i o ile jest to możliwe – i pytania zabezpieczające hasło.

Zagrożenia: słabe hasło może zostać odgadnięte lub złamane z wykorzystaniem techniki Brute Force (metoda ataku, w której atakujący używają oprogramowania do „wypróbowania” wielu różnych kombinacji w krótkim czasie w celu skompromitowania hasła).

Sposoby zabezpieczania: stosowanie mocnych haseł.

Wskazówka: można wypracować własną metodę wytwarzania haseł dla różnych serwisów, np. poprzez skojarzenie przedmiotu z daną witryną i dodanie krótkiej historii: KSIĄŻKA-leży-NA-biurku-0248. Wskazane hasło zawiera zarówno małe, jak i duże litery, posiada znaki specjalne z drukowalnych znaków ASCII oraz znaki UNICODE (polskie znaki), dodatkowo składa się aż z 28 znaków i nie zostało skompromitowane w żadnym wycieku danych.

4.2. Stosowanie różnych haseł.

Mocne hasło powinno być przede wszystkim unikalne. Oznacza to, że zalecane jest wykorzystywanie różnych haseł w różnych usługach i nie powielanie ich nawet w niepełnym zakresie (np. poprzez zmianę cyfry na końcu).

Zagrożenia: stosując te same hasła w różnych usługach narażamy się na kompromitację wszystkich usług jeżeli dojdzie do wycieku danych z jednej z nich. Skompromitowane konta (np. konta e-mail oraz konta serwisów społecznościowych) mogą zostać wykorzystane do nadużyć, np. do podszywania się pod skompromitowaną osobę w relacjach z innymi osobami fizycznymi lub prawnymi, w tym w relacjach z naszym podmiotem.

Sposoby zabezpieczania: stosowanie różnych haseł w różnych usługach.

4.3. Narzędzia wspomagające przechowywanie i generowanie (mocnych) haseł.

Istnieją narzędzia wspomagające zarówno przechowywanie, jak i generowanie mocnych haseł. Są to tzw. menedżery haseł. Dostępne są na rynku płatne rozwiązania (w których baza haseł najczęściej przechowywana jest przez usługodawcę), jak i bezpłatne (w których baza haseł najczęściej przechowywana jest przez użytkownika, np. w ramach usługi chmurowej).

Wskazówka: jednym z bardzo popularnych bezpłatnych menedżerów haseł jest aplikacja KeePass, pozwalająca na generowanie i przechowywanie haseł w zaszyfrowanej bazie danych, dostępnej po wprowadzeniu zapamiętanego mocnego hasła oraz – jeśli zostanie to skonfigurowane – dodatkowego klucza w postaci wygenerowanego pliku. Aktualną wersję aplikacji KeePass można znaleźć na stronie twórcy: https://keepass.info/download.html.

4.4. Dodatkowe składniki uwierzytelniania wspomagające ochronę tożsamości (silne uwierzytelnianie).

Klasyczne uwierzytelnianie użytkownika wymaga podania loginu i hasła. W przypadku przejęcia obu składników logowania, cyberprzestępca uzyskuje dostęp do celu, np. konta e-mail lub konta społecznościowego.

Silne uwierzytelnianie pozwala uniknąć włamania, gdyż atakujący nie posiada dodatkowego składnika logowania, np. telefonu, na którym wyświetlony zostaje unikalny kod o określonej żywotności działania (np. 30 sekund).

Przykładowe metody dystrybucji dodatkowego składnika uwierzytelniania:

- kod przesyłany poprzez wiadomość e-mail lub sms;
- kod wyświetlany w ramach tzw. tokenu sprzętowego lub aplikacji mobilnej (np. Google Authenticator, Microsoft Authenticator).