UKE | Urząd Komunikacji Elektronicznej

we współpracy z

FUNDACJA bezpieczna cyberprzestrzeń

PODRĘCZNIK BEZPIECZNEGO KORZYSTANIA ZE ŚRODKÓW KOMUNIKACJI ELEKTRONICZNEJ W CYBERPRZESTRZENI

Warszawa, grudzień 2018r.

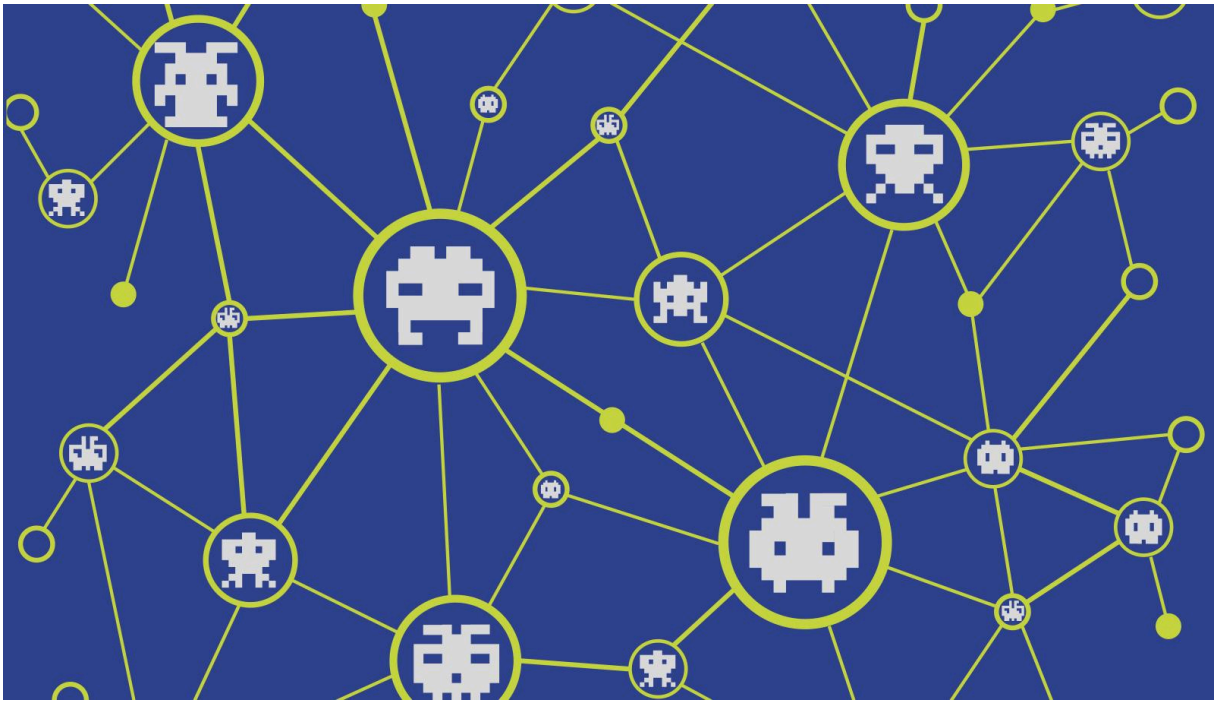
Spis treści

Wstęp

Prezes Urzędu Komunikacji Elektronicznej zobligowany przepisami ustawy o Prawie Telekomunikacyjnym publikuje drugą uaktualnioną wersję podręcznika opublikowanego w 2014 roku. Jego celem jest uświadomienie odbiorcy o tym jak ważne obecnie jest bezpieczeństwo w sieci. Każdy użytkownik powinien zwrócić szczególną uwagę na to w jaki sposób powinien zachowywać się w cyberprzestrzeni, jak zabezpieczać swoje dane i urządzenia aby uniknąć cyberataków.

Podręcznik składa się z pięciu rozdziałów, w których znajdują się ważne informacje dotyczące mechanizmów zagrożeń, konsekwencji skutecznych cyberataków i sposobów zabezpieczenia swoich urządzeń i systemów komputerowych. Przywołanie w treści wielu przykładów uświadamia odbiorców o tym, że w łatwy sposób mogą stać się ofiarami cyberprzestępców. Zapoznanie się z zagrożeniami, a następnie z zestawem informacji dotyczących najważniejszych technik zabezpieczenia komputerów, przeglądarek internetowych czy urządzeń mobilnych zwiększy odporność na wszelkiego rodzaju podatności. Praktyczne wskazówki opisane w zrozumiały sposób pomogą każdemu użytkownikowi wprowadzić zmiany, które poprawią jego bezpieczeństwo.

Poradnik nie zawiera wszystkich przykładów, zasad i porad dotyczących bezpiecznego korzystania ze środków komunikacji elektronicznej w cyberprzestrzeni. Urząd Komunikacji Elektronicznej planuje dalsze prace nad jego rozwojem. Jeżeli chciałbyś zgłosić swoje uwagi dotyczące treści tej edycji poradnika oraz tego o co powinien zostać rozbudowany w przyszłości, to prześlij swoją opinię na adres email: uke@uke.gov.pl z tytułem maila „Poradnik bezpieczeństwa w cyberprzestrzeni – uwagi".



1 Ogólna charakterystyka zagrożeń w cyberprzestrzeni i ich potencjalne skutki

Nasza codzienna obecność w cyberprzestrzeni, bez względu na to z jakich usług korzystamy, oprócz wymiernych, niewątpliwych korzyści niesie za sobą zagrożenia. Cyberprzestrzeń stała się miejscem bardzo aktywnych działań przestępczych. Masowość niektórych usług sprawia, że pewne metody ataku mogą mieć bardzo szerokie oddziaływanie i w rezultacie przynieść przestępcom ogromne zyski. W sposób oczywisty każdy internauta jest na nie narażony. Na szczęście większość z ataków, ze względu na swój masowy charakter, jest udanych tylko wtedy kiedy Twój komputer nie posiada podstawowych, rekomendowanych metod zabezpieczeń. Dlatego warto zainteresować się bezpieczeństwem swojego komputera i sprawić aby w wyniku kilku podstawowych czynności znaleźć się poza grupą największego ryzyka.

Poradnik ten powstał w celu zapoznania internautów z potencjalnymi zagrożeniami jakie wynikają z korzystania z usług dostępnych w Internecie i konsekwencjach braku lub nieodpowiedniego zabezpieczenia urządzeń. Czytelnik znajdzie w nim rekomendowane środki ostrożności oraz najbardziej popularne sposoby zabezpieczania urządzeń i programów, dzięki czemu będzie mógł zminimalizować czyhające na niego niebezpieczeństwa.

„Jednym z najczęstszych zdarzeń są skuteczne ataki pozwalające przejąć kontrolę nad komputerem.”

Przypadek 1 – pobranie pliku z nieznanego źródła

Pan Kowalski planuje założyć firmę. W internecie znalazł wiele porad jak się do tego przygotować. Jednym z kroków jest odpowiednie wypisywanie faktur, a że nigdy wcześniej tego nie robił postanowiła poszukać szczegółowych informacji na ten temat w internecie. Przeglądając przykładowe szablony faktur, jedna szczególnie go zainteresowała więc postanowił ją pobrać. Nie sprawdził on jednak źródła strony internetowej. Zwrócił jedynie uwagę że jest to format obsługiwany przez jego komputer i oprogramowanie biurowe. Zadowolony ze udało mu się znaleźć dokładnie taki dokument jakiego poszukiwał przystąpił do dalszego planowania swojego biznesu. Niestety jeszcze tego samego dnia nie mógł zalogować się na żadną z platform, z których korzystał, a jego komputer działał bardzo wolno.

„Intensywnemu korzystaniu z serwisów społecznościowych towarzyszą zagrożenia przejęcia kontroli nad kontami użytkowników."

Przypadek 2 – sensacyjna wiadomość w serwisie społecznościowym

Pani Kowalczyk aktywnie udziela się w mediach społecznościowych i udostępnia każdą ważną chwilę na swojej tablicy. Podczas wstawiania postu otrzymała wiadomość od znajomego o treści „Cześć, nie wiem czy wiesz ale na tej stronie, ktoś wrzucił Twoje przerobione zdjęcia, nie wygląda to dobrze". Przerażona Pani Kowalczyk bez zastanowienia kliknęła w link podany na stronie. W celu odblokowania zdjęcia podała swoje dane do logowania oraz numer telefonu aby uzyskać PIN z kodem. Wpisując przesłany kod do formularza Pani Kowalczyk wyraziła zgodę na usługę SMS premium. Na profilu Pani Kowalczyk zaczęły pojawiać się wpisy, których nie była autorem, a rachunek za telefon był kilkukrotnie wyższy niż zwykle.

„Bezpieczeństwo naszych pieniędzy w czasach coraz powszechniejszego dostępu do kont internetowych dla każdego z nas staje się priorytetem. Często nierozważne zachowania sieciowe kończą się poważnymi konsekwencjami i utratą środków finansowych."

Przypadek 3 – przelew weryfikacyjny

Pan Nowak przeglądając oferty pracy znalazł ogłoszenie, które wydawało mu się szczególnie interesujące. Była to oferta pracy idealnie pasująca do jego kwalifikacji. Szczególną ciekawość wzbudziło w nim wynagrodzenie oferowane za prace na danym stanowisku. Nie zastanawiając się szybko przesłał swoje zgłoszenie. Po chwili otrzymał wiadomość zwrotną od „osoby rekrutacyjnej" z prośbą wykonania przelewu weryfikacyjnego na 1zł. Niska kwota przelewu nie wzbudziła w Panu Nowaku jakichkolwiek podejrzeń co w perspektywie przyszłych wysokich zarobków nie stanowiło dla niego problemu. Po wykonaniu przelewu kontakt ten niestety się urwał. W tym czasie cyberprzestępcom udało się założenie konta w innym banku na dane Pana Nowaka, co w następstwie zostało wykorzystane do wyłudzania pożyczek i praniu brudnych pieniędzy.

Przypadek 4 – ważna wiadomość od operatora telekomunikacyjnego

Pan Lewandowski dostał wiadomość mailową od swojego operatora telekomunikacyjnego. Jak każdego miesiąca była to faktura. Bez zastanowienia rozpoczął proces opłaty faktury na wskazany w mailu numer konta bankowego. Jednak po kilku dniach dostał kolejną wiadomość z fakturą na inna kwotę. Doszedł do wniosku że musiało dojść do jakiejś pomyłki ze strony operatora. Niestety w kolejnych dniach dostał kilka wiadomości z prośbą o wpłacenie należności. Sprawdzając wszystkie maile oraz konto bankowe zorientował się że pozornie identycznie wyglądająca wiadomość z fakturą zawierała fałszywe dane do przelewu, a tym samym stał się ofiarą przestępstwa i utracił swoje pieniądze.

„Nierozważne i pochopne działania, które z pozoru mają poprawić nasze bezpieczeństwo, również bywają metodą ataku. Cyberprzestępcy odwołują się w czasie tych ataków do znanych powszechnie symboli bezpieczeństwa takich jak certyfikat czy antywirus."

Przypadek 5 – aplikacja zwiększająca bezpieczeństwo

Pan Dąbrowski usłyszał od znajomych, że warto dbać o swoje bezpieczeństwo w sieci. Tym bardziej wzbudziła w nim ciekawość wyświetlona reklama dotycząca darmowego konta klienta VPN. Zachęcony opisem, że zwiększy to jego bezpieczeństwo i prywatność w sieci, a co więcej umożliwi szyfrowanie połączenia, bez dłuższego namysłu pobrał aplikacje. Zadowolony pochwalił się swoim znajomym ze udało mu się znaleźć świetną aplikację. Niestety dobre samopoczucie nie trwało długo. W krótkim czasie zorientował się, że aplikacja pozornie mająca zwiększyć jego bezpieczeństwo spowodowała utratę dostępu do kont bankowych, a co gorsza upływ środków pieniężnych.

Przypadek 6 – nowe oprogramowanie antywirusowe

Pan Wójcik był lekko przerażony kiedy w czasie surfowania po Internecie nagle na w jego komputerze pojawiło się okienko informujące, że jego komputer został zainfekowany groźnym wirusem. Zaakceptował odpowiedni przycisk aby dowiedzieć się więcej. Czekały na niego dwie wiadomości – dobra i zła. Zła była taka, że wirusów było aż 3, dobra że uzyskał propozycję i możliwość darmowego przeskanowania swojego komputera i usunięcia wirusów. Rzeczywiście wirusy zostały usunięty, ale skaner wykrył kolejne kilkanaście wirusów. Ich usunięcie możliwe było tylko po zakupie licencji na pełną wersje oprogramowania antywirusowego. Z racji tego, że i tak przymierzał się do tego dokonał zakupu online korzystając ze swojej karty kredytowej. Jednak działanie programu antywirusowego nie spełniało jego oczekiwań – informacje o nowych wirusach i problemy z tym związane pojawiały się dalej, co gorsza na wyciągu z transakcji kartą kredytową pojawiły się nieautoryzowane transakcje.

Powyższe przykłady to kilka typowych historii, które zdarzają się internautom, a które związane są zagrożeniami w Internecie. Skonfrontuj je ze swoimi doświadczeniami i doświadczeniami swoich

znajomych. Być może odnajdziesz znane Ci historie. Spróbuj je na nowo przemyśleć i zapoznaj się dokładnie z zamieszczonymi w dalszej części poradnika opisami mechanizmów ataków stosowanych przez cyberprzestępców, skutkami tych ataków i najważniejszymi metodami obrony przed nimi.

2 Najważniejsze zagrożenia przy korzystaniu z usług telekomunikacyjnych w sieci Internet

2.1 Ataki na przeglądarki internetowe

2.1.1 Mechanizm zagrożenia

Przeglądarki internetowe są instalowane niemal na każdym komputerze, a obecnie stanowią najczęściej atakowaną aplikacje komputerową. Każda z przeglądarek korzysta z wielu wtyczek innych firm (tj. JavaScript, Flash, ActiveX). Wtyczki te często zawierają luki w zabezpieczeniach, które wykorzystywane są do uzyskania dostępu do systemów np. poprzez instalowanie oprogramowania ransomware, eksfiltrowanie danych, oprogramowanie szpiegujące aktywność. Do ataku dochodzi m.in. w sytuacji, która jest absolutnie naturalna dla korzystającego z przeglądarki, czyli w chwili odwiedzin strony internetowej. Jeśli otworzysz stronę, która zawiera samoczynnie uruchamiający się kod komputerowy (np.: komponent ActiveX lub aplet Java) i kod ten jest złośliwy, to Twój komputer może być zainfekowany. Do takiego ataku najczęściej dochodzi w sytuacji kiedy odwiedzasz niezaufane witryny sieciowe lub dasz się namówić na otwarcie linku zamieszczonego w wiadomości typu spam.

2.1.2 Skutki ataku

Skutki ataku zależą bezpośrednio od rodzaju złośliwego oprogramowania, które zostanie zainstalowane na Twoim komputerze. Przeglądarki to potężne, bogate w dane narzędzie, które zaatakowane mogą zapewnić cyberprzestępcy ogromną ilość informacji o Tobie, w tym adres, numer telefonu, dane kart kredytowych, e-maile, identyfikatory, hasła, historię

przeglądani itp.. To wszystko może doprowadzić do utraty dostępu do różnego rodzaju serwisów takich jak banki, portale społecznościowe, e-mail.

2.1.3 Porady jak się bronić

Jednym z najbardziej skutecznych metod ochrony przed atakami na przeglądarki, i atakami w ogóle, jest korzystanie z konta komputerowego z wyłączonymi prawami administracyjnymi. Praktyka wskazuje, że przy takich ustawieniach niezwykle rzadko dochodzi do skutecznego ataku na komputer. Dodatkowym ważnym i skutecznym sposobem obrony jest korzystanie z ostrzeżeń, które generują najbardziej popularne przeglądarki internetowe oraz informacji dotyczących bezpiecznego konfigurowania danej przeglądarki. Przy próbie wejścia na strony, które z bardzo dużym prawdopodobieństwem infekują komputery odwiedzających, przeglądarki wyświetlają specjalne strony, które przestrzegają przed takimi odwiedzinami. Tylko źle pojęta determinacja internauty i ominięcie tych ostrzeżeń prowadzi do odwiedzin takiej strony i niestety bardzo prawdopodobnej infekcji.

Również skuteczną, aczkolwiek nie dla wszystkich akceptowalną, metodą ograniczenia ryzyka skutecznego ataku na przeglądarkę internetową jest wyłącznie obsługi przez przeglądarkę elementów AciveX i apletów Java, przez które odbywa się większość ataków.

2.2Ataki na pocztę elektroniczną

2.2.1 Mechanizm zagrożenia

Bardzo często poczta elektroniczna wykorzystywana jest przez cyberprzestępców. W tym przypadku popularność zyskały ataki typu phishing. Jest to atak, w którym działanie intruza wsparte jest poprzez działanie ofiary. Intruz namawia swoją ofiarę do wykonania pewnej czynności w wyniku czego atakujący będzie w stanie osiągnąć swój cel. Najczęściej namawia do otwarcia załącznika dodanego do wiadomości. Taki załącznik zawiera w sobie złośliwe oprogramowanie, które jest uruchamiane wraz z jego otwarciem. Używanymi formatami plików w takich atakach są formaty związane z popularnymi aplikacjami takimi jak czytniki tekstów czy pakiety biurowe (doc, docx, pdf). Otwarciu tych drugich często towarzyszy dodatkowa prośba o zaakceptowanie użycia tzw. makr. Przestępcy są na tyle zdeterminowani, że podszywają się pod znane firmy i instytucje aby nakłonić użytkowników np. do opłaty faktury na podmieniony numer konta.

2.2.2 Skutki ataku

Po zainstalowaniu złośliwego oprogramowania możliwe jest, że intruz w praktyce przejmuje kontrolę nad komputerem. Jest w stanie wykradać z niego używane przez

internautę hasła, wykradać dane zawarte w plikach znajdujących się na komputerze, używać przejętego komputera w ataku na inne komputery, w roli stacji przesiadkowej czy też stać się komputerem zombie, który został fragmentem tzw. botnetu. W niektórych przypadkach takie ataki skutkują utratą pieniędzy.

2.2.3 Porady jak się obronić

Najskuteczniejszą metodą obrony przed tymi atakami jest nieotwieranie załączników, przesłanych od podejrzanych nadawców, szczególnie jeśli są spersonalizowane. Ponad to należy pamiętać o uważnym przeczytaniu maila i zachować czujność gdy:

- Wiadomość zawiera szczegółowe instrukcje dalszego postępowania, np.: „otwórz załącznik".
- Wiadomość w swej treści, lub poprzez wyraźne wskazanie, zawiera zachętę do szybkiego działania, gdyż zwłoka może spowodować problemy, np.: może nastąpić blokada konta, egzekucja długu, wstrzymanie świadczenia usługi, itp. Działanie pod presją ma Cię zmusić do popełnienia błędu.
- Wiadomość często zawiera błędy ortograficzne lub gramatyczne, jest napisana nieskładnie i niechlujnie, w wyjątkowych sytuacjach jest napisana z wykorzystaniem automatycznego tłumaczenia treści na język polski, co akurat czyni ją na tyle niewiarygodną, że w praktyce odsuwa groźbę skutecznego ataku.
- Wiadomość przesłana od znanej nam firmy/instytucji nie zawiera logo i zdjęć bądź wyglądają inaczej inaczej niż do tej pory, w dodatku dotyczą kwestii finansowych. Może to być przykład wyłudzenia pieniędzy.
- Atakujący w swoim mailu prosi o dane, do których nie powinien mieć dostępu. Klasycznym przykładem jest próba wymuszenia podania hasła lub niektórych danych osobowych.

Dodatkowo aby nie dopuścić do automatycznej infekcji poprzez pocztę elektroniczną warto:

- Wyłączyć autopodgląd otrzymywanych informacji, co uniemożliwi automatyczny ich odczyt i wykonanie złośliwego kodu, w sytuacji kiedy email takowy zawiera.
- Wyłączyć obsługę Java i HTML, których wykonanie może również skutkować w infekcji złośliwym kodem.

Oprócz podstawowej porady nieotwierania załącznika, aby obronić się przed tego typu atakiem, warto również pamiętać o aktualizacji swojego systemu operacyjnego i aplikacji oraz wyłączeniu niepotrzebnych w systemie opcji, np.: obsługi makr czy języka JavaScript. Zupełnym minimum jest posiadanie oprogramowania antywirusowego, które jest w stanie wykryć jako niebezpieczne większość załączników zawierających wirusy komputerowe.

Jedną z powszechniejszych metod inicjacji ataku jest dotarcie do przyszłej ofiary poprzez pocztę elektroniczną. Cyberprzestępcy robią to głównie poprzez rozsyłanie spamu. Spam rozsyłany jest do osób, których adresy emailowe zostały pozyskane i dołączone do list wykorzystywanych przez spamerów. Dlatego ważne jest aby korzystać z kilku podstawowych porad ograniczających możliwość dołączenia swojego adresu email do takich list. Te porady są następujące:

- Nie odpowiadaj nigdy na spam przesłany do Ciebie – taka odpowiedź to najlepsze potwierdzenie poprawności Twojego adresu email.
- Jeśli swój adres email umieszczasz w Internecie to nie zapisuj go w pełnej postaci, a w takiej która będzie niemożliwa lub trudna do przeczytania przez automaty, które spamerzy wykorzystują w zbieraniu adresów emailowych. Zamiast zapisywać adres w postaci jan.kowalski@adresinternetowy.pl zapisz go na przykład jako „jan.kowalski at adresinternetowy kropka pl". Wszyscy zainteresowani, w odróżnieniu do automatów, sobie poradzą.
- Jeśli do Twojej skrzynki przedostał się spam spróbuj jego próbką „zasilić" swój mechanizm antyspamowy, np.: poprzez dodanie adresu spamera do listy tych, od których nie chcesz dostawać korespondencji.
- W korespondencji skierowanej do dużej grupy odbiorców stosuj funkcję „ukrytej kopii" to zarówno dobra praktyka netykiety sieciowej jak i metoda uniknięcia narażenia wszystkich tych adresów na dodanie do list spamerskich w sytuacji przejęcia takiej korespondencji.

2.3 Ataki na systemy operacyjne i aplikacje komputerowe

2.3.1 Mechanizm zagrożenia

Cyberprzestępcy bardzo chętnie przygotowując swoje ataki kierują je na systemy operacyjne i aplikacje, które są w grupie tych najbardziej popularnych. Działa tu prosta zasada efektywności podejmowanych wysiłków. Opracowanie skutecznej metody ataku na bardzo popularny system lub aplikację daje potencjalnie znacznie większe korzyści. Mnogość skutecznych ataków na wybrany system operacyjny czy aplikację nie należy kojarzyć bezkrytycznie ze słabością tego rozwiązania.

Opracowanie ataku polega na znalezieniu słabości systemu operacyjnego lub aplikacji i opracowania specjalnego programu, który będzie w stanie taką słabość wykorzystać. Mówi się wtedy, że system lub aplikacja posiada „dziurę". Taka „dziura" staje się miejscem w systemie komputerowym poprzez który atakujący może dostać się do jego środka.

2.3.2 Skutki ataku

Celem atakującego jest zdobycie jak największych uprawnień w zaatakowanym

systemie. Jest on wtedy w stanie zrobić praktycznie dowolną czynność. Często zdarza się że może wykorzystać taki system do ataku na inne, aby ukryć prawdziwą tożsamość atakującego. Ta metoda jest na przykład powszechnie stosowana przy dystrybucji materiałów zawierających nielegalne treści (np.: pornografii z udziałem dzieci). Chroniąc swój system bronisz nie tylko ten system, ale w praktyce również pośrednio inne systemy, co więcej unikniesz kłopotów związanymi z odpowiedzialnością za udział w ataku na innych.

Najczęściej występującymi skutkami ataków na systemy operacyjne i aplikacje są:

- Kradzież danych znajdujących się na zaatakowanym komputerze.
- Wykorzystanie przejętego komputera do ataków na inne systemy, np.: poprzez budowanie tzw. Botnetów, wykorzystanie ich w atakach typu DDoS (Distributed Denial of Service) czy rozsyłaniu spamu.

2.3.3 Porady jak się obronić

Najskuteczniejszą i jednocześnie konieczną metodą ochrony przed atakami na systemy operacyjne i aplikacje komputerowe jest dbanie o to, aby były one zaktualizowane. Systemy i aplikacje posiadają mechanizmy automatycznej aktualizacji, które w sposób ciągły sprawdzają dostępność nowych „łat" pobierają je i instalują na komputerze. Ta ostatnia czynność, czyli instalacja, w większości przypadków nie jest uruchamiana automatycznie lub jest uruchamiana w tym trybie tylko po upłynięciu pewnego czasu. Wymaga ona akceptacji przez użytkownika. Bardzo ważne jest aby takiej zgody na instalację poprawek bezpieczeństwa udzielać najszybciej jak się da. Dzięki temu usuwamy się z listy, tych którzy na taki atak są podatni. W praktyce eliminuje to ryzyko skutecznego ataku automatycznego. Jeśli Twój system lub aplikacja nie aktualizuje się automatycznie to należy systematycznie sprawdzać dostępność „łat" dla danego systemu. Optymalną częstotliwością aktualizacji jest: raz w tygodniu dla aplikacji, z których korzystasz codziennie i raz na miesiąc dla pozostałych.

2.4Ataki w mediach społecznościowych

2.4.1 Mechanizm zagrożenia

Media społecznościowe obecnie stanowią nieodłączny element aktywności w internecie. Gromadzą miliardy użytkowników, dlatego w sposób oczywisty stały się polem zainteresowania cyberprzestępców. W tym przypadku wykorzystują oni coraz większy wachlarz możliwości. Oprócz ataków socjotechnicznych, cyberprzestępcy korzystają ze złośliwego oprogramowania, luk w bezpieczeństwie czy phishing po to, aby zdobyć dane dostępne w mediach społecznościowych. Najczęściej spotykane ataki socjotechniczne polegają na namówieniu

użytkownika serwisu do wykonania pewnej czynności, która w rezultacie obróci się przeciwko niemu. Zazwyczaj jest to akceptacja przez użytkownika pewnego działania aplikacji, podanie własnych danych, czasami nawet podanie loginu i hasła do podstawionego fałszywego systemu uwierzytelnienia lub przesłanie nowego hasła na prośbę atakującego. Wówczas najczęściej wygląda to tak, że atakujący przesyła fałszywego emaila z linkiem do systemu i prosi w takiej wiadomości o ustawienie nowego hasła, co oczywiście podyktowane jest „zasadami bezpieczeństwa". Namówienie odbywa się z wykorzystaniem skłonności użytkownika do zapoznania się z potencjalnie bardzo ciekawą dla niego informacją, np.: sensacyjna informacja polityczna, społeczna czy obyczajowa. Chęć szybkiego dotarcia do takiej informacji zabija czujność i powoduje szybką zgodę na przekazanie własnych danych lub uruchomienie nieznanej aplikacji. Skutki tego działania bywają widoczne od razu, np.: publikacja kompromitującej informacji na własnym profilu lub przeciwnie utrzymywane są w ukryciu, tak aby nie wzbudzać podejrzeń i móc możliwe długo korzystać z przejętych danych lub działania złośliwego kodu.

2.4.1 Skutki ataku

Są dwa podstawowe skutki ataków na serwisy społecznościowe – przejęcie danych osobowych użytkownika i przejęcie kontroli nad jego kontem. To pierwsze może posłużyć do najróżniejszych celów związanych z atakiem na tożsamość użytkownika. Co ciekawe może być dopiero przygrywką do prawdziwego, dedykowanego ataku na użytkownika, w którym zdobywa się jego wyjątkowe zaufanie w związku z faktem posiadania wielu poufnych informacji o ofierze.

Przejęcie kontroli nad kontem służy zazwyczaj do ataków wymierzonych w reputację ofiary. Publikowane są na nim kompromitujące informacje. Czasami ataki takie kończą się publikacją informacji lub przesłaniem wiadomości z pozoru wiarygodnych, które mają wywołać określone skutki. Na przykład może to być wiadomość o tym, że nasz znajomy lub członek rodziny znalazł się w trudnej sytuacji i potrzebna jest mu natychmiastowa pomoc w postaci przekazania środków pieniężnych. W przypadku osób wpływowych np.: dziennikarzy, ekspertów czy polityków, publikacja wiadomości ma wywołać poważne działania typu dalsze rozgłaszanie nieprawdziwej informacji czy ruchy o konsekwencjach finansowych (np.: związane z inwestycjami na rynkach finansowych).

2.4.2 Porady jak się obronić

Zdecydowanie najlepszą formą obrony przed atakami w mediach społecznościowych jest zachowanie czujności poprzez wcześniejsze zweryfikowanie źródła informacji czy nie uleganie namowom do wykonywania podejrzanych czynności. Warto pamiętać przy tej okazji również o silnym haśle, a co więcej o unikaniu użycia tego samego hasła na wielu platformach. Ważne jest również, aby nie instalować bezmyślnie nieznanych aplikacji, nie klikać

w podejrzane wiadomości, nawet w te przesłane od bliskich znajomych, które często związane są z sensacyjnymi informacjami. Zaleca się podejrzliwie spoglądać na przychodzące e-maile (rzekomo od administracji serwisów społecznościowych), gdyż mogą one zawierać linki do złośliwego oprogramowania. Również wiadomości, które pojawiają się na Twoim profilu, a dotyczą ofert pracy czy atrakcyjnych transakcji, powinny być traktowane z odpowiednią dozą podejrzliwości, tym bardziej jeżeli wymagają przelewu weryfikacyjnego. Proste sprawdzenie w wyszukiwarce czy oferta, która trafiła do Ciebie nie jest internetowym scamem może szybko wyjaśnić sytuację. Warto regularnie aktualizować zabezpieczenia na kanałach cyfrowych i społecznościowych, w tym ograniczyć zgodę na dostęp do swoich danych dla wszystkich aplikacji, które o taką zgodę zwracają się do Ciebie. Nawet jeśli są dla Ciebie wiarygodne i znane. Jeśli serwis społecznościowy oferuje dwuczynnikowe uwierzytelnienie to powinieneś z niego skorzystać.

2.5Ataki na urządzenia mobilne

2.5.1 Mechanizm zagrożenia

Urządzenia mobilne dla wielu internautów stały się podstawowym urządzeniem dostępu do Internetu. Z racji tego, że posiadasz smartfona czy tableta prawie cały czas przy sobie to przechowujesz na nim najbardziej przydatne i istotne informacje. Właśnie ta sytuacja sprawia, że Twoje urządzenie mobilne jest szczególnym obszarem zainteresowania cyberprzestępców. Najgroźniejsze ataki na urządzenia mobilne odbywają się przez instalację na Twoim urządzeniu aplikacji zawierających złośliwe oprogramowanie. Takie aplikacje mogą trafić na urządzenie poprzez różne kanały dystrybucji. Najbardziej popularne z tych kanałów to:

- Internetowe sklepy z aplikacjami, w których cyberprzestępcy umieszczają programy zawierające złośliwy kod. Jeśli właściciele sklepu nie zadbają o szczegółową kontrolę zamieszczanych w nim aplikacji to dochodzi do takiego właśnie zagrożenia. Co więcej – zdarza się, że złośliwe oprogramowanie jest przedstawiane jako rozwiązanie o właściwościach dokładnie odwrotnych – na przykład jako program antywirusowy na telefon komórkowy.
- Niezaufane witryny internetowe oferujące oprogramowanie na urządzenia mobilne – np.: gry czy aplikacje użytkowe.
- Linki zawarte w SMS-ach. Takie SMS-y mają charakter reklamy „atrakcyjnych produktów” lub informacji o konieczności instalacji elementów poprawiających bezpieczeństwo – np.: instalacji certyfikatu pozwalającego na dostęp do usług bankowych.

Ważne jest również abyś zadbał o zasady prywatności dotyczące Twojego urządzenia mobilnego. Jest ono wyposażone w mechanizmy, które pozwalają na ustalenie wielu informacji na Twój temat, którymi z pewnością nie chciałbyś się dzielić z innymi bez kontroli. Sama lista wykonanych połączeń

telefonicznych może być informacją poufną. Ale to nie wszystko. Większość urządzeń mobilnych jest dziś wyposażona w moduł GPS. Na co dzień bardzo przydatny, na przykład przy odnajdowaniu celów podróży, stanowi jednak również zagrożenie. Bez odpowiedniej kontroli może informować o Twoim położeniu. Jeśli na przykład pozwalasz na to, aby program do robienia zdjęć Twoim smartfonem mógł dołączać do nich informację o miejscu ich wykonania, a później sam publikujesz te zdjęcia w sieci, to zdradzasz bardzo precyzyjnie miejsce swojego pobytu. Ryzykowne jest również korzystanie z darmowych i otwartych punktów dostępu Wi-Fi. Punkty te często są niezabezpieczone i mogą ułatwić hakowanie urządzeń mobilnych w tym kont w mediach społecznościowych, PayPal, a nawet rozmowy VoIP.

2.5.2 Skutki ataku

Skutki ataku na urządzenie mobilne są zazwyczaj bardzo poważne. Atakujący przejmuje kontrolę nad całością urządzenia lub częścią jego funkcji. Dzięki temu może na przykład wysyłać SMS-y obciążające Twój rachunek za telefon, albo przechwytywać bez Twojej wiedzy kody potwierdzające operacje bankowe, które przy jednoczesnym zdobyciu danych dostępu do Twojego konta bankowego mogą być wykorzystywane do kradzieży pieniędzy. W wyniku cyberataku może dochodzić również do wykradania wszelkich poufnych informacji, które przechowujesz na swoim urządzeniu. Biorąc pod uwagę, że „przy sobie" lubimy mieć naprawdę bardzo istotne informacje, to taki atak może mieć bardzo poważne skutki związane z utratą prywatności.

2.5.3 Porady jak się obronić

Najważniejsza metodą obrony przed negatywnymi konsekwencjami ataków na urządzenia przenośne jest zadbanie o to aby nie znalazły się na nim programy zawierające złośliwe oprogramowanie. Kieruj się poniższymi zasadami jeśli chcesz poprawić bezpieczeństwo korzystania z urządzenia mobilnego:

- W szczególny sposób uważaj na to, co instalujesz na swoim smartfonie lub tablecie. Powinieneś posiadać oprogramowanie antywirusowe, które będzie kontrolowało Twoje instalacje.
- Instaluj tylko te aplikacje, do których masz zaufanie. Takie, które pochodzą z legalnego i sprawdzonego źródła. Wszelkie „atrakcyjne" nowości są w grupie podwyższonego ryzyka.
- Jeśli nie jesteś pewien aplikacji, a bardzo Ci na niej zależy, to zrób swoje własne rozeznanie w sieci, aby sprawdzić czy jest ona bezpieczna. Prawie na pewno znajdziesz ostrzeżenie przed jej instalacją, jeśli nie jest bezpieczna.
- Nie daj się namówić na szybkie działanie i instalacje programów, które ktoś Ci podsunął „ze względów bezpieczeństwa". Sprawdzaj źródło takiej porady. Jeśli na przykład taka informacja

przedstawiana jest jako pochodząca od banku, to zanim zainstalujesz „certyfikat bezpieczeństwa" skontaktuj się z bankiem i zweryfikuj informację. Swoją drogą takie działanie pomoże nie tylko Tobie, ale i innym klientom banku, których to po Twoim zgłoszeniu bank będzie mógł ostrzec o nowym zagrożeniu.

Pamiętaj też o mechanizmach naruszających Twoją prywatność. Aby lepiej ją chronić zastosuj kilka ważnych zasad:

- Świadomie udzielaj zgody poszczególnym aplikacjom na dostęp do informacji o Twoim położeniu, dostępie do listy adresowej kontaktów, wykonanych połączeniach czy innych miejsc w telefonie, w których przechowujesz prywatne dane.
- Raz na miesiąc dokonaj dokładnego przeglądu aplikacji, którym pozwalasz na dostęp do danych o Twojej lokalizacji. Czasami działając szybko nieopatrznie udzielasz takiej zgody – warto to zweryfikować.
- Dokonuj przeglądu aplikacji na swoim urządzeniu. Te, z których nie korzystasz usuń.
- Koniecznie aktualizuj system operacyjny i aplikacje na Twoim urządzeniu mobilnym. Pamiętaj, że urządzenia mobilne nie posiadają mechanizmów automatycznej aktualizacji. Musisz zrobić to ręcznie, dlatego raz na tydzień sprawdzaj czy nie ma nowszych wersji systemów i aplikacji, które masz zainstalowane.
- Unikaj korzystania z darmowego i otwartego punktu dostępu Wi-Fi.

3 Najbardziej popularne i skuteczne sposoby zapewnienia bezpieczeństwa w cyberprzestrzeni

3.1 Hasła

Hasła od zawsze były podstawowym narzędziem ochrony dostępu. Tak jest i dzisiaj. Praktycznie wszystkie serwisy sieciowe i zasoby własne posiadają funkcję, w większości wymaganą, ochrony dostępu poprzez hasło. Należy ją bezwzględnie stosować. Jednak zwykłe stosowanie hasła to nie wszystko. Jeśli nie zastosujemy kilku ważnych zasad to hasło z bardzo ważnego i skutecznego narzędzia ochrony może przerodzić się w jego najsłabszy punkt. Dlatego należy pamiętać o następujących zasadach stosowania hasła:

- Konieczne jest stosowanie tzw. silnego hasła. Wiąże się to ze stosowaniem w nim różnej kategorii znaków – małych i wielkich liter, cyfr, znaków specjalnych. Dodatkowo wymagane jest stosowanie hasła o minimalnej długości i odpowiednio często zmienianego. Wszystko to powoduje, że stajesz przed bardzo trudnym zadaniem. Wielu z internautów nie radzi sobie z nim i kończy się to stosowaniem haseł, które jednocześnie są zapisywane na kartce lub na pulpicie komputera i łatwo mogą wpaść w ręce niepowołanej osoby. Ale jest dobra informacja. Obecnie praktycznie wszystkie systemy i serwisy pozwalają na wprowadzanie bardzo długich haseł (zazwyczaj o długości do 128 znaków). Dlatego możesz zastosować hasło, które jest wybraną frazą lub całym zdaniem, np.: „W Szczebrzeszynie chrząszcz brzmi w trzcinie”. Z pewnością je z łatwością zapamiętasz a jednocześnie będzie ono wystarczająco trudne do odgadnięcia.
- Niezwykle ważne jest aby stosować różne hasła do różnych serwisów. Szczególnie ważne jest to aby najważniejsze serwisy, na przykład do usług finansowych lub zawierające wrażliwe dane

osobowe, miały swoje oddzielne dedykowane hasła. Hasła i inne dane do logowania są bardzo często wykradane przez cyberprzestępców bezpośrednio z serwisów świadczących usługi. Czasami są one publikowane w Internecie. Jeśli w ten sposób przejęte będzie Twoje hasło do któregoś z serwisów, a stosujesz je również w innych serwisach, to automatycznie narażony jesteś na to, że cyberprzestępcy uzyskają łatwy dostęp do tych zasobów.

- Odpowiednio zmieniaj swoje hasło w swoich serwisach. Nie obawiaj się - nie musisz robić tego zbyt często. To bardzo kłopotliwe i prowadzi do porzucenia tej ważnej czynności. Podziel sobie swoje konta dostępu na te bardzo ważne – zawierające istotne dane i te mniej ważne, do których włamanie nie będzie dla Ciebie wiązało się z poważnymi problemami. W pierwszych zmieniaj hasło minimum raz na kwartał – w drugich raz na rok.
- Przy mnogości różnych serwisów i kont z pewnością posiadasz kilka jeśli nie kilkanaście kont. Jeśli naprawdę posiadasz ich dużo i masz kłopot z ich zapamiętaniem to zastosuj menadżer haseł. To prosta aplikacja, w której możesz składować swoje hasła. Ty natomiast potrzebujesz zapamiętać wtedy tylko jedno główne hasło właśnie do tej aplikacji. Dobry menadżer hasła potrafi nie tylko zapamiętać Twoje hasło, ale również sam je automatycznie składować jeśli je po raz pierwszy ustanawiasz (np.: w nowym serwisie) i sam je wpisywać wtedy kiedy na to pozwolisz. Choć z tą drugą zasadą warto uważać i dla najważniejszych serwisów, które powinny być najlepiej chronione, zawsze najlepiej samemu wpisywać hasło. Jest wiele menadżerów haseł. Są to programy płatne i bezpłatne. Te drugie potrafią być wystarczająco dobre. Jeśli chcesz znaleźć ciekawe propozycje wpisz w wyszukiwarkę internetową następujące wyrazy: „darmowy menadżer haseł".

  Wśród popularnych narzędzi można wymienić:

  - Funkcje zapamiętywania haseł wbudowane w przeglądarki - Google Chrome, Mozilla, Firefox, Internet Explorer. We wszystkich zapamiętane hasła mogą być dodatkowo chronione "hasłem głównym" - należy z tej funkcji korzystać, inaczej dowolny wirus będzie mógł za jednym zamachem ukraść wszystkie hasze hasła. Przeglądarki zapamiętają tylko hasła do aplikacji webowych.
  - LastPass - program zintegrowany z większością przeglądarek, o bardzo rozbudowanych funkcjach bezpieczeństwa. Może zapamiętywać dowolne hasła i notatki.
  - KeePass - otwarte oprogramowanie pozwalające na edytowanie i bezpieczne przechowywanie listy haseł w zaszyfrowanym pliku, ale nie zintegrowane z przeglądarkami. Może zapamiętywać dowolne hasła i notatki.
  - KeePassX - wersja dostępna dla Linuks, MacOS i Windows

3.2 Oprogramowanie antywirusowe

Posiadanie oprogramowania antywirusowego jest konieczne. Stało się ono jednym z podstawowych elementów ochrony komputera przed atakami sieciowymi. Podejmując wybór dotyczący programu antywirusowego można skorzystać z jednego z wielu dostępnych rozwiązań komercyjnych. Również darmowe programy antywirusowe wykazują dużą skuteczność. Nie ma jednego najlepszego programu antywirusowego. Wiele rankingów wskazuje na różne rozwiązania. Jeśli jesteś zainteresowany darmowym programem antywirusowym możesz wpisać w wyszukiwarkę „ranking darmowych antywirusów". Wyniki wyszukiwania skierują Cię do wielu pozycji rekomendujących dobre programy. Możesz również skorzystać z propozycji darmowych programów antywirusowych przedstawionych poniżej.

Dodatkowo przy korzystaniu z programu antywirusowego trzeba pamiętać o:

- Ciągłej aktualizacji bazy wirusów komputerowych, co pozwoli na wykrywanie kolejnych mutacji lub zupełnie nowych rodzajów wirusów. Sam program antywirusowy również powinien być aktualizowany. Najlepiej jedno i drugie ustawić jako funkcje automatycznej aktualizacji i nigdy nie zwlekać jeśli taka aktualizacja wymaga potwierdzenia z Twojej strony.
- Korzystaniu tylko z jednego programu antywirusowego, gdyż działanie więcej niż jednego programu na jednym komputerze może spowodować zakłócenia.
- Instalacji oprogramowania tylko ze sprawdzonych źródeł. Cyberprzestępcy potrafią podsunąć Ci do instalacji program, który tylko z pozoru jest programem antywirusowym, a w rzeczywistości sam infekuje Twój komputer. Nigdy nie reaguj na komunikaty antywirusowe z nieznanego Ci źródła – to może być próba oszustwa i prowadzić do infekcji Twojego komputera.
- Warto mieć taki program antywirusowy, który potrafi również skanować dołączane do Twojego komputera zewnętrzne nośniki pamięci, np.: na pendrivach.
- Nie używaj na stałe wersji demonstracyjnych i testowych. Testowe (evaluation, trial) wersje nawet najlepszych antywirusów po okresie testowym często wyłączają funkcje aktualizacji. Antywirus bez aktualizacji jest bezużyteczny. Jeśli nie możesz kupić pełnej wersji, wybierz produkt, który z założenia jest darmowy. Jeśli podejmujesz decyzję o zakupie, kieruj się wynikami niezależnych testów skuteczności, np. AV Comparatives, AV-Test, Virus Bulletin.
- Darmowe, w pełni funkcjonalne antywirusy to na przykład Microsoft Security Essentials, Avira, Agnitum, BitDefender, ClamAV , Avast[1].

[1] Przykłady programów antywirusowych oraz znajdująca się nad nimi porada dotycząca wersji demonstracyjnych i testowych,pochodzą z publikacji: „Bezpieczeństwo informatyczne szkół i instytucji publicznych – poradnik".

3.3Tworzenie kopii zapasowych (backup danych)

Nie ma chyba osoby, która w swoich doświadczeniach z komputerem przynajmniej raz nie znalazła się w tej bardzo kłopotliwej i nieprzyjemnej sytuacji związanej z utratą danych. Taka sytuacja to najlepszy motywator do rozpoczęcia regularnego tworzenia kopii zapasowych swoich danych (ang. backup). Zacznij go robić zanim trafi Ci się naprawdę poważna historia z utratą danych, która będzie Cię drogo kosztowała. Backup danych powinieneś robić wg ustalonego planu oraz dodatkowo w niektórych sytuacjach związanych z użytkowaniem Twojego komputera. Kieruj się przy tym kilkoma ważnymi zasadami:

- Wykonaj backup kiedy szykujesz się do istotnych zmian na swoim komputerze, na przykład zamierzasz robić w nim „porządki" usuwać wiele plików i programów.
- Twórz kopie danych również wtedy kiedy zamierzasz robić reinstalację swojego komputera.
- Pamiętaj abyś robił backup na inny nośnik niż dysk twardy Twojego komputera. Do tego najlepiej nadaje się nośnik zewnętrzny – np.: dedykowany dysk twardy, który na czas backupu dołączasz do swojego komputera lub wydzielone zasób sieciowy, np.: dysk na serwerze sieciowym lub przydzielony Ci fragment dysku w tzw. chmurze, na którym możesz składować swoje dane.
- Idealnie jest jeśli możesz wykonać backup na więcej niż jednym nośniku zewnętrznym, przynajmniej tych najbardziej istotnych danych. Każdy nośnik może ulec uszkodzeniu, takie zabezpieczenie jeszcze bardziej zminimalizuje ryzyko całkowitej utraty danych.
- Miejsce składowania Twoich danych dopasuj do ich poufności. Dane, które chcesz aby pozostały poufne najlepiej składować na nośniku, nad którym masz pełną kontrolę. Dla takich danych rozważ możliwość ich zaszyfrowania.

Zastanawiasz się co tak naprawdę powinieneś backupować? Podpowiedzią mogą tu być informacje na temat rodzajów backupów. Wyróżnia się trzy najważniejsze rodzaje backupu:

- Pełny backup – wtedy kiedy kopiujesz wszystkie dane (ang. full backup).
- Backup przyrostowy – wtedy kiedy kopiujesz tylko te dane, które zmieniły się lub pojawiły od ostatniego backupu przyrostowego (ang. incremental backup).
- Backup różnicowy – wtedy kiedy kopiujesz dane, które zmieniły się lub pojawiły od ostatniego backupu pełnego (ang. differentia backup).

Strategia backupu zależy od Ciebie. Możesz zdecydować się na kopiowanie wszystkich danych za każdym razem (full backup), ale pamiętaj, że będziesz potrzebował na to dużo miejsca na dysku – jeśli chcesz tak backupować np.: dysk 250 GB to już po czterech backupach będziesz musiał dysponować dyskiem o pojemności 1 TB. Dlatego rozsądnym rozwiązaniem jest stosowanie backupu przyrostowego. Na początku zrób pełny backup danych, a następnie wykonuj backup przyrostowy,

który będzie uwzględniał tylko te pliki, które się zmieniły lub pojawiły od ostatniego backupu, który wykonałeś.

Zastanawiasz się jak odnaleźć wszystkie zmienione i nowe pliki. Nie obawiaj się – to nie jest zadanie dla Ciebie, tylko dla programu, który powinieneś wykorzystywać do regularnego kopiowania danych. W ustawieniach każdego dobrego programu znajdziesz opcję wyboru backupu przyrostowego, a program będzie wiedział, że Twój pierwszy backup powinien być pełny. Jeśli chcesz znaleźć program, który pozwoli Ci zabezpieczać Twoje dane poprzez regularne tworzenie kopii zapasowych, to wpisz do wyszukiwarki wyrazy: „darmowe programy do backupu danych".

Jeśli już wiesz jak i które dane backupować to pozostaje pytanie jak często? Oczywiście Ty sam znasz najlepsza odpowiedź na to pytanie. Są osoby, które w związku z charakterem swojej pracy i częstotliwością zmian ważnych danych na komputerze, muszą tworzyć kopie zapasowe nawet kilka razy dziennie. Twórz swoje kopie zapasowe raz na tydzień, na przykład na koniec tygodnia. Wydaje się, że to często, ale jeśli okaże się że wszystko co musisz zrobić to podłączenie do komputera dysku zewnętrznego i uruchomienie programu do backupu danych, to zadanie to nie przejawia się jako specjalnie uciążliwe. Jeśli jednak uznałeś, że nie musisz tego robić aż tak często, to rób kopie zapasowe raz na miesiąc – to absolutne minimum do zachowania poczucia bezpieczeństwa.

3.4Aktualizacja oprogramowania

W sytuacji, kiedy praktycznie codziennie pojawiają się nowe sposoby na atakowanie komputerów internautów, aktualizacja oprogramowania, z którego korzystasz stała się jednym z najważniejszych zadań. Dotyczy to zarówno wszystkich programów, z których korzystasz jak i samego systemu operacyjnego. Odnosi się to również do każdego urządzenia, które jest w twoim posiadaniu – komputera, tabletu, smartfonu. Producenci oprogramowania i systemów operacyjnych cały czas pracują nad wprowadzaniem poprawek do swoich produktów. Zazwyczaj mają do tego wydzielone zespoły, które same wyszukują błędów w produktach lub obsługują błędy zgłoszone przez użytkowników tych produktów, a czasami od osób które hobbystycznie lub zawodowo zajmują się ich wyszukiwaniem. Takich błędów pojawia się rocznie co najmniej kilka tysięcy. Nie sposób samemu wprowadzić wszystkich poprawek. Dodatkowo wymaga to zazwyczaj specjalistycznej wiedzy. Dlatego zdecydowana większość producentów przygotował w swoich produktach opcję automatycznego ściągania i instalacji poprawek. Zadanie jako zostało dla Ciebie to skorzystanie z tej opcji. Kieruj się poniższymi zasadami jeśli chcesz dobrze przygotować swój system i programy do bezpiecznego działania, a później utrzymać odpowiedni stan bezpieczeństwa. Zasady te dotyczą zarówno programów komputerowych jak i samego systemu.

- W czasie instalacji nowego programu zawsze, jeśli masz taką możliwość, wybieraj opcję automatycznej aktualizacji programu. Jeśli chcesz zachować nad tym procesem większą kontrolę to pozostaw sobie decyzję o aktualizacji, ale koniecznie korzystaj z opcji informowania o jej pojawieniu się.
- Dla programów, z których już korzystasz sprawdź i ustaw jeśli potrzeba opcję automatycznej aktualizacji programu. Ta opcja jest zazwyczaj dostępna we właściwościach programu.
- Nigdy nie zwlekaj z aktualizacją programu w sytuacji kiedy otrzymujesz powiadomienia o dostępności aktualizacji. Cyberprzestępcy bardzo często wykorzystują „dziury" w systemach tuż po tym jak producenci powiadomili o ich istnieniu, co jest jednoznaczne z publikacją poprawek.
- Jeśli to tylko możliwe nie korzystaj z programów i systemów, które nie są lub przestały być aktualizowane i poprawiane przez producentów. Ich użycie stwarza poważne niebezpieczeństwo włamania do Twojego komputera.
- W przypadku poważnych aktualizacji oprogramowania, w szczególności zmiany wersji systemu operacyjnego, wykonaj kopię zapasową systemu.

3.5 Bezpieczna konfiguracja aplikacji i serwisów internetowych

Posiadanie aktualnego, „załatanego" programu komputerowego jest podstawą jego bezpieczeństwa. Nie zapewnia to jednak 100% bezpieczeństwa, które swoją droga w ogóle nie jest możliwe do osiągnięcia. Dlatego jeśli chcesz aby programy, z których korzystasz najczęściej, były dodatkowo zabezpieczone, powinieneś sam wprowadzić kilka prostych ustawień. Trudno aby w tym poradniku podać wszystkie ważne ustawienia, które powinieneś rozważyć. Przedstawiamy ogólne zasady dotyczące bezpiecznej konfiguracji najbardziej popularnych kategorii programów i serwisów – przeglądarek internetowych, poczty elektronicznej i serwisów społecznościowych. W szczególności te ostatnie mają bardzo często ustawienia domyślne, które nie chronią należycie Twojego bezpieczeństwa, np.: poprzez zbyt liberalne ustawienia prywatności, w wyniku których większość informacji, które kierujesz do osób znajomych jest w praktyce dostępna dla każdego. Jeśli chcesz zapoznać się ze szczegółowymi instrukcjami dotyczącymi gotowych propozycji ustawień to wpisz w przeglądarkę wyrazy: „ustawienia bezpieczeństwa [nazwa programu lub serwisu]".

3.5.1 Przeglądarki internetowe

- Dostosuj ustawienia bezpieczeństwa i prywatności w swojej przeglądarce. Warto włączyć zaawansowaną opcje bezpiecznego przeglądania, które chroni przed niebezpiecznymi witrynami. Ponad to warto pamiętać o zarzadzaniu certyfikatami bezpieczeństwa.
- Jeśli nie jest dla Ciebie bardzo ważne stosowanie elementów ActiveX oraz skryptów JavaScript to wyłącz ich obsługę. Z możliwością ich obsługi wiąże się bardzo dużo ataków.

- „Wtyczki" do przeglądarki instaluj tylko poprzez przeglądarkę. Dokonaj przeglądu posiadanych „wtyczek". Pozostaw tylko te, z których korzystasz.
- Jeśli Twoja przeglądarka daje Ci możliwość kontrolowania poziomu zaufania odwiedzanej strony to skorzystaj z tej opcji. Dzięki temu zostaniesz ostrzeżony przed odwiedzinami niebezpiecznej strony, np.: stron phishingowych i stron instalujących złośliwe oprogramowanie (ang. malware).
- Jeśli chcesz zachować większą prywatność skorzystaj z opcji automatycznego czyszczenia historii odwiedzin stron internetowych oraz instalacji na Twoim komputerze „ciasteczek" (tzw. cookies). Przy okazji warto pamiętać, że większość popularnych przeglądarek posiada opcję anonimowego przeglądania stron.
- Skorzystaj z wbudowanego lub zewnętrznego mechanizmu do blokowania „wyskakujących okienek" (ang. pop-up windows).
- Korzystaj z możliwości używania bezpiecznych protokołów (SSL i TLS)
- Pamiętaj o uruchomieniu opcji automatycznej aktualizacji Twojej przeglądarki.

3.5.2 Poczta elektroniczna

- Stosuj hasło dostępu do Twojej skrzynki pocztowej.
- Wyłącz wykonywanie elementów ActiveX i skryptów JavaScript. W obsłudze poczty są one praktycznie niepotrzebne.
- Jeśli nie jest to dla Ciebie ważne wyłącz obsługę HTML.
- Stosuj wbudowane lub zewnętrzne programy do filtrowania spamu. Spam oprócz tego, że jest nielegalną formą reklamy, jest również nośnikiem bardzo wielu zagrożeń, głównie zaszytych w załącznikach do spamu i linkach znajdujących się w treści wiadomości.
- Najlepiej jeśli Twoja poczta będzie obsługiwana z wykorzystaniem bezpiecznych, szyfrowanych, kanałów komunikacji. W konfiguracji poczty zawsze wybieraj bezpieczne protokoły SSL dla poczty wychodzącej i przychodzącej. Jeśli nie wiesz jak to zrobić to skontaktuj się z administratorem poczty (np.: z firmą oferującą darmowe skrzynki pocztowe).
- Dla szczególnie poufnej poczty stosuj szyfrowanie. Do tego celu możesz się posłużyć darmowym programem zewnętrznym.

3.5.3 Media społecznościowe

- Stosuj silne hasło dostępu do Twojego serwisu społecznościowego. Najlepiej jeśli będziesz używał funkcji dwuskładnikowego uwierzytelnienia (patrz: 3.1 Hasła).
- Jeśli Twój profil społecznościowy nie służy powszechnej reklamie zrób takie ustawienia, aby publikowane przez Ciebie treści były dostępne tylko dla Twoich znajomych. Jeśli chcesz zobaczyć

co na Twoim profilu widzi dowolna osoba to skorzystaj z opcji „wyświetl jako" dostępnej na Twoim profilu .

- Ogranicz możliwość wprowadzania wpisów na Twoim profilu przez inne osoby. Opcja minimum to grono najbliższych znajomych, do których masz zaufanie.
- Ogranicz możliwość wyszukiwania informacji o Tobie.
- Przejrzyj ustawienia pokazujące uprawnienia aplikacji, którym pozwoliłeś na instalację na Twoim profilu. Wszystkie aplikacje, z których nie korzystasz usuń z profilu.
- Ogranicz informowanie na Twoim profilu o Twojej lokalizacji. W szczególności jeśli informujesz o długiej nieobecności w domu wraz z całą rodziną. To najlepszy sposób na poinformowanie złodzieja, o tym że Twój dom pozostał bez opieki.

3.6Bezpieczeństwo fizyczne

Bezpieczeństwo Twojego komputera to nie tylko bezpieczna konfiguracja programów, stosowanie haseł i wykonywanie kopii zapasowych. Utrata bezpieczeństwa może być bardzo prozaiczna – Twoje urządzenie po prostu może zostać zgubione lub skradzione. Wraz z nim wszystkie dane, które raz że stracisz (jeśli ich wcześniej nie zabezpieczyłeś) a dwa, że mogą wpaść w niepowołane ręce. Zresztą straty powiązane z brakiem stosowania odpowiednich zasad bezpieczeństwa fizycznego mogą być dokładnie takie same w sytuacji kiedy nawet na chwilę nie zadbasz o bezpieczny dostęp do swojego urządzenia. Pozostawienie bez opieki urządzenia może skończyć się wykasowaniem Twoich danych lub skopiowaniem ich bez Twojej wiedzy. Poniższe zasady pozwolą Ci na uniknięcie kłopotów związanych z utratą fizycznej kontroli nad sprzętem i złagodzenie skutków strat w przypadku kiedy dojdzie do takiego problemu.

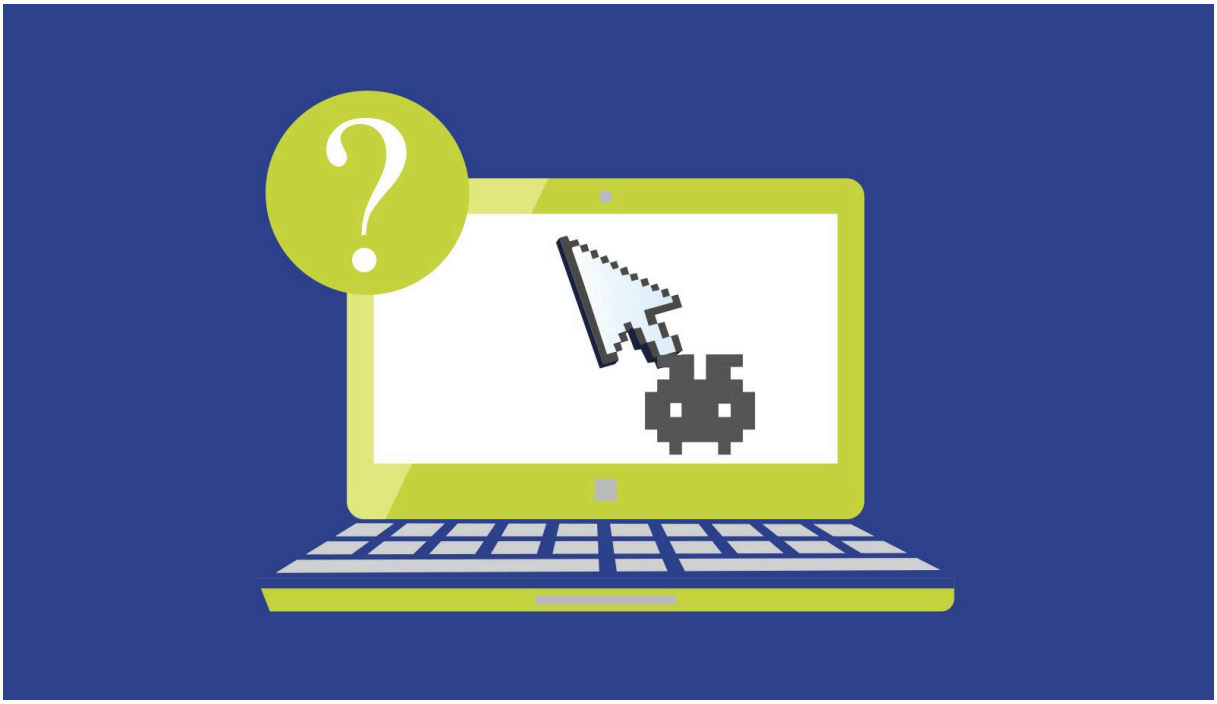
- Nie pozostawiaj swojego urządzenia bez kontroli. Im bardziej publiczne miejsce tym większe ryzyko utraty urządzenia.
- Jeśli opuszczasz miejsce, w którym korzystasz z urządzenia lub zostawiasz swoje urządzenie (np.: telefon) to koniecznie zablokuj do niego dostęp. Żadne Twoje urządzenie nie powinno być dostępne bez konieczności wprowadzenia hasła lub kodu zabezpieczającego.
- Nigdy nie wyrzucaj swojego zniszczonego urządzenia do śmieci. Pamiętaj, że nośnik danych w nim się znajdujący wcale nie musi być zniszczony i istnieje łatwy sposób dostępu do znajdujących się na nim danych. Jeśli chcesz pozbyć się swojego urządzenia to dane na nim powinny zostać profesjonalnie usunięte.
- Pamiętaj, że urządzeniami przenośnymi są również pamięci USB – czasami zawierają one niezwykle istotne dane, które nie powinny znaleźć się w niepowołanych rękach. Takie urządzenia

łatwo zgubić. Staraj się je doczepiać do innych rzeczy (np.: kluczy czy „smyczy") aby nie było łatwo je zgubić. Najlepiej aby Twój nośnik USB zawierał tylko zaszyfrowane dane.

- W szczególny sposób pamiętaj o bezpieczeństwie swojego urządzenia w trakcie podróży. Dworce, lotniska i inne miejsca przebywania pasażerów są jednym z najczęstszych miejsc utraty urządzeń.
- Poufne dane na swoich nośnikach pamięci powinieneś przetrzymywać w wersji zaszyfrowanej. Konieczne jest aby dostęp do nich był zabezpieczony hasłem lub kodem dostępu.
- Jeśli Twoje urządzenie posiada możliwość identyfikacji jego lokalizacji to uruchom taki serwis. Odpowiednio zabezpiecz dostęp do niego. Jeśli dojdzie do kradzieży lub zguby będziesz mógł spróbować ustalić miejsce, w którym znajduje się urządzenie.

3.7 Matryca działań związanych z zabezpieczeniami

	PRZEGLĄDARKA	POCZTA	APLIKACJE	URZĄDZENIA MOBILNE	SERWISY SPOŁECZNOŚCIOWE
HASŁO	**nie**	**tak**	**tak**	**tak**	**tak**
ANTYWIRUS	**nie**	**tak**	**nie**	**tak**	**nie**
BACKUP	**nie**	**tak**	**tak**	**nie**	**Nie**
AKTUALIZACJA	**tak**	**tak**	**tak**	**tak**	**nie**
KONFIGURACJA	**tak**	**nie**	**tak**	**tak**	**tak**
BEZP.FIZYCZNE	**nie**	**nie**	**nie**	**tak**	**nie**



4 Stałeś się ofiarą ataku w cyberprzestrzeni – co dalej

4.1 Sposoby rozpoznawania skutecznego ataku

Bardzo często skutecznemu atakowi komputerowemu towarzyszą charakterystyczne objawy. Ich wczesne rozpoznanie pozwoli Ci na szybkie podjęcie działań zaradczych. Dlatego bądź wyczulony na poniższe sytuacje. Jeśli przydarzyła Ci się któraś z nich to bardzo poważny sygnał, że z Twoim komputerem stało się coś złego – nie lekceważ takiego sygnału.

- Twój komputer wyraźnie działa wolniej, a przy okazji daje sygnały intensywnego działania, np.: pracy dysku, w sytuacji kiedy Ty sam nie podejmujesz żadnych działań, które by uzasadniały duże obciążenie pracy procesora i dysku komputera lub częste migotanie diody sygnalizującej aktywne działanie.
- Z dysku Twojego komputera nagle znikły niektóre pliki i foldery lub wprost przeciwnie – z nieznanej Ci przyczyny pojawiły się nowe pliki i foldery.
- Otrzymałeś informację o tym, że rozsyłasz spam albo, że zostałeś wpisany na „czarną listę” (ang. Blacklist) adresów komputerowych stanowiących zagrożenie sieciowe.
- Otrzymałeś informacje, że dodajesz wiadomości w profilach społecznościowych lub forach internetowych.
- Otrzymałeś informację, że Twój komputer uczestniczył w ataku komputerowym na inne komputery.
- Twój komputer znacznie częściej ulega chwilowym awariom. Pojawiają się błędy w działaniu aplikacji, zawiesza się lub zupełnie wyłącza. Potrafi też sam się ponownie uruchomić.

- Twój program typu firewall sygnalizuje, że jakiś program z Internetu próbuje połączyć się z Twoim komputerem.
- Twoje dane znalazły się na liście danych przejętych i skompromitowanych w ataku sieciowym, np.: opublikowano na takiej liście Twoje hasło do któregoś z serwisów.
- Na swoim komputerze znalazłeś pliki, aplikacje lub odnotowałeś procesy, które są Ci nieznane.

4.2Sposoby postępowania w przypadku ataku

Jeśli nie jesteś specjalistą bezpieczeństwa komputerowego będzie Ci trudno poradzić sobie ze skutkami ataku komputerowego, dlatego warto w takiej sytuacji skorzystać z porad i pomocy specjalistów. Niemniej jednak jest wiele rzeczy, które z pewnością potrafisz zrobić sam. Szybkie działanie i prawidłowa reakcja może Cię uchronić przed większymi, negatywnymi skutkami ataku na Twój komputer i Twoje dane.

Jeśli doszło do ataku pamiętaj o następujących działaniach:

- Jeśli masz podejrzenie, że Twoje hasło do któregoś z serwisów zostało skompromitowane to natychmiast je zmień.
- Jeśli atak na Ciebie jest powiązany z atakiem na innych internautów z jakieś konkretnego serwisu internetowego to koniecznie zastosuj wszystkie porady, które wystosował do użytkowników tego serwisu jego właściciel. Pamiętaj aby sprawdzić wiarygodność tych porad. Najczęściej ich źródłem są oficjalne wypowiedzi właścicieli serwisów dla innych mediów oraz oficjalna strona tego serwisu lub przesłany do Ciebie mail.
- Koniecznie zgłoś swój incydent do właściciela serwisu, z którym związany jest problem. Np.: operator telekomunikacyjny lub bank. Jeśli uważasz, że zostałeś w szczególny sposób poszkodowany – na przykład wykradziono Twoje ważne dane osobowe, to możesz taki przypadek również zgłosić do UODO (możesz to zrobić online: Strona UODO)
- Dokumentuj wszystkie swoje działania i to co odnotowałeś na swoim komputerze. Prosta notatka z wszystkich kroków, które podjąłeś oraz zestaw wykonanych tzw. zrzutów ekranu może być decydująca w dochodzeniu Twoich roszczeń. Zaleca się przechowywanie tych danych na innym komputerze lub nośniku pamięci.
- Jeśli to możliwe to zupełnie zrezygnuj z dalszych działań na skompromitowanym komputerze. Odłączenie go od sieci i wyłączenie w większości sytuacji jest najlepszym zabezpieczeniem śladów nielegalnych działań wobec Ciebie i może być w przyszłości skutecznie wykorzystana do przeprowadzenia analizy ataku.
- Warto wykonać skanowanie swojego komputera, które może wykryć zainstalowane na nim złośliwe oprogramowanie. Jeśli już posiadasz antywirusa i on nic nie wykrył to skorzystaj do tego

celu z antywirusa innej firmy. Pamiętaj jednak aby go nie instalować na Twoim komputerze – skorzystaj z wersji online. Możesz znaleźć takie serwisy wpisując w wyszukiwarkę „darmowy antywirus online”

- Sprawdź miejsce innych potencjalnych strat – np.: Twoje konto bankowe, czy nie pojawiły się tam objawy ataku na Ciebie. Jeśli jesteś przekonany o ataku na Twoje konto bankowe lub kartę kredytową to koniecznie skontaktuj się z bankiem i zgłoś ten przypadek oraz poproś o instrukcję postępowania.
- We wszystkich przypadkach kontaktów z podmiotami zewnętrznymi staraj się przekazywać konkretną, rzeczową informację. Jeśli nie znasz się wystarczająco dobrze na komputerach i sieciach poproś o pomoc znajomą osobę, która posiada choćby minimum wiedzy z tego zakresu.
- Po wykonaniu wszystkich podstawowych działań, jeśli nadal masz przekonanie o tym, że Twój problem nie został rozwiązany, koniecznie skontaktuj się profesjonalistami i poproś o pomoc. Spróbuj uzyskać pomoc bezpłatną. Jeśli nie jest to możliwe to dokonaj szybkiej analizy potencjalnych strat związanych z zaniechaniem działania i kosztów związanych z ich uniknięciem. Podejmij racjonalną decyzję.
- Po odzyskaniu dostępu do swoich zasobów, np.: konta pocztowego czy profilu społecznościowego, na nowo zastosuj wszystkie zasady bezpieczeństwa z nim związane, a w szczególności bezpieczne ustawienia.

Wstępny schemat postępowania w przypadku stwierdzenia cyberataku

5 Przydatne linki

5.1 Strony internetowe zawierające dobre praktyki

Akademia NASK

Niebezpiecznik

Sekurak

Zaufana Trzecia Strona

5.2 Dostawcy usług telekomunikacyjnych

Poniżej zamieszczone zostały linki do stron poświęconych bezpieczeństwu teleinformatycznemu. Strony te prowadzone są przez dostawców usług internetowych dla klientów indywidualnych i zawierają informacje na temat darmowych rozwiązań i porad poprawiających bezpieczeństwo komputera.

Orange	Bezpiecznie tu i tam
Toya	Bezpieczeństwo w Internecie

5.3 Strona organizacji wspierającej przygotowanie poradnika

W serwisie Fundacji Bezpieczna Cyberprzestrzeń znajduje się wiele porad i propozycji dotyczących sposobów poprawy bezpieczeństwa swojego komputera i bezpiecznych zachowań w Internecie.

Strona Fundacji Bezpieczna Cyberprzestrzeń

Słowniczek

ActiveX – element kodu komputerowego pozwalający na przekazywanie danych pomiędzy różnymi programami działającymi w systemie operacyjnym MS Windows.

Botnet – sieć komputerów przejętych przez cyberprzestępcę, nad którymi ma on kontrolę. Botnet może być wykorzystany do ataku na inne komputery lub serwisy – np.: do ataku DDoS.

DDoS – skrót od „Distributed Denial of Service” – atak komputerowy prowadzący do blokady serwisu sieciowego. Najczęściej wykonywany z wykorzystaniem botnetu.

Drive-by download – mechanizm ataku na przeglądarkę internetową polegający na instalacji na komputerze złośliwego kodu. Do instalacji wystarczający jest fakt odwiedzin zainfekowanej strony internetowej.

Dwuczynnikowe uwierzytelnienie (ang. two factor authentication) – uwierzytelnienie, w którym wykorzystywane są dwa składniki, np.: zwykłe hasło i przesłany SMS-em nr kodu autoryzacji operacji.

JavaScript – skryptowy język programowania bardzo często wykorzystywany na stronach internetowych.

Phishing – oszustwo polegające na podstawieniu ofierze sfałszowanej strony internetowej lub innego interfejsu, w którym powinien podać swoje dane uwierzytelniające. Dane te przechwytuje bezpośrednio cyberprzestępca.

Scam – oszustwo internetowe, które w większości przypadków wykorzystuje element ataku socjotechnicznego.

Zombie – jedno z określeń komputera, który został przejęty przez cyberprzestępcę i który stał się fragmentem sieci botnet.