Tom 35/2022, ss. 189-214
ISSN 2719-4175
e-ISSN 2719-5368
DOI: 10.19251/ne/2022.35(11)
www.ne.mazowiecka.edu.pl

Paweł Sajler-Fudro
e-mail: pawel@sajler.com
Szkoła Główna Handlowa w Warszawie
ORCID ID: https://orcid.org/0000-0002-2468-4422

ZAGROŻENIA BEZPIECZEŃSTWA W UŻYTKOWANIU SYSTEMÓW INFORMATYCZNYCH – KLASYFIKACJA I METODY ZAPOBIEGANIA

SAFETY THREATS IN THE USE OF IT SYSTEMS – CLASSIFICATION AND PREVENTION METHODS

Streszczenie

Celem opracowania jest ocena znaczenia zagrożeń związanych z bezpieczeństwem informatycznym oraz wskazanie na możliwości zabezpieczania się. Właściwe użytkowanie systemów informatycznych jest fundamentalne dla zapewnienia ich bezpieczeństwa. Wśród wielu czynników wymienianych jako istotne dla bezpieczeństwa systemów informatycznych pojawia się tzw. czynnik ludzki. Sposób korzystania z systemu przez użytkowników, determinuje jego bezpieczeństwo

Summary

The purpose of this paper is to assess the importance of IT security risks, and to point out possibilities for protection. The proper use of information systems is fundamental to their security. Among many factors mentioned as important for the security of IT systems there is the so-called human factor. The way the system is used by users determines its security and guarantees confidentiality, availability and integrity of data. The study presents reports on IT

oraz gwarantuje poufność, dostępność i spójność danych. W opracowaniu przedstawiono raporty prezentujące wydatki na bezpieczeństwo IT w organizacjach oraz stosunek Europejczyków do bezpieczeństwa w internecie. Podjęto próbę usystematyzowania użytkownikowi, przyczyn i zagrożeń, w wyniku których może dojść do nieuprawnionej ingerencji w systemy IT, wraz z wskazaniem sposobu radzenia sobie z nimi przy wykorzystaniu aktualnej wiedzy i doświadczeń. Podkreślono również rolę systematycznych szkoleń dla wyeliminowania pomyłek ludzkich oraz poprawy bezpieczeństwa użytkowników korzystających z systemów informatycznych.

Słowa kluczowe: zagrożenia systemów informatycznych, bezpieczeństwo systemów informatycznych, cyberbezpieczeństwo, cyfryzacja, bezpieczeństwo informacji, bezpieczeństwo użytkowników internetu

Kody klasyfikacji JEL: C81, C82, C83, G28, O33, O38

security spending in organizations and the attitude of Europeans to online security. It attempts to systematize the user, the causes and threats resulting in unauthorized interference with IT systems, together with an indication of how to deal with them using current knowledge and experience. The role of systematic training to eliminate human error and to improve the safety of users using IT systems was also emphasised.

Keywords: threats to information systems, security of information systems, cyber security, digitalization, information security, Internet users' security

WPROWADZENIE

Pierwszy raz, po zakończeniu drugiej wojny światowej, stajemy w obliczu poważnego konfliktu zbrojnego w Europie. Konflikt między Rosją dysponującą drugą pod względem wielkości armią świata (Global Firepower 2020), a Ukrainą – zmienia oblicze postrzegania bezpieczeństwa. Stany Zjednoczone, Unia Europejska oraz państwa reprezentujące wartości demokratyczne w obliczu zagrożenia suwerenności Ukrainy zareagowały sankcjami wobec Rosji. Wśród propozycji reakcji znalazł się również zmasowany cyberatak na infrastrukturę Rosji (NBS News, 2022). Coraz częściej opinia publiczna dowiaduje się o działaniach w przestrzeni świata cyfrowego, polegających na kradzieży danych, utracie ich spójności, próbach szyfrowania dla okupu (ransomware) (Krawiec, 2019, str. 52), czy atakach na instytucje rządowe, jednak sytuacja, w której cyberatak traktowany jest na równi z działaniami militarnymi wobec agresora, w tak poważnym konflikcie jest bezprecedensowa. Wskazuje również jak

istotny jest aspekt bezpieczeństwa użytkowników korzystających z produktów w sieci internetowej. Wbrew pobieżnemu poglądowi o braku istotności zwykłego użytkownika internetu na działania skierowane przeciw państwom, organizacjom, bankom czy korporacjom, należy podkreślić, że w wielu przypadkach ataki wykorzystują skradzioną tożsamość, zatem istnieje realna potrzeba ochrony pojedynczych użytkowników w sieci internetowej. Tak pojmowana ochrona przejawia się nie tylko w trosce administratorów i specjalistów ds. bezpieczeństwa, ale również sprowadza się do przestrzegania przez użytkowników zasad bezpiecznego korzystania z usług oferowanych w sieci. Celem opracowania jest ocena znaczenia zagrożeń związanych z bezpieczeństwem informatycznym oraz wskazanie na możliwości zabezpieczania się.

Aktualnie dużo pisze się na temat bezpieczeństwa systemów IT. W prasie można spotkać wiele artykułów traktujących o zagadnieniu bezpieczeństwa IT, w bankach, firmach masowo przetwarzających dane swoich klientów, organizacjach. Również prezentowana skala i wielkość kradzieży danych obrazuje czytelnikowi znaczenie bezpieczeństwa. Jest to temat interesujący, ponieważ wciąż wiele osób nie rozumie co i w jaki sposób może stać się po podłączeniu komputera do sieci. Z innej perspektywy wiadomo, że możliwe jest podejmowanie aktywności, których przykładem jest działanie administratorów czy pracowników działów IT, którzy zdalnie potrafią połączyć się z komputerem i wykonać na nim dowolną operację. Niemal każdego dnia pojawiają się informacje o kradzieży danych, szyfrowaniu komputerów, czy żądaniach okupu w zamian za udostępnienie oprogramowania, które je odszyfruje. Cennych danych przechowywanych w pamięci systemów nie można przenieść w bezpieczne miejsce, ponieważ niemożliwe będzie korzystanie z nich na bieżąco, a takie zastosowanie i ciągła aktualizacji świadczą o ich wadze i wartości. O istotności zagadnienia świadczy wysokość planowanych nakładów na ochronę przed atakami. Firma analityczno-badawcza Gartner w sierpniu 2018 roku opublikowała informacje o światowych wydatkach na bezpieczeństwo IT w organizacjach (Gartner, 2018). Dane podzielone na segmenty rynku, pokazują wzrost z roku do roku nakładów, które według szacunków do 2022 roku na świecie osiągną kwotę 134 bilionów dolarów.

Tabela1. Światowe wydatki na bezpieczeństwo w rozbiciu na segmenty (mln USD).

Segment rynku	2017	2018	2019
Bezpieczeństwo aplikacji	2,434	2,742	3,003
Bezpieczeństwo „chmury"	185	304	459
Bezpieczeństwo danych	2,563	3,063	3,524
Bezpieczeństwo identyfikacji w związku z dostępem	8,823	9,768	10,578
Bezpieczeństwo infrastruktury	12,583	14,106	15,337
Integracja Zarządzania Ryzykiem	3,949	4,347	4,712
Sprzęt do ochrony sieci	10,911	12,427	13,321
Pozostałem programy informacyjne związane z bezpieczeństwem	1,832	2,079	2,285
Usługi ochrony	52,315	58,920	64,237
Oprogramowanie chroniące użytkowników	5,948	6,395	6,661
RAZEM:	**101,544**	**114,152**	**124,116**

Źródło: Gartner (2018)

1. ZAGROŻENIA I SPOSOBY ATAKÓW CYBEROSZUSTÓW

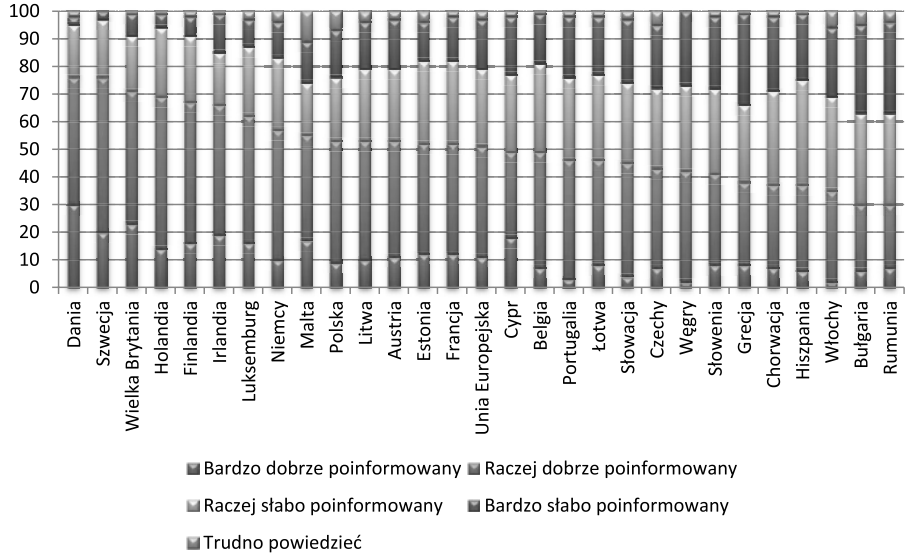
Aby lepiej zrozumieć przyczyny występowania zagrożeń, warto krótko zapoznać się z ich definicją oraz klasyfikacją. Zagrożenie z perspektywy systemu informatycznego można zdefiniować jako pewne zdarzenie, które może naruszyć integralność systemu powodując jego zniszczenie lub straty. Najczęściej spotykane w literaturze podziały zagrożeń mają charakter ogólny i są klasyfikowane z uwagi na czynnik wywołujący lub lokalizację. W ten sposób zagrożenia dzielimy na:

- wywołane przez czynnik ludzki lub programy komputerowe,
- związane z fizycznym bezpieczeństwem systemu,
- zagrożenia z tłem politycznym,
- zewnętrzne i wewnętrzne,
- aktywne i pasywne.

Zagrożenia związane z czynnikiem ludzkim stanowią najobszerniejszą i najczęściej spotykaną grupę identyfikowanych zagrożeń systemów informatycznych. Wewnątrz nich wprowadza się podział na zagrożenia umyślne (atak, włamanie, kradzież), oraz nieumyślne (spowodowane brakiem wiedzy i umiejętności użytkownika systemu).

Według raportu Związku Banków Polskich opublikowanego w styczniu 2020 r., 40 % Polaków deklaruje, że jest słabo poinformowanych na temat ryzyka cyberprzestępstw w sieci (Związek Banków Polskich, 2020, str. 13). Polska pod tym względem wypada nieznacznie powyżej średniej unijnej. Najwyżej

swoją świadomość bezpieczeństwa w internecie oceniają Duńczycy i Szwedzi oraz Brytyjczycy, najgorzej wypada ona w Bułgarii i Rumunii.



Wykres 1.Stosunek Europejczyków do bezpieczeństwa w internecie, Komisja Europejska, 2019

Źródło: Związek Banków Polskich (2020)

Świadomość zagrożeń bezpieczeństwa w sieci, jest fundamentalnym elementem zapobiegającym zagrożeniom wywoływanym przez użytkowników. Jak widać z powyższych danych pomimo faktu, że Polacy znajdują się powyżej średniej unijnej z deklaracją 53 % łącznie bardzo dobrze i dobrze poinformowanych, to i tak oznacza to że co drugi użytkownik nie posiada wystarczającego zasobu informacji dotyczących bezpieczeństwa, a to naraża go na zagrożenia płynące z sieci.

Według Barometru cyberbezpieczeństwa opublikowanego przez KPMG (KPMG, 2019, str. 14), czynnik ludzki jest największym wyzwaniem dla firm (63 %) w zapewnieniu oczekiwanego poziomu zabezpieczeń, a brak wykwalifikowanej kadry jest większym problemem niż zbyt mały budżet (61 %).

Do najczęściej identyfikowanych zagrożeń nieumyślnych zaliczamy:

- przekazanie uprawnień dostępu,
- niezmienianie lub słabą „siłę" hasła,
- przebywanie w miejscach w których umożliwiona jest rejestracja haseł dostępowych do systemu,

- niestosowanie się do zasad bezpieczeństwa np. kontroli dostępu w budynkach.

Z nieumyślnym przekazaniem uprawnień mamy do czynienia na przykład w sytuacji, gdy użytkownik odpisze na specjalnie spreparowany mail który do złudzenia przypomina korespondencję z zaufanej instytucji lub jednostki, np. banku, działu IT w którym proszony jest o autoryzację za pomocą loginu i hasła. Podobna sytuacja ma miejsce w przypadku, gdy użytkownik skorzysta z linku zachęcany do kliknięcia w niego przez podobnie spreparowany mail. Najczęściej link przekierowuje go do specjalnie przygotowanej strony internetowej, do złudzenia przypominającej oryginał i w taki sposób użytkownik dokonuje logowania do systemu, nieświadomy tego, że właśnie przekazał swoje dane do włamywaczy.

Innym sposobem na wyłudzanie haseł np. do portali społecznościowych jest zamazywanie tła zdjęcia, które próbuje wyświetlić użytkownik z jednoczesną informacją, że pełny obraz zostanie wyświetlony po zalogowaniu (kliknięciu w umieszczony w komunikacie dla ułatwienia przycisk), ponieważ treść jest przeznaczona dla pełnoletnich użytkowników. Z pozoru prosty sposób do rozszyfrowania, jednak taką metodą ofiarami cyberprzestępców padli użytkownicy portalu Instagram. Ich konta posłużyły następnie do logowania w innych aplikacjach, dopuszczających taki sposób uwierzytelnienia użytkownika. Analizując konta znajomych ofiary w portalu haker przystępował do kolejnej fazy ataku – zidentyfikowania współpracowników. Następnie stosując wyrafinowane socjotechniki uzyskiwał od niczego nie podejrzewającej osoby (identyfikował się jako znajomy korzystając z komunikatora internetowego portalu) login i hasło do konta firmowego - przystępując do zasadniczej części ataku. Często w mediach społecznościowych hakerzy podszywają się pod ekspertów, rekruterów, ankieterów lub osoby potencjalne zainteresowane ofertą firmy. W taki sposób uwiarygadniając się, próbują uzyskać informacje dotyczące organizacji, w której pracuje ofiara. Następnie poprzez kolejne ”krzyżowe kontakty” osiągają kolejne poziomy wiarygodności, przekazując zestaw specyficznych informacji, tak aby na końcu uzyskać dostęp do tożsamości firmowej (loginu i hasła) nieświadomej ofiary.

Spotykaną na dużą skalę metodą jest podszywanie się pod instytucje rządowe. Taki sposób przyjęli oszuści korzystający z pandemii koronawirusa COVID-19, podszywając się pod Ministerstwo Zdrowia. W spreparowanych wiadomościach SMS zawarta jest informacja, że po zalogowaniu się do przesłanego w SMS linku, prowadzącego da bankowości internetowej możliwe jest

sprawdzenie wariantów dostępnej pomocy od Państwa. Znane są również ataki, w których oszuści z zachęcający do inwestycji na rynku FOREX, informowali użytkowników o konieczności zainstalowania aplikacji, z pomocą której, możliwa będzie szybka analiza i podejmowanie decyzji związanych z inwestycjami. Aplikacja okazywała się jednak być programem udostępniającym pulpit komputera użytkownika. W ten sposób przestępcy mogli obserwować czynności wykonywane przez użytkownika na jego komputerze, odczytując loginy i hasła do jego kont. Przykładem innego scenariusza jest atak pishingowy[1], w którym oszuści spreparowali zachętę do skorzystania z tarczy antykryzysowej i pozyskania do 10000 zł. SMS prowadzi do fałszywej bramki płatności i pod pozorem weryfikacji wyłudzane są tam dane dotyczące ID klienta, hasła, nazwiska panieńskiego matki oraz numeru PESEL. Takie dane wystarczają do przejęcia konta bankowości elektronicznej i resetu w nim hasła. Następnie użytkownik może zrealizować wszystkie możliwe scenariusze, wynikające z funkcjonalności konta (NestBank, 2020).

2. UWIERZYTELNIANIE, HASŁA ORAZ SPOSOBY ATAKÓW NA HASŁA

Według badań Związku Banków Polskich oraz Centrum Prawa Bankowego i Informacji, prowadzony w grudniu 2019 roku, 49 % Polaków zmieniło hasło do bankowości internetowej w ciągu ostatnich 12 miesięcy, 11 % nie pamięta tego faktu, 2 % grupy respondentów nie korzysta z bankowości internetowej, a 38 % nie zmieniło hasła na przestrzeni roku. Podobnie sytuacja wygląda w przypadku bakowości mobilnej, gdzie 39% Polaków zmieniło hasło w ciągu ostatniego roku, 20% nie korzysta z bankowości mobilnej, 7% nie pamięta tego faktu, a 34% nie zmieniło hasła (Związek Banków Polskich, 2020, strony 10-11). Wielu użytkownikom wydawać się może, że kryteria bezpieczeństwa stosowane w polityce haseł są zbyt restrykcyjne. Wymaganie zmian w określonym, stosunkowo krótkim czasie, stosowanie wymagań co do zawartości hasła (duże, małe litery, znaki specjalne, brak możliwości użycia charakterystycznych słów takich jak imiona, dni tygodnia, nazwy miesięcy etc.), wszystko to powoduje często irytację. Wynika ona z faktu, że w codziennych obowiązkach coraz częściej sięga się do zabezpieczonych narzędzi internetowych, a to gene-

[1] Phishing to wysyłanie szkodliwych wiadomości, udających pochodzące z zaufanych źródeł. Cele ataku phishingowego to:
- dostarczenie złośliwego oprogramowania do komputera użytkownika,
- wyłudzenie danych do uwierzytelniania,
- zdobycie informacji potrzebnych do przeprowadzenia innego ataku. (Nadnagy, 2020, str. 251)

ruje potrzebę posiadanie hasła tak aby możliwe było korzystanie np. z internetowego dostępu do konta bankowego, dostępu do profilu zaufanego podczas załatwiania spraw urzędowych, logowania do aplikacji rozliczeniowych telefonii, telewizji itp., korzystania z portali społecznościowych, programów pocztowych. Aby zrozumieć lepiej ideę i wymagania stawiane jakości haseł, należy dokładnie przeanalizować rolę, jaką pełnią one w zabezpieczeniu kont użytkownika oraz narzędzi internetowych. Podczas tzw. logowania do aplikacji, konta bankowego, portalu internetowego, wpisanie poprawnego loginu i hasła uwierzytelnia użytkownika, czyli potwierdza, że osoba lub aplikacja (w świecie wirtualnym występują również automatyczne akcje podejmowane przez systemy komputerowe, które również podlegają uwierzytelnieniu w środowiskach aplikacji, które np. udostępniają usługi) jest faktycznie tym za kogo się podaje. Mówimy wówczas o uwierzytelnieniu użytkownika. Aby uwierzytelnienie było wiarygodne, bo przecież w świecie wirtualnym użytkownik nie pojawia się bezpośrednio w celu potwierdzenia swojej tożsamości, należy zastosować reguły, które konsekwentnie to umożliwią.

Spośród najczęściej spotykanych metod uwierzytelniania wyróżniamy metody oparte na hasłach, oparte o tzw. żetony, zdalne uwierzytelnianie użytkownika, uwierzytelnianie dwuskładnikowe i biometryczne. System haseł jest najpowszechniej stosowanym systemem uwierzytelniania. System komputerowy po wprowadzeniu przez użytkownika hasła, porównuje hasło do tego które zostało wcześniej zdefiniowane przez użytkownika posługującego się identyfikatorem (ID). Porównanie dotyczy zatem pary identyfikator – hasło, zdefiniowane w bazie haseł systemu. Pozytywna weryfikacja hasła z pary, oznacza uwierzytelnienie identyfikatora. Do identyfikatora najczęściej przypisane są uprawnienia użytkownika, zatem poprawne uwierzytelnienie decyduje, czy użytkownik ma prawo wstępu do aplikacji systemu. Często pojęcie uwierzytelniania jest mylone z pojęciem autoryzacji. Autoryzacja to potwierdzenie, że użytkownik posiada uprawienia do wykonywania określonej czynności w systemie (Gospodarowicz, 2018, str. 124), aplikacji i w żadnym wypadku nie można jej utożsamiać ze sprawdzeniem jego tożsamości, czyli uwierzytelnieniem.

Zgodnie z powyższym poprawne uwierzytelnienie użytkownika jest fundamentalne, o ile dalsze operacje prowadzone przez niego w systemie mają istotną wagę decyzyjną lub dyspozycyjną. Co istotne z perspektywy bezpieczeństwa informacji, w systemach identyfikator użytkownika pozostaje jawny, jedynie hasło jest zaszyfrowane i znane użytkownikowi i systemowi weryfikującemu. W związku z tym znajomość hasła powoduje możliwość podszycia się

pod użytkownika i autoryzowanie czynności, dyspozycji w systemie. Spośród znanych i stosowanych ataków umożliwiających złamanie hasła użytkownika znane są:

- Ataki na słowniki, czyli tabele bazy danych lub plik, w którym przechowywane są wzorce ID i odpowiadających im haseł, dzięki którym system podczas uwierzytelnienia może sprawdzić zgodność hasła z tym co wprowadził użytkownik posługujący się konkretnym ID. Z reguły zasoby te są silnie chronione, poprzez kontrolę dostępu, szyfrowanie – jednak wyrafinowany i zdeterminowany haker może pozyskać tą informację i zrobić z niej użytek.
- Atak na konta z wykorzystaniem popularnych haseł – intruz porównuje zbiory znanych i popularnych haseł do odgadnięcia hasła konkretnego użytkownika systemu.
- Ataki na konkretne konta użytkowników – to przypadek, w którym atakujący obiera sobie za cel konkretne konto użytkownika. Znając ID użytkownika systemu oszust podejmuje próbę złamania hasła. Metody łamania hasła są różne, od próby złamania za pomocą słownika popularnych haseł (Brotherston i Berlin, 2019, str. 129), po próby rejestracji podglądu hasła wpisywanego przez użytkownika.
- Przejęcie stacji roboczej – które może nastąpić w sposób bezpośredni lub programowy. Pierwszy to sytuacja, w której użytkownik nieopatrznie opuści swój komputer, który oszust następnie przejmuje i wykorzystuje do niecnych celów. Drugi sposób polega na zdalnym przejęciu stacji roboczej. W tym przypadku w odróżnieniu od fizycznego przejęcia użytkownik często nie ma świadomości, że jego komputer został zaatakowany. Zdarzają się przypadki, w których podczas tego rodzaju ataku, komputer użytkownika wykorzystywany jest jako dodatkowa moc obliczeniowa potrzebna hakerowi.
- Wykorzystanie omyłek użytkownika – czyli wykorzystanie już wcześniej opisywanych socjotechnik w celu ujawnienia hasła. Zdarzają się wciąż rozwiązania, wspierające użytkownika w wyborze hasła. W takim przypadku otrzymuje on wygenerowane hasło, które jest podpowiedzią systemu. Aktualnie rezygnuje się z tego typu rozwiązań, ponieważ zauważono, że użytkownicy w takim mechanizmie podpowiedzi poprawnego hasła nie zapamiętują go lecz zapisują, co nie jest zgodne z polityką bezpieczeństwa. Innym przypadkiem, w którym atakujący wykorzystują omylność użytkownika, są coraz rzadziej spotykane

systemy, które umożliwiają pierwsze logowanie z pomocą domyślnego, powszechnie znanego hasła. Po pierwszym logowaniu użytkownik jest proszony o zmianę hasła na własne jednak mechanizmy walidacyjne nowego hasła dopuszczają możliwość wprowadzenia starego. Stąd użytkownicy nie zmieniają go bagatelizując wagę zagadnienia. Taka sytuacja stanowi doskonałą pożywkę dla atakujących.

- Monitorowanie elektroniczne, podglądanie – często stosowane podczas prób uwierzytelnienia w systemach zdalnych. Użytkownik rozpoczynając połączenie zdalne wysyła hasło, które jest podatne na podsłuch. Oszuści próbują również monitorować stacje robocze z pomocą oprogramowania szpiegującego (ang. spyware). Podglądanie stanowi jedną z najstarszych i najmniej złożonych metod odgadnięcia ID i hasła, ale o dziwo wciąż bardzo skuteczną. Najczęściej ofiarami oszustów w tej metodzie padają osoby uwierzytelniające się w przestrzeniach publicznych (porty lotnicze, dworce, przystanki, środki masowego transportu, restauracje, puby, itp.), oraz wszystkich tych miejscach, które pozwalają na obserwację urządzenia służącego do uwierzytelnienia, przez osoby postronne.
- Wykorzystanie wielokrotnego użycia hasła – szczególnie użytkownicy, którzy uwierzytelniają się w wielu systemach, dla upraszczania zapamiętania stosują to samo lub bardzo podobne hasło do swoich ID. W przypadku złamania takiego hasła, haker ma możliwość również, uzyskać dostęp do innych systemów, do których uprawnienia posiada użytkownik.

3. SZKODLIWE OPROGRAMOWANIE

Zagrożenia wywołane przez programy komputerowe, po tych związanych z czynnikiem ludzkim stanowią kolejną równie obszerną grupę. W świecie wirtualnym, w którym podmiotem jest system, aplikacja lub program, trudno o jednoznaczny rozdział przyczyn wywoływanych przez ludzi oraz programy, ponieważ najczęściej czynnikiem zagrożenia jest działanie człowieka w programie, aplikacji, systemie. Oczywiście istnieje pewna grupa programów, które potrafią działać autonomicznie i w ramach tej grupy możemy mówić zagrożeniach wywołanych przez programy komputerowe. Z tej perspektywy niniejszy akapit zawiera informację o zidentyfikowanych według aktualnego stanu wiedzy programach komputerowych wywołujących zagrożenia bezpie-

czeństwa. W ten sposób możemy wyróżnić następujące rodzaje szkodliwego oprogramowania (ang. malware) (Stallings i Brown, 2019, strony 246-247):

- Programy z języka angielskiego określane jako adware, oprogramowanie służące do wyświetlania reklam - może ona powodować wyskakiwanie dodatków reklamowych lub przekierowywanie przeglądarki na inne witryny. Przykładem takiego oprogramowania reklamowego jest wyskakujące okienko informujące użytkownika, że oto stał się szczęśliwym wygranym wartościowej nagrody. W rzeczywistości jest to adware zintegrowane najczęściej z innym złośliwym oprogramowaniem mającym na celu przekierowanie na złośliwą witrynę, wyłudzającą dane.
- Komplet napastniczy (ang. crime kit) czyli zestaw narzędzi do generowania automatycznie nowego szkodliwego oprogramowania komputerowego. Rozwój zestawów napastniczych spowodował, że dzisiaj z łatwością mogą używać ich mniej zaawansowani użytkownicy. Przykładem takiego rozwiązania jest komplet napastniczy Zeus, który ewoluował od rozwiązania skupiającego się na wyłudzeniach bankowych transakcji internetowych, by ostatecznie stać się zaawansowanym rozwiązaniem zagrażającym przedsiębiorstwom z różnych branż (Shah, 2010).
- Autoruter (ang. autorooter) czyli wrogie narzędzie hakerskie, używane do zdalnych włamań do nowych maszyn.
- Tylne drzwi (ang. backdoor), oprogramowanie wykorzystujące mechanizm omijający zwykłą (podstawową) kontrolę bezpieczeństwa systemu lub programu. Działanie takiego mechanizmu może skutkować nieupoważnionym dostępem do funkcji w programie lub systemie. Przykładem takiego oprogramowania jest spyware o nazwie FinSpy (znane również pod nazwą FinFisher). Oprogramowanie to może zostać zainstalowane na systemach desktopowych (Windows, Linux, macOS), oraz na systemach mobilnych (iOS, Android). Powołując się na informację dostępną na stronie producenta oprogramowania antywirusowego, firmy Kaspersky, z pomocą FinSpy można przejąć całkowitą kontrolę nad urządzeniem desktopowym lub mobilnym. W każdym przypadku aplikacja udostępnia pełny zestaw narzędzi do przejęcia takiej kontroli. Niepokój wzbudza zakres możliwości jaki oferuje aplikacja w przypadku urządzeń mobilnych. Otóż w tym zakresie, napastnik, może przejąć pełną kontrolę nad urządzeniem włącznie z nagrywaniem rozmów głosowych i VoIP, podsłuchiwania popularnych komu-

nikatorów WhatsApp, WeChat, Skype, Viber, Line, Telegram, Signal i Threema (Shoshin, 2019). Do zainfekowania dochodzi najczęściej poprzez kliknięcie linku w odpowiednio spreparowanej wiadomości mail lub SMS. Najbardziej narażeni na działanie programu są właściciele systemów Android. Właściciele urządzeń z systemem iOS są bezpieczniejsi, ponieważ napastnik musi uzyskać fizyczny dostęp do urządzenia, aby go zainfekować. Warto nadmienić, że oprogramowanie FinSpy (FinFisher) (Kaspersky, 2021) dostępne jest w wersji komercyjnej, co znacząco ułatwia pozyskanie go i zastosowanie.

- Pobieracze (ang. downloaders), kod programów dołączany najczęściej do malware. Po zainicjowaniu, na atakowanym systemie następuje „w tle" proces pobierający większe pakiety złośliwego oprogramowania.
- Pobieranie uboczne (ang. drive-by download), podobny mechanizm do wymienionego w poprzednim punkcie, różniący się miejscem ataku. W tym przypadku, atak na system następuje z poziomu zaatakowanej witryny internetowej, z wykorzystaniem luk zabezpieczeń w przeglądarce internetowej, którą posługuje się użytkownik atakowanego systemu.
- W literaturze pojawia się również definicja tzw. wyzyskiwaczy (ang. exploits) czyli kodu ukierunkowanego na konkretną słabość. Przykładem takiego programu jest DirtyCow, który wykorzystuje opisany powyżej program FinSpy do uzyskania dostępu do konta z pełną kontrolą nad systemem operacyjnym, w celu przejęcia kontroli nad urządzeniem.
- Zatapiacze (ang. flooders) to rodzaj szkodliwego oprogramowania wykorzystujący duże ilości danych przesyłanych następnie do atakowanego systemu tak, aby doprowadzić do jego zajętości i tym samym zrealizowania formy ataku określanej jako odmowa dostępu systemu (DoS – ang. denial of service), Ping of Death (wysłanie zapytania o rozmiarze większym niż 65535 bajtów – narażała starsze systemy Windows 3.11,95, NT na awarię lub zawieszenie pracującej w nich aplikacji), ICMP (Internet Control Message Protokol), przeciążenia HTTP.
- Rejestratory aktywności (ang. keyloggers), przekazujące kod wciskanych przez użytkownika systemu klawiszy klawiatury. Przykładem złośliwego keyloggera jest Eye Pyramid, złośliwe oprogramowanie, które zagroziło wielu włoskim instytucjom publicznym. Zainstalowane

keyloggery były odpowiedzialne za wykradanie ID i haseł do uwierzytelniania, a następnie do uzyskiwania poufnych informacji. Poszkodowanymi tej cyberprzestępczej kampanii byli prezes Europejskiego Banku Centralnego – Mario Draghi, oraz premierzy Matteo Renzi i Mario Monti. Innym przykładem jest keylogger PunkeyPOS, z pomocą którego zainfekowano terminale POS. Keylogger w tym przypadku instaluje się razem ze skanerem pamięci RAM urządzenia POS, w której przechowywane są informację odczytywane z karty kredytowej klienta. Informacja odczytana z karty wraz z danymi odczytanymi przez keylogger z klawiatury, następnie w formie zaszyfrowanej trafia do serwera cyberprzestępców. W ten sposób oszuści uzyskali informacje poufne dotyczące kart kredytowych, należących do tysięcy osób.

- Bomba logiczna (ang. logic bomb), „uśpiony" kod wstrzykniętego złośliwego oprogramowania do systemu, uruchamiający swoje działanie po wykonaniu przez użytkownika specyficznej sekwencji czynności (warunku uruchomienia). Spośród najbardziej znanych i spektakularnych ataków z wykorzystaniem bomb logicznych, należy wymienić atak na serwery banku UBS. Bombę wprowadził do sieci administrator Roger Duronio, który następnie został oskarżony i skazany ze ten czyn na 8 lat i 1 miesiąc więzienia, oraz karę restytucji na rzecz UBS w wysokości 3,1 miliona dolarów. Podobny przypadek z wykorzystaniem bomby logicznej odnotowała firma Siemens Corporation. Jej pracownik kontraktowy David Tinley zaszył bombę logiczną w przygotowanym przez siebie arkuszu kalkulacyjnym. Arkusz co pewien czas ulegał uszkodzeniu – w związku z działaniem bomby logicznej, a Tinley za dodatkową opłatą był proszony o jego naprawienie. Bomby logiczne zostały wykryte w momencie, gdy Tinley, przebywając poza miastem, został poproszony o podanie hasła administracyjnego do arkusza. 19 lipca 2019 r. David Tinley przyznał się do winy.
- Makrowirusy, złośliwe oprogramowanie wbudowane w kodzie makr dokumentów (tekstowych, arkuszy kalkulacyjnych, itp.), lub ich szablonów, uruchamiane podczas ich otwierania. Tak uruchomione makrowirusy replikują się na podobne dokumenty istniejące już w systemie (stacji roboczej), najczęściej wyrządzając w nich nieodwracalne szkody.
- Zestawy administracyjne (ang. rootkit), rodzaj złośliwego oprogramowania stosowany przez napastnika po włamaniu się do systemu i uzyskaniu dostępu administracyjnego.

- Programy spamujące (ang. spammer programs), używane do wysyłania dużej ilości niepotrzebnych wiadomości na konta atakowanej organizacji.
- Programy szpiegujące (ang. spyware), przesyłające do intruzów (w przypadku rozważań na temat nieuprawnionej ingerencji w system) informacje nielegalnie pozyskane w stacji roboczej (komputerze) użytkownika. W praktyce znane są użycia programów szpiegujących jako elementu zabezpieczenia i monitorowania aktywności użytkownika systemu. Informacje dotyczące aktywności użytkownika, kodów wciskanych klawiszy, ruchu sieciowego, głosu, obrazu.
- Konie trojańskie (ang. trojan horse) programy prezentujące użyteczną „z pozoru" funkcję, równocześnie skrywając funkcje niebezpieczną (Kowalewski i Kowalewski, Ochrona informacji i systemów teleinformatycznych w cyberprzestrzeni, 2017, str. 19).
- Wirusy - najczęściej spotykany w praktyce rodzaj złośliwego oprogramowania, próbujący rozprzestrzenić się na inne stacje robocze (komputery), wyrządzając w nich szkody (Kowalewski i Kowalewski, Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm, 2017, str. 40).
- Robaki (ang. worm), tym mianem określa się złośliwe programy komputerowe potrafiące działać niezależnie i rozsiewać swoje kopie na inne stacje robocze. Różnica pomiędzy wirusami, a robakami polega na tym, że wirus infekuje kod, który jeżeli zostanie wykonany wykona również złośliwe (zainfekowane) sekwencje, natomiast robak działa autonomicznie.
- Zombie (ang. zombie boot), złośliwe oprogramowanie – zainstalowane na zainfekowanej stacji roboczej, serwerze lub innym elemencie sieci komputerowej, zdolnym do przechowywania oprogramowania i wykonywania jego kodu - uaktywniające się samodzielnie w celu zaatakowania innych maszyn.

Oprócz wyżej opisanych spotykamy się również z zagrożeniami związanymi z fizycznym bezpieczeństwem systemów i sprzętu. Grupa zagrożeń fizycznego bezpieczeństwa zawiera:

- przypadki fizycznej utraty sprzętu w związku z kradzieżą, zagubieniem, utratą sprzętu pod przymusem (napad, terroryzm, niekontrolowane paramilitarnych zachowanie grup bojowników w różnych niebezpiecznych rejonach świata), dewastacją,

- próby nieuprawnionego dostępu bezpośrednio do urządzeń lub infrastruktury sieciowej (nieuprawniony dostęp do pomieszczeń serwerowni, serwerów itp.),
- próby nieuprawnionego dostępu do przestrzeni biurowej firmy – w takich przypadkach atakujący ma możliwość bezpośredniego podglądu np. loginów i haseł w otwartej przestrzeni biurowej, możliwość rozpoczęcia próby ataku poprzez pozostawienie na stawisku pracy zainfekowanej pamięci USB, lub w ekstremalnych sytuacjach kradzież stacji roboczej która następnie posłuży do ataku na system informatyczny organizacji.

4. ZAGROŻENIA Z TŁEM POLITYCZNYM

Zagrożenia z tłem politycznym stanowią kolejną grupę, która nabiera coraz większego znaczenia. W kontekście użytkownika końcowego, działania takie często oznaczają niejawną inwigilację i ograniczenia dostępu do zasobów internetowych. Z perspektywy dużych organizacji, sytuacja polityczna oraz możliwość jej zmian ma istotne znaczenie dla oceny ryzyka funkcjonowania systemów IT. Doskonałym przykładem takiego działania są duże międzynarodowe banki, które w poszukiwaniu informatyków, często decydują się na lokalizację swoich biur w krajach o mniej stabilnych systemach politycznych. W przypadku Europy, osoby zatrudnione w tych biurach, korzystają z serwerów w Szwajcarii, Anglii, Irlandii, łącząc się z nimi w sposób bezpieczny ze swoich lokalizacji. W sytuacji wystąpienia zagrożenia z jakim mieliśmy do czynienia w kontekście działań militarnych np. w rejonie półwyspu Krymskiego, pomiędzy Rosja i Ukrainą, w ten sposób zabezpieczone dane nie były narażone na nieuprawniony wyciek. Najciekawszym kontekstem w tej grupie, są zagrożenia wynikające z prawdopodobnych scenariuszy wojen cybernetycznych i prób przejęcia kontroli nad dużymi systemami przesyłowymi (np. energetycznymi), czy rządowymi. Spośród wymienianych przykładów ataków cybernetycznych na państwa, wymieniany jest atak na systemy komputerowe austriackiego MSZ 4 stycznia 2020 r. (TVP, 2020) W rzeczywistości skala ataków tego typu ataków jest ogromna, i tylko część z nich udaje się zidentyfikować jako działania innego państwa, a zatem nadać im kontekst polityczny. Wojny cybernetyczne są scenariuszami wojen hybrydowych, które staja się rzeczywistością w dobie możliwości przejęcia zdalnej kontroli nad kluczowymi systemami funkcjonowania Państwa, bez konieczności użycia wojska i broni. Od wielu lat tworzone są specjalne komórki działające w ramach

struktur państwa mające na celu przeciwdziałanie tego typu zagrożeniom. Dla przykładu w Polsce pracuje prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, który pełni rolę CSIRT (ang. Computer Security Incident Response Team) odpowiadając za koordynacje reagowania na incydenty komputerowe występujące w obszarze wskazanym przez art. 26 ust 7 ustawy z dnia 5 lipca 2018 o krajowym systemie cyberbezpieczeństwa (Dz.U.2018 poz. 1560).

5. ZAGROŻENIA ZEWNĘTRZNE I WEWNĘTRZNE

W grupie zagrożeń zewnętrznych znajdują się wszystkie te, które pochodzą z zewnątrz organizacji. W tej grupie znajdziemy zarówno zagrożenia wywołane przez czynnik ludzki jak i programy komputerowe. Można wyobrazić sobie również zagrożenia fizycznego bezpieczeństwa systemu inspirowane z zewnątrz organizacji oraz te z tłem politycznym. Grupa zagrożeń wewnętrznych to wszystkie te, które inicjowane są z wnętrza organizacji (Grzywacz, 2016, str. 126).

6. ZAGROŻENIA AKTYWNE I PASYWNE

W literaturze spotykany jest również podział na zagrożenia aktywne i pasywne (Bandera i Grzywacz, 2016, str. 157), przyjmujący za kryterium podziału sposób ingerencji w system informatyczny. Tym samym do grupy zagrożeń pasywnych autorzy zaliczają te które, które skutkują ujawnieniem informacji w sposób nieuprawniony, bez oddziaływania na system informatyczny, oraz zagrożenia aktywne, które czynnie oddziałowują na system informatyczny.

7. SPOSOBY UNIKANIA ZAGROŻEŃ

Według badań prowadzonych przez Związek Banków Polskich w 2018 – 25 % Polaków nie zwraca uwagi na symbol kłódki i oznaczenie „https://" na początku adresu strony internetowej (Związek Banków Polskich, 2020, str. 7). Symbol kłódki, który pojawia się najczęściej z lewej strony wpisywanego adresu internetowego w przeglądarce, jest informacją, że połączenie z serwerem jest szyfrowane. Nie oznacza to jednak pełnego bezpieczeństwa. Należy również sprawdzić pochodzenie wystawionego w ten sposób certyfikatu oraz dla kogo został wystawiony. W ten sposób można zweryfikować pochodzenie strony (systemu) z którą się łączymy. Cyberprzestępcy również korzystają z bezpiecz-

nych połączeń, tak aby, możliwie najbardziej uwiarygodnić strony internetowe za pomocą których wyłudzają nasze dane, stąd taka kontrola jest bardzo istotna. Kolejnym równie istotnym elementem z perspektywy bezpieczeństwa jest sprawdzenie, czy w adresie wpisywanej strony znajduje się tekst „https://" (ang. hypertext transfer protocol secure) - oznacza to, że połączenie jest bezpieczne (korzysta z szyfrowanej wersji protokołu http). Szczególnie istotne jest podejście użytkowników do korespondencji otrzymywanej kanałami elektronicznymi. Jak wiadomo, istnieje wiele okoliczności, w których użytkownicy są zmuszeni do ujawniania swoich adresów mail, każde takie ujawnienie wiąże się z zapisem w zewnętrznej bazie danych i możliwością użycia adresu przez stronę zapisującą. Adresy mail udostępniane są na stronach internetowych, w prasie, ogłoszeniach itp. Dzieje się tak za zgodą właściciela użytkownika adresu, jednak nie zawsze cel, który przyświeca w związku z ekspozycją adresu jest spójny z działaniami cyberoszustów. W taki sposób pozyskany adres może stać się przyczynkiem do rozwoju opisanych powyżej scenariuszy wyłudzeń tożsamości. Aby unikać takich sytuacji, użytkownicy powinni rozpatrzyć stworzenie dodatkowych skrzynek mailowych z przypisanymi do nich adresami e-mail i poziomami zaufania do bezpieczeństwa korespondencji, która w nich się pojawia (od najwyższego – zaufana skrzynka mail, do najniższego – skrzynki, na którą trafia spam). Zaufana skrzynka mail to ta, której adres nie jest udostępniany do „świata" Internetu. Tutaj dostęp mają wyłącznie zaufani użytkownicy (coraz częściej dostawcy usług pocztowych udostępniają możliwość filtrowania skrzynek pocztowych pod kątem tzw. spamu, dzięki czemu możliwe jest zdefiniowanie takich ograniczeń). Skrzynka najmniej zaufana, czyli taka, do której bez przeszkód może trafić korespondencja określana jako spam, nie zapewniająca żadnego poziomu bezpieczeństwa informacji, umożliwiająca jedynie „ręczne filtrowanie" otrzymanych na nią wiadomości. Oczywiście od inwencji użytkownika zależy, ile i z jakim priorytetem skrzynek utworzy, niemniej operowanie dwoma wyżej wymienionymi w znaczący sposób zmniejsza ryzyko zareagowania na niechcianą wiadomość, pod warunkiem, że użytkownik oprócz wspomnianego podziału zastosuje jeszcze stosowne zasady czytania i interpretowania wiadomości. Należy również podkreślić, że taki sposób radzenia sobie z wyłudzeniami i niechcianą korespondencją to tylko narzędzie wspomagające, w żaden sposób nie zwalniające użytkownika z obowiązku weryfikowania i reagowania na treść wiadomości. Ogólnie przyjętą metodą jest, aby treść widomości, w której nadawca oczekuje od odbiorcy specyficznej aktywności lub decyzyjności, taktować jako pocho-

dząca z niezaufanego źródła, a zatem mogącą wyłudzać informacje lub dane. Od odbiorcy zależy jaki poziom weryfikacji posłuży mu do zaakceptowania dyspozycji z wiadomości i podjęcia w związku z nią akcji (telefon do adresata i weryfikacja głosowa, bezpośrednie osobiste sprawdzenie pochodzenia wiadomości u adresata lub w organizacji, którą reprezentuje). Jeżeli rozważania kierujemy na grunt zawodowy, należy wspomnieć, że dobrze rozwinięte organizacje, posiadają najczęściej zbiór zasad jakimi powinien kierować się użytkownik (odbiorca widomości) w sytuacji otrzymania wiadomości powodującej podejrzenia co do intencji jej nadawcy. Takie zasady opisane są w postaci polityk bezpieczeństwa organizacji, a jej członkowie mają obowiązek bezwzględnego stosowania się do nich. Niezależnie od wytycznych w każdej sytuacji podejrzenia otrzymania korespondencji wyłudzającej nie należy podejmować aktywności opisanych w jej treści, a incydent zgłosić do wyznaczonej komórki w organizacji lub jeżeli niesie on poważne skutki np. ekonomiczne i występuje na gruncie prywatnym – do organów ścigania. Jest to bardzo istotne, ponieważ bez takiej informacji nie będzie możliwe podjęcie aktywności, dzięki którym możliwa będzie identyfikacja oszusta.

Do łamania haseł, oszuści często wykorzystują tzw. słowniki popularnych haseł. Dzieje się tak ponieważ użytkownicy często tworzą hasła łatwe do zapamiętania (jak wyżej napisano użytkownik najczęściej posiada wiele haseł do różnych systemów, a to może przysporzyć trudności z ich zapamiętaniem), stąd częstą – niestety złą praktyką wśród użytkowników - są hasła łatwe do zapamiętania. W ten sposób do haseł użytkowników trafiają nazwy dni tygodnia, imiona, nazwy miejscowości, budynków biurowych w których pracują itp. Taką sytuację skutecznie wykorzystują oszuści tworząc listy haseł, które następnie są wykorzystywane przez hasło-łamacze (ang. password cracker) do odgadnięcia hasła bezpośrednio przez próbę logowania, lub do jego odszyfrowania. Przykładem takiego oprogramowania jest ogólnie dostępny łamacz haseł o nazwie John the Ripper (Openwall, 2019), czy Cain and Abel (Darknet, 2017). Warto nadmienić, że z poziomu systemu hasła podlegają również ochronie, przez np. haszowanie, jednak istnieją metody umożliwiające hakerom odszyfrowanie haszowanego hasła, poprzez porównanie ich z opisywaną wyżej listą haseł prostych, oraz odszyfrowanie wartości tzw. soli w zawartości haszowanego hasła. Coraz częściej spotkać można szereg reguł walidacyjnych (to one najczęściej wprawiają użytkownika w irytację), wymagających określonej długości hasła, użycia nie tylko znaków alfanumerycznych, ale również specjalnych, czy zróżnicowania wielkości liter. Wszystkie czynniki wymienio-

ne w zdaniu poprzednim są wynikiem rozważań na temat dostępnych i stosowanych przez hakerów metod łamania haseł. Najczęstszym błędem są właśnie wspomniane już wyrazy słownikowe, nazwy proste. Na czas łamania hasła, wpływ ma jego długość. Aktualnie oszuści dysponują znacznymi mocami obliczeniowymi komputerów, aby szybko prowadzić działania porównujące i odszyfrowania haseł. Dzisiaj metody odkrycia hasła nie sprowadzają się wyłącznie do porównań słownikowych, ale są również wynikiem analizy ogromnych zbiorów haseł odszyfrowanych przez hakerów w wyniku włamań do portali czy systemów internetowych. Wielomilionowe zbiory haseł pozwalają oszustom na dokonanie oszacowań co do kryteriów wyboru rodzaju hasła przez użytkowników. Taka znajomość zachowania i decyzji użytkowników przy wyborze hasła pozwala na znaczne zawężenie zbiorów danych „wzorcowych" haseł, które są użyte do porównania. Zmniejsza to ilość mocy obliczeniowej potrzebną do odszyfrowania hasła pojedynczego użytkownika. Dlatego istotne jest, aby przy wyborze hasła użytkownik posługiwał się odpowiednimi kryteriami:

- długości hasła – ma to wpływ na czas odszyfrowywania,
- użyciem różnej wielkości liter – wpływa na ilość potrzebnych do porównania danych słownikowych,
- użyciem znaków specjalnych – znacząco utrudnia atak z użyciem słowników,
- wyborem niepopularnego hasła, najlepiej składu nic nieznaczących łącznie liter. Prostym przepisem na stworzenie takiego hasła jest wymyślenie zdania, z którego stworzone zostanie następnie hasło np. „Najlepsze wakacje które spędziłem od 10 lat były w Australii ;-)". Następnie z pierwszych liter wyrazów, cyfr i znaków specjalnych tworzymy hasło: **Nwkso10lbwA;-)**. Tak stworzone hasło spełnia wszystkie wymogi opisane powyżej.

Również istotne jest, że najczęściej haker pozyskując plik lub tabelę bazy danych z informacjami o parze ID - hasło, potrzebuje czasu, aby odszyfrować zależności i hasła. Częsta zmiana hasła minimalizuje ryzyko, ponieważ zanim haker użyje odszyfrowanego hasła, użytkownik posługuje się już nowym, a zatem uwierzytelnienie dla hakera zwróci negatywny wynik.

Spośród metod zabezpieczających, na uwagę zasługuje uwierzytelnienie dwuetapowe (dwuskładnikowe). Omówienie tego sposobu uwierzytelnienia wykracza poza zakres niniejszego opracowania, dlatego autor zdecydował się jedynie wspomnieć o jego istnieniu, ograniczając się do krótkiego opisu. Tego

typu uwierzytelnienie najczęściej spotykane jest w systemach bankowych. Zgodnie z dyrektywą PSD2, banki zobowiązane są do jego stosowania. Idea tego rodzaju zabezpieczenia polega na uwierzytelnieniu, które użytkownik prowadzi co najmniej dwoma niezależnymi kanałami komunikacji. W przypadku logowania do systemu bankowego, użytkownik w pierwszej kolejności wpisuje swoje ID, następnie hasło oraz dodatkowe zabezpieczenie w postaci kodu z karty kodów udostępnianych przez bank, kodu tokena, lub kodu SMS przesłanego na numer telefonu użytkownika. Rozwiązanie polegające na wykorzystaniu karty ze zdrapywanymi kodami nie jest już obecnie stosowane. Tokeny, czyli urządzenia, które generują ciąg cyfr za pomocą funkcji jednokierunkowej wykorzystującej dwa parametry – stały ID danego urządzenia i zmienny – ciąg cyfr generowany najczęściej w określonym czasie), są stosowanie już bardzo rzadko i w specyficznych sytuacjach (np. zabezpieczenie kanału VPN w pracy zdalnej). Najczęściej stosowanym „drugim" zabezpieczeniem jest kod SMS, wysyłany na numer telefonu zdefiniowanego przez użytkownika. Jest to rozwiązanie zarówno praktyczne jak i korzystne ekonomicznie, a zwarzywszy na powszechną dostępność telefonów komórkowych dla użytkowników, nie ogranicza ono liczby potencjalnych klientów bankowości internetowej.

W przypadku ataku na konkretne konto użytkownika, najczęściej stosowanym zabezpieczeniem jest ograniczenie ilości prób zalogowania po wprowadzeniu niewłaściwego hasła. Tego typu ataki są w głównej mierze monitorowane i udaremniane przez administratorów. Użytkownik ma możliwość wpływania na tego typu ataki poprzez chronienie swojego ID oraz nieupowszechnianie informacji, które mogłyby prowokować włamywacza do podejmowania próby łamania hasła dostępowego do jego konta. W przypadku działań administracyjnych, w przypadku wrażliwych systemów stosuje się monitoring aktywności użytkowników. Administratorzy mogą zablokować aktywności pochodzące z określonych adresów IP dla komputerów (użytkowników), które wielokrotnie nieskutecznie próbują zalogować się do systemu. Najczęściej przyjmuje się, że użytkownik może wprowadzić trzy do pięciu niepoprawnych haseł zanim konto zostanie zablokowane. Po zablokowaniu konta wymagany jest kontakt z infolinią bądź osobisty z odpowiednią komórka organizacji, w celu odblokowania możliwości dostępu. Architektura funkcjonalności logowania umożliwia również wsparcie użytkownika w sytuacji problemu z przypomnieniem hasła, realizowane poprzez pytania i odpowiedzi pomocnicze, które użytkownik definiuje podczas procesu zakładania konta

lub pierwszego logowania. Niektóre systemy, głównie komercyjne, coraz częściej umożliwiają logowanie za pomocą ID oraz haseł z kont np. portali społecznościowych czy popularnych przeglądarek internetowych. W znaczący sposób ułatwia to użytkownikowi zapamiętania hasła.

Działania w celu wyeliminowania pomyłek ludzkich, polegają na prowadzeniu częstych szkoleń, podczas których użytkownicy są zaznajamiani, lub przypomina się im o najczęściej stosowanych zagrożeniach związanych z wykorzystaniem kanałów elektronicznych (Capiga, 2015, str. 182), manipulowania informacją, oraz przedstawia mechanizmy zapobiegania im. W proces szkoleniowy powinny zostać włączone również testy pishingowe organizacji, aby utrwalić i zweryfikować poziom bezpieczeństwa pracowników po szkoleniach, oraz ogólny poziom bezpieczeństwa organizacji. Cykliczne szkolenia stanowią bardzo istotny element działalności organizacji, ponieważ jak wskazują badania ludzie uważają złośliwe informacje pochodzące z wnętrz organizacji (30 %), oraz błędy ludzkie (25 %), za dwa największe zagrożenia cyberbezpieczeństwa (Security magazine, 2019). Obie te kategorie należy uznać za działania związane tzw. „czynnikiem ludzkim", stąd istotne znaczenie szkoleń w organizacji.

Zapobieganie monitorowaniu elektronicznemu, polega przede wszystkim na zachowaniu zasad bezpieczeństwa uniemożliwiających zainstalowanie oprogramowania szpiegowskiego na komputerze użytkownika:

- otwieranie bezpiecznej korespondencji,
- wchodzenie (klikanie) na bezpieczne linki,
- nieudostępnianie zasobów komputera,
- blokowanie komputera,
- zabezpieczenie możliwości otwarcia systemu,
- nieprzekazywanie ID oraz haseł innym użytkownikom.

Dla użytkowników często podróżujących, ważnym aspektem zabezpieczającym przed monitorowaniem elektronicznym, jest korzystanie z sieci zabezpieczonych. Często w obrębie dworców, lotnisk spotyka się sieci niezabezpieczone. Logowanie do takich sieci umożliwia korzystanie z zasobów internetu, jednak stwarza ryzyka ataku oszustów (Chell, Erasmus, Colley i Whitehouse, 2018, str. 33). Generalnie zasadą jest unikanie logowania do sieci niezabezpieczonych. Przeciwdziałanie podglądaniu hasła polega na unikaniu uwierzytelniania w miejscach publicznych, a jeżeli jest to koniecznością, sprawdzenia czy miejsce, w którym uwierzytelnienie ma nastąpić zabezpiecza użytkownika przed możliwością podglądu wpisywanego ID i hasła. Należy również zwró-

cić uwagę na obecność osób postronnych (np. w przestrzeni biurowej) i przy stwierdzeniu możliwości podglądu hasła starać się wprowadzić je w taki sposób, aby przysłonić go przed obserwatorami.

Należy unikać korzystania z tych samych haseł w wielu systemach. W ramach jednej organizacji definiowane przez użytkownika hasło, może być walidowane tak, aby nie pojawiało się więcej niż jeden raz. Obecnie stosowane są rozwiązania korzystające z funkcji platform tożsamości (Microsoft, 2020). Takie podejście umożliwia weryfikowanie i uwierzytelnienie poświadczeń w wielu aplikacjach, urządzeniach i usługach, za pomocą jednego ID i hasła.

Działania prewencyjne w przypadku złośliwego oprogramowania są podobne do tych, które podejmuje się w przypadku działań związanych z „czynnikiem ludzkim".

Adware – jako niechciana reklama, pojawia się najczęściej już w wyniku zainfekowania komputera. Istnieje wiele sposobów zainfekowania, jednak najczęściej to te, które są związane z dostępem do interenetu i wiadomościami mail. Czytając przejęte przez intruzów strony internetowe oraz wiadomości mail z nieznanego źródła, użytkownicy narażają swoje stacje robocze na zainfekowanie adware. Aby tego uniknąć należy starać się korzystać ze stron internetowych zabezpieczonych (protokół „https://", oraz znak kłódki świadczący o certyfikacie i bezpieczeństwie – opisywane wyżej), w żadnym wypadku nie należy otwierać wiadomości, których kontekst wydaje się podejrzany, a treści chociażby tytułu są nie związane z tematami interesującymi użytkownika. Należy również bezwzględnie unikać czytania wiadomości z informacją o wystawionej rzekomo fakturze, dopłacie do ogłoszenia z portalu internetowego. W razie takiej sytuacji, jeżeli informacja pochodzi od rzekomo renomowanej firmy należy starać się skontaktować i potwierdzić taką sytuację, przed otwarciem wiadomości mail. Adware mogą również przeniknąć do stacji roboczej podczas pobierania plików z interenetu, próby darmowej wersji gry internetowej itp. W celu minimalizowania tego typu sytuacji należy również posiadać zainstalowaną w stacji roboczej aktualną wersję oprogramowania antywirusowego oraz pamiętać o cyklicznych skanowaniach systemu komputera, tak aby możliwe było sprawdzenie nie tylko bieżących plików i treści witryn przeglądanych przez użytkownika, ale również kontrola systemu plików i rejestrów danej maszyny.

Podstawowym sposobem zapobiegania zainfekowaniu oprogramowaniem backdoor FinSpy jest unikanie klikania w linki z nietypowych wiado-

mości mail i SMS, oraz nie dopuszczanie do możliwości przejęcia fizycznej kontroli, przez intruza, nad urządzeniami (tu z systemem iOS).

Zarówno pobieracze, wyzyskiwacze jak i rejestratory klawiszy (ang. keylogger) są najczęściej wprowadzane do systemu wspólnie z innym złośliwym oprogramowaniem. Metody infekowania najczęściej sprowadzają się do zachęty użytkownika do kliknięcia linku w wiadomości mail lub SMS. Infekcja następuje również przez pobrania plików z niezweryfikowanych źródeł w internecie.

W przypadku bomb logicznych w opisywanych przykładach ich użycia, pojawia się ponownie - już opisywany - czynnik ludzki (w tym przypadku celowe działanie osób posiadających stosowne uprawnienia do wprowadzenia bomb do sieci lub oprogramowania). Podstawowe środki przeciwdziałania, jakie powinni podjąć użytkownicy to czujność i poprawna ocena informacji w tym linków dostarczanych w wiadomościach mail oraz SMS, posiadanie aktualnego oprogramowania antywirusowego, zaplanowanych skanowań systemu, pobieranie zweryfikowanych plików z sieci internet (unikanie korzystania ze stron, których treści zawierają błędy ortograficzne i gramatyczne, zdania są nielogicznie sformułowane). Ponadto, w ramach organizacji wymagane jest wdrożenie, najlepiej w ramach polityki bezpieczeństwa, mechanizmów przeciwdziałania przed nieodpowiednim zachowaniem osób posiadających uprawnienia do zarządzania kluczowymi ogniwami infrastruktury IT, poprzez np. monitorowanie z zastosowaniem systemów klasy SIEM (Security Information and Event Management).

Dla unikania negatywnych skutków działania makrowirusów, rekomenduje się przede wszystkim unikanie pracy z makroinstrukcjami (makrami) dokumentów o nieznanym pochodzeniu. Pakiety biurowe posiadają stosowne zabezpieczenia informując użytkowników otwierających dokumenty o istniejących w nich makrach oraz potencjalnych zagrożeniach płynących z korzystania z nich. Użytkownik informowany w ten sposób ma możliwość zablokowania makra przed uruchomieniem w dokumencie. Sprawdzenie pochodzenia (autora) i celu istnienia makra w dokumencie zabezpiecza przed zainfekowaniem makrowirusem. Duże organizacje posiadające wewnątrz opisane reguły bezpieczeństwa, poddają okresowym przeglądom kod dokumentów posiadających m.in. makroinstrukcje, dla wykrycia potencjalnych zagrożeń ze strony makroinstrukcji czy bomb logicznych. Jest to proces skomplikowany, ponieważ wymaga podejmowania szeregu dodatkowych aktywności na etapie tworzenia makroinstrukcji (np. dokładnego opisu kodu – zrozumiałego dla

późniejszej analizy), ale dzięki temu minimalizuje się ryzyko, które w przypadku zmaterializowania znacznie przewyższyłoby nakłady na wspomniane działania.

Spam docierający na skrzynki pocztowe użytkowników, nie stanowi większego zagrożenia o ile nie zawiera wirusów czy fałszywych linków wyłudzających dane, które nieopatrznie użytkownik zechce wykorzystać w swoich aktywnościach. Najczęściej mierzalnych efektem istnienia spamu jest irytacja użytkownika w powodu otrzymywania niezamawianych, niechcianych, niepotrzebnych wiadomości. Inaczej temat spamu wygląda z perspektywy organizacji. Przede wszystkim niechciana korespondencja:

- może zawierać malware, oraz linki wyłudzające, które użytkownik może zastosować wprowadzając do infrastruktury organizacji, tym samym umożliwiając atak cyberoszustom,
- prowadzi do obciążenia infrastruktury w związku z koniecznością przesyłu niepotrzebnych informacji pomiędzy serwerami i użytkownikami końcowymi (zajętość),
- dekoncentruje użytkowników, zajętych podejmowaniem decyzji co zrobić z wiadomością pozbawioną kontekstu komunikacyjnego, na wykonywaniu swoich podstawowych obowiązków.

Dlatego na poziomie administracyjnym analizuje się i stosownie filtruje ruch wiadomości pocztowych użytkowników, tak aby możliwie ograniczyć obecność spamu. Od samych użytkowników natomiast wymaga się zgłaszania niezamawianych wiadomości, tak aby podjąć działania monitorujące aktywność ich nadawców względem organizacji i oszacować zmianę statusu wiadomości na spam.

Podobnie jak w opisanych powyżej przypadkach, przeciwdziałanie programom szpiegującym, koniom trojańskim, wirusom, robakom oraz programom typu zombie, sprowadza się do przestrzegania reguł polegających na unikaniu pobierania i wykorzystywania oprogramowania z nieznanych źródeł, stosowania zasad odczytywania wiadomości i wykorzystywania zawartych w nich załączników i linków. Ważnym elementem zapobiegania jest również aktualizowanie i skanowanie sprzętu w poszukiwaniu złośliwego oprogramowania. Jako nadrzędną zasadę użytkownik powinien przyjąć analogicznie do tej obowiązującej w ruchu drogowym – zasadę ograniczonego zaufania.

PODSUMOWANIE I WNIOSKI KOŃCOWE

Różnorodność podejmowanych przez cyberoszustów działań nie pozwala na zdefiniowanie jednego skutecznego środka zapobiegania niebezpieczeństwom. Większość opisywanych, aktualnych metod sprowadza się do monitorowania i doraźnego przeciwdziałania aktywności oszustów, które z czasem rozwijają się i stają bardziej wyrafinowane. Dzisiejsze możliwości użycia sztucznej inteligencji, algorytmów genetycznych, dużych mocy obliczeniowych przenoszą oszustów i dbających o bezpieczeństwo, w nowe wymiary, w których rywalizują - jedni dla własnych korzyści, drudzy dla bezpieczeństwa danych systemów, organizacji i ich użytkowników. Rywalizacja, która w szybko zmieniającym się świecie zdaje się nie mieć końca. Użytkownikom w obliczu tak skomplikowanych procesów pozostaje zachowanie intuicyjnego podejścia do otrzymywanych informacji, wspomnianego ograniczonego zaufania oraz nade wszystko bezwzględne przestrzeganie zaleceń i reguł bezpieczeństwa.

Bibliografia

Bandera, R. i Grzywacz, J. (2016). Zagrożenia bezpieczeństwa w bankowości elektronicznej. *Zeszyty Naukowe PWSZ w Płocku Nauki Ekonomiczne t.XXIV*, strony 151-168.

Brotherston, L. i Berlin, A. (2019). *Bezpieczeństwo defensywne*. Gliwice: Helion.

Capiga, M. (2015). *Bezpieczeństwa transakcji finansowych w Polsce*. Warszawa: CeDeWu.

Chell, D., Erasmus, T., Colley, S. i Whitehouse, O. (2018). *Bezpieczeństwo aplikacji mobilnych Podręcznik hakera*. Gliwice: Helion.

Gospodarowicz, A. (2018). Bezpieczeństwo nakowości internetowej i bankowości mobilnej. w A. Gospodarowicz, *Bankowość elektroniczna. Istota i innowacje* (strony 117-132). Warszawa: C.H.Beck.

Grzywacz, J. (2016). *Bankowość elektroniczna w przedsiębiorstwie*. Warszawa: Oficyna Wydawnicza Szkoła Główna Handlowa w Warszawie.

Kowalewski, J. i Kowalewski, M. (2017). *Ochrona informacji i systemów teleinformatycznych w cyberprzestrzeni*. Warszawa: Oficyna Wydawnicza Politechniki Warszawskiej.

Kowalewski, J. i Kowalewski, M. (2017). *Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm*. Warszawa: Oficyna Wydawnicza Politechniki Warszawskiej.

Krawiec, J. (2019). *Cyberbezpieczeństwo Podejście systemowe*. Warszawa: Oficyna Wydawnicza Politechniki Warszawskiej.

Nadnagy, C. (2020). *Socjotechnika Sztuka zdobywania władzy nad umysłami*. Gliwice: Helion.

Stallings, W. i Brown, L. (2019). *Bezpieczeństwo Systemów Informatycznych Zasady i praktyka*. Gliwice: Helion.

Ustawa z dnia 5 lipca 2018 o krajowym systemie cyberbezpieczeństwa (Dz.U.2018 poz. 1560)

Raport ZBP Cyberbezpieczny portfel. Edycja III (2020, styczeń). Związek Banków Polskich https://www.zbp.pl/getmedia/156b5c44-bfcc-46cb-a5d1bd0d141e9ed0/ZBP_CyberbezpiecznyPortfel2020

Barometr cyberbezpieczeństwa. W obronie przed atakami (2019, kwiecień) KPMG - https://assets.kpmg/content/dam/kpmg/pl/pdf/2019/04/pl-Raport-KPMG-Barometr-Cyberbezpieczenstwa-W-obronie-przed-cyberatakami.pdf

(www1) Global Firepower (2022) https://www.globalfirepower.com/countries-listing.php

(www2) NBC News (2022) https://www.nbcnews.com/politics/national-security/biden-presented-options-massive-cyberattacks-russia-rcna17558

(www3) Gartner (2018) https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

(www4) NestBank (2020) https://nestbank.pl/dla-twojej-firmy/bezpieczenstwo/bezpieczenstwo-kont-bankowych

(www5) Shah C. (2010) https://www.mcafee.com/blogs/other-blogs/mcafee-labs/zeus-crimeware-toolkit/

(www6) Shoshin P. (2019) https://www.kaspersky.com/blog/finspy-commercial-spyware/27606/

(www7) Kaspersky (2021) https://www.kaspersky.pl/o-nas/informacje-prasowe/3455/spyware-finfisher-wraca-z-rozbudowanym-arsenalem

(www8) TVP (2020) https://www.tvp.info/46060957/hakerzy-zaatakowali-systemy-komputerowe-austriackiego-msz

(www9) Openwall (2019) https://www.openwall.com/john/doc/

(www10) Darknet (2017) https://www.darknet.org.uk/2007/01/cain-and-abel-download-windows-password-cracker/

(www11) Security magazine (2019) https://www.securitymagazine.com/articles/90734-human-factor-is-a-persistent-cybersecurity-threat-survey-says

(www12) Microsoft (2020) https://docs.microsoft.com/pl-pl/azure/active-directory/authentication/overview-authentication