PIOTR BISIALSKI **WOJCIECH WRZESIEŃ**

Bezpieczny pracownik w sieci
Security Awareness

Warszawa 2018

Materiał opracowano w ramach dotacji celowej udzielonej w 2018 r. przez Ministerstwo Cyfryzacji na realizację zadania pn. „Działania mające na celu podnoszenie kompetencji kadr administracji publicznej w obszarze cyberbezpieczeństwa”.

Spis treści

W niniejszym opracowaniu wykorzystano treści dostępne w Biuletynie OUCH!. Polska wersja biuletynu ukazuje się od kwietnia 2011 w ramach współpracy CERT Polska i SANS Institute. OUCH jest tworzony i konsultowany przez zespół ekspertów bezpieczeństwa z SANS Securing The Human.

I. Wstęp

Szanowni Państwo

W Państwa ręce oddajemy zestaw informacji dotyczących problematyki bezpieczeństwa ogólnego pracowników w firmie i jej otoczeniu. Materiały zawarte w niniejszym opracowaniu koncentrują się na zagadnieniach, które dotykają każdego pracownika mającego styczność zarówno z dokumentacją tradycyjną jak i nowoczesnymi narzędziami charakterystycznymi dla trwającej właśnie ery cyfrowej.

W przedstawionych w dalszej części materiałach poruszono zagadnienia z obszarów socjotechniki i sposobów jej wykorzystywania w cyfrowym świecie. Zwrócono uwagę na proste sposoby ochrony lub ograniczenie potencjalnych niebezpieczeństw na jakie narażeni są użytkownicy sieci firmowych i Internetu. Przedstawiono również tematykę bezpieczeństwa urządzeń mobilnych oraz związane z tym moduły bezpieczeństwa w podróży i korzystania z sieci bezprzewodowych.

Mamy nadzieję że informacje przekazane oraz dostępne na naszych szkoleniach będą pomocne w codziennym bezpiecznym korzystaniu z sieci oraz będą inspiracją do poszerzenia wiedzy w tym zakresie.

II. Wprowadzenie do zagadnienia

Cyberprzestrzeń w XXI wieku jest jednym z najważniejszych obszarów tworzonych i eksplorowanych przez człowieka. Internet i tworzona w nim sfera działań funkcjonuje dopiero nieco ponad ćwierć wieku ale skutecznie zmienił wszelkie obszary życia. Powstały nowe dziedziny biznesu, sztuki, komunikacji i sportu. Skrócił się w wielu domenach życia dystans jaki dzielił ludzi mieszkających w różnych geograficznie miejscach. Dostęp do wiedzy nigdy dotąd nie był tak łatwy praktycznie dla każdego. Problemem jest oczywiście weryfikacja jakości i wartości udostępnianej w sieci wiedzy ale to jest odrębny problem badawczy.

Poza niewątpliwie przeważającą ilością dobrych cech tej nowej sfery współczesnego życia korzystanie z niej wiąże się również poddawaniem ludzi przemocy słownej, przedstawianiem informacji prawdziwej i fałszywej, manipulacji. Wiele osób czuje się swobodnie korzystając

z technologii, równocześnie robiąc to w sposób bezpieczny. Jednak są osoby, które mogą nie czuć się tak swobodnie, zwłaszcza jeśli nie wychowywały się z komputerami i dostępem do Internetu. Dlatego nieustanne zwiększanie świadomości zagrożeń płynących z cyfrowego świata ale przekładających się na realne szkody jest powinnością zarówno pracodawców jak i organizacji społecznych a także mediów.

Zwiększając wykładniczo swój zasięg zarówno geograficzny jak i znaczeniowy - Internet staje się polem odwzorowania działań człowieka z realnego świata ale jednocześnie działania te są modyfikowane, często płytsze i podatne na zagrożenia.

Przeprowadzone badania wskazują jednoznacznie ze poza celowymi działaniami przestępczymi istnieje sfera działań wynikająca z braku świadomości podejmowanych w sieci działań przez pracowników. Jest to często wynikiem przyzwyczajeń przenoszonych pomiędzy płaszczyzna prywatną i służbową. Dlatego tak ważne jest nieustanne przypominanie o mechanizmach jakie są wykorzystywane przez przestępców i jednocześnie o pułapkach rutynowych codziennych zachowań. Skutki są często trudne do przewidzenia a ponoszone konsekwencje mogą być bardzo przykre.

III. Wywieranie wpływu na ludzi

W jaki sposób można nakłonić kogoś do wykonania tego czego my chcemy? Czy jest to możliwe? Kto stosuje te metody świadomie? Dlaczego jesteśmy podatni na tego typu działania?

Badania naukowe na ten temat prowadzi od wielu lat Robert Beno Cialdini – profesor psychologii Uniwersytetu Stanowego w Arizonie zajmujący się psychologią społeczną.

Jest znany przede wszystkim jako autor książki „Wywieranie wpływu na ludzi", będącej rezultatem ponad 15 lat badań. Opisał w niej metody stosowane do wywierania wpływu na ludzi w postaci sześciu „zasad".

1. Zasada wzajemności

   Zasada ta jest jednym z najpowszechniejszych mechanizmów, które ludzie stosują zarówno świadomie jak i całkowicie bezwiednie. Jeżeli ktoś wyświadczył nam nawet niewielką przysługę czujemy potrzebę zrewanżowania się tej osobie. Mały prezent

kojarzy się nam miło i jesteśmy skłonni do lepszego postrzegania osoby, która nam go ofiarowała. Oczywiście nie musi to być fizyczny prezent ale również pomoc w załatwieniu jakiejś sprawy czy wskazanie rozwiązania.

Najprostszym sposobem zaobserwowania tego zjawiska jest sytuacja, w której po wizycie u kogoś odczuwamy naturalną potrzebę zaproszenia tej osoby z rewizytą. Innym przykładem zobowiązania gdzie „nie wypada" inaczej postąpić jest zaproszenie do restauracji i potem rewanż z naszej strony dla zapraszających . Naukowcy twierdzą że jest to zjawisko powszechne w każdej kulturze i jest konsekwencją odkrycia i rozwoju potrzeby dzielenia się żywnością i nabytymi umiejętnościami – „ja pokażę tobie jak robić to a ty pokażesz mi jak robić tamto". Silne podświadome przeświadczenie o konieczności stosowania tej zasady w życiu leży u podstaw działań wykorzystywanych również w działaniach socjotechników.

2. Zobowiązanie i konsekwencja

W codziennym życiu a także wśród wielu społeczeństw jako przekazywana tradycyjnie wartość ważną rolę odgrywa zasada konsekwencji. W teorii wywierania wpływu uzupełnieniem tej zasady jest zobowiązanie lub zaangażowanie.

„Psychologowie od dawna zdają sobie sprawę z siły ludzkiego dążenia do zgodności między słowami, przekonaniami, postawami i czynami. Dążenie do zgodności ma trzy źródła. Po pierwsze, konsekwencja jest cnotą wysoce cenioną przez społeczeństwo. Po drugie, niezależnie od społecznych konsekwencji, postępowanie konsekwentne jest zwykle korzystne dla tych, którzy potrafili się na nie zdobyć. Po trzecie, konsekwentne trzymanie się jakiejś linii postępowania jest wygodną „ drogą na skróty", pozwalającą poradzić sobie z komplikacjami współczesnego życia. Konsekwentne trzymanie się poprzednich decyzji zwalnia z konieczności rozpatrywania wciąż napływających informacji — wystarcz postępować zgodnie z raz dokonanymi postanowieniami."[1] Mechanizm ten jest bardzo często wykorzystywany przez ludzi stosujących manipulację. Wprowadzenie „ofiary" na ścieżkę, która prowadzi do zajęcia przez nią jakiegoś stanowiska ,opowiedzenia się za jakąś sprawą prowadzi do dalszego konsekwentnego ulegania próbom manipulacji zgodnie z założonym przez manipulującego kierunkiem.

[1] Robert B. Cialdini-„Wywieranie wpływu na ludzi Teoria i praktyka"

3. Społeczny dowód słuszności

   Zasada społecznego dowodu słuszności oznacza, że to, jak inni ludzie postępują bywa podstawą do naszych własnych wyborów i sposobu postepowania. Czy te poglądy i zachowanie są słuszne i właściwe w naszym własnym przypadku. Wykazanie ze inni tak zrobili jest bardzo często swoistym przyczółkiem do nakłonieni do zachowania zaplanowanego przez manipulującego. Na przykład: wszyscy wokół biegają i również ja biegam bo jest to modne, wszyscy prezentują wyniki na portalu społecznościowym ja również. Ale czy tego naprawdę chcę? Bardzo silne w codziennym życiu są przejawy naśladowania przy różnych aktywnościach takich jak, decyzja o zakupach, bywanie w modnych miejscach czy nawet wyboru rodzaju diety. Zasada ta może być używana do skłaniania ludzi do uległości za pomocą dostarczania im informacji, że inni też tak zrobili i robią to o co zostali poproszeni.

4. Sympatia i podobieństwo

   Ludzie mają naturalną skłonność udzielania zaufania tym osobom, które lubią i znają. Osoby próbujące manipulować często starają się zaprzyjaźnić, w ten sposób wchodzą do zaufanego kręgu, z którego łatwo pozyskiwać informacje. Innym aspektem ważnym dla tej zasady jest fizyczna atrakcyjność. Dużo łatwiej wzbudzić zaufanie jeżeli próbuje tego osoba zadbana, pachnąca i elokwentna. Innymi wykorzystywanymi w trakcie manipulacji elementami jest wzbudzenie poczucia podobieństwa poprzez te same wspomnienia o odwiedzonych miejscach i zachowaniach w danej sytuacji oczywiście te działania są podbudowane dużą ilością kontaktów.

5. Autorytet

   Mamy skłonność do ulegania, przyznawania racji autorytetom co oznaczać może uleganie jedynie symbolom czy oznakom autorytetu. Badania wskazują, że symbolami tymi są tytuły, ubrania i samochody. Ludzie, którzy wykorzystują tego typu symbole, potrafią często silniej wpływać na innych, nawet jeżeli nie są rzeczywistymi autorytetami. Warto w takiej sytuacji pomyśleć czy za symbolami autorytetu stoi prawdziwy autorytet i czy w związku z tym warto mu w pełni zaufać.

6. Niedostępność

   Reguła niedostępności polega na przypisywaniu większej wartości tym możliwościom, które stają się dla ludzi niedostępne. Hasło „ograniczona liczba egzemplarzy w tej

cenie" czy „promocja ograniczona czasowo", są doskonałym zobrazowaniem tej zasady. Mamy poczucie że rzeczy trudnodostępne są uważane za cenniejsze. Dla wielu osób dobra, usługi czy informacje uważane za osiągalne tylko dla ograniczonej grupy zyskują na wartości tylko z tego powodu. Najbardziej pożądane są te rzeczy, których niedostępność jest ogłoszona od niedawna. Kluczowym działaniem jest danie sobie prawa do chłodnej oceny danej sytuacji czy okazji.

Przytoczone powyżej zasady są wykorzystywane do większości przestępstw i nadużyć przeprowadzanych w cyberprzestrzeni.

IV. Socjotechnika

Socjotechnika lub inaczej inżynieria społeczna jest praktycznym zastosowaniem opisanych w poprzednim rozdziale zasad. Oczywiście zasady te mogą być wykorzystane w ramach działań sprzedażowych czy marketingowych ale niestety często są wykorzystywane do popełniania przestępstw. Ponieważ cyberprzestrzeń jest częścią naszej dzisiejszej rzeczywistości również tam działania manipulacyjne są stosowane.
Możliwe że miałeś już do czynienia z phishingiem. Są to wiadomości e-mail wysyłane przez cyberprzestępców do milionów potencjalnych ofiar na całym świecie, które mają na celu je oszukać, nabrać lub zaatakować. Zazwyczaj wiadomości te wydają się pochodzić z zaufanego źródła, np. z banku lub od kogoś znajomego. E-maile często zawierają pilną wiadomość lub specjalną ofertę dla Ciebie, tak dobrą, że żal byłoby z niej nie skorzystać. Jeśli klikniesz na link w takiej wiadomości phishingowej, możesz zostać zabrany do złośliwej strony internetowej, która będzie próbowała włamać się do Twojego komputera albo pozyskać Twój login i hasło. Wiadomość e-mail z phishingiem może też posiadać zainfekowany załącznik, który po otwarciu będzie próbował zainfekować i przejąć kontrolę nad Twoim komputerem. Cyberprzestępcy wysyłają te wiadomości do możliwie największej liczby osób, wiedząc, że im więcej osób je otrzyma, tym więcej będzie ich potencjalną ofiarą.

V. Portale społecznościowe

Portale społecznościowe ewoluują są coraz bardziej dostosowywane do naszych potrzeb ale również kreują potrzeby na które my się godzimy. Dla użytkowników są rozrywką, miejscem spotkań, możliwością odnalezienia starych kontaktów i osób „po latach”, zaspokojenia

potrzeby podglądania i z drugiej strony potrzeby opowiadania o sobie. Dla portali społecznościowych jest to możliwość coraz precyzyjniejszego profilowania użytkowników a co za tym idzie sprzedaży bardzo dobrych nośników reklamowych. Jednak poza tymi dwoma aktorami

Powszechną obawą dotyczącą serwisów społecznościowych jest ryzyko utraty prywatności i zamieszczenia zbyt wielu informacji o sobie. Nieumiejętne dzielenie się informacjami może prowadzić do:

Zniszczenia Twojej kariery:

Krępujące informacje zamieszczone w sieci mogą wpłynąć negatywnie na Twoją przyszłość. Wiele organizacji traktuje przeglądanie serwisów społecznościowych w poszukiwaniu informacji o kandydacie do pracy jako cześć procesu rekrutacyjnego. Każdy wstydliwy post, niezależnie od tego jak dawno został opublikowany, może sprawić że nie dostaniemy wymarzonej posady. Ponadto zdarza się, że podobne działania w stosunku do aplikujących studentów przeprowadzają szkoły wyższe.

Ataki bezpośrednio na Ciebie:

Cyberprzestępcy mogą zbierać dostępne informacje aby potem użyć ich przeciwko Tobie. Na przykład, będąc w posiadaniu pewnych informacji osobistych mogą z łatwością odgadnąć odpowiedź na „sekretne pytanie" wykorzystywane przy odzyskiwaniu hasła w innych serwisach internetowych, a może nawet ubiegać się o przyznanie przy ich użyciu kredytu.

Ataki na Twojego pracodawcę:

Informacje udostępniane na stronach portali społecznościowych przez pracowników konkretnych firm lub podmiotów mogą posłużyć jako doskonałe źródło danych dla konkurencji lub być wykorzystane przez przestępców przygotowujących się do ataku na serwery pracodawcy. Ponadto, działania podejmowane przez pracowników w Internecie mogą niekiedy mimowolnie odbić się na wizerunku firmy. Upewnij się jaka polityka odnośnie serwisów społecznościowych obowiązuje w Twoim miejscu pracy i jak powinieneś zabezpieczyć dane i reputację Twojej organizacji. Najbardziej efektywnym sposobem ochrony przed tymi zagrożeniami jest ostrożność w publikowaniu informacji o sobie. Zawsze rozważ% czy informacje, które udostępniasz dzisiaj mogłyby zostać(użyte przeciwko Tobie w przyszłości. Zawsze ustawienia prywatności na swoim profilu społecznościowym tak, aby ograniczyć osobom niepowołanym dostęp do informacji osobistych które opublikowałeś! lub będziesz publikował w serwisie. Pamiętaj jednak, że wszystkie zamieszczone informacje,

pomimo poprawnych ustawień prywatności mogą# zawsze nieumyślnie wyciec z serwisu poprzez inne usługi (na przykład aplikacji na Facebooku, której udzielcie! odpowiednich pozwoleń) lub połączonych z Twoim profilem znajomych. Dlatego zamieszczając jakiekolwiek informacje w serwisie najlepiej jest założ że każda z nich stanie się kiedyś dostępna publicznie. Takie podejście może uchronić przed wieloma przykrymi konsekwencjami. Bądź świadomy jakie treści inni zamieszczają o Tobie. Jeśli Twoi znajomi publikują informacje, zdjęcia lub inne dane dotyczące Twojej osoby, a Ty nie chcesz aby je udostępniano publicznie, poproś o ich usunięcie.

VI. Bankowość elektroniczna

Bardzo dobrze rozwinięta w naszym kraju bankowość elektroniczna jest częstym polem do przeprowadzania ataków na klientów banków. Środowisko bankowe jest mocno zdeterminowane do informowania swoich klientów o zasadach bezpiecznego korzystania z usług on-line.

Zachęcamy do zapoznania się poniżej z wybranymi zasadami bezpiecznego korzystania z Internetu i bankowości elektronicznej przygotowanymi przez Związek Banków Polskich[2].

1. Nie otwieranie przesyłek poczty elektronicznej niewiadomego pochodzenia oraz załączonych do nich plików lub linków, szczególnie w przypadkach gdyby wskazywały na okoliczności zdarzeń, które nie miały miejsca z Państwa udziałem.
2. Nikt oprócz użytkownika nie powinien być w posiadaniu informacji poufnych związanych z identyfikacją i uwierzytelnieniem jego tożsamości w serwisach bankowości elektronicznej.
3. Jeśli do systemu bankowości internetowej logujesz się i autoryzujesz transakcje przy wykorzystaniu certyfikatu cyfrowego na nośniku kryptograficznym (np. karta kryptograficzna, eToken) - zawsze podłączaj to urządzenie do komputera w momencie korzystania z bankowości internetowej. Po wylogowaniu odłącz eToken/kartę i schowaj w bezpiecznym miejscu,

[2] https://zbp.pl/wydarzenia/archiwum/komentarze/2015/kwiecien/bezpieczenstwo-bankowosci-elektronicznej

4. Jeśli z bankowości internetowej korzystasz z jednorazowych kodów autoryzacyjnych SMS – weryfikuj treść SMS i zwrócić szczególną uwagę na datę i kwotę przelewu oraz numery rachunków prezentowane w wiadomości.
5. Sprawdzaj numer rachunku odbiorcy, gdy kopiujesz dane do przelewu.
6. Regularnie sprawdzaj historię przeprowadzonych transakcji, w tym transakcji wysyłanych w „paczkach".
7. Korzystaj z aktualnego oprogramowania antywirusowego i zapory sieciowej (firewall).
8. Upewnij się czy masz zainstalowaną najnowszą wersję przeglądarki i wszystkie poprawki do systemu operacyjnego.
9. Jeśli to możliwe najlepiej używaj komputera przeznaczonego wyłącznie do korzystania z bankowości internetowej.
10. Nie instaluj oprogramowania nieznanego pochodzenia.
11. Zadbaj, aby hasło dostępu do systemu czy autoryzacji było wystarczająco silne.
12. Nie pobieraj aplikacji bankowości mobilnej z niezaufanych źródeł - aplikacje mobilne możesz pobrać z autoryzowanych sklepów: App Store, Google Play etc.
13. Korzystając z bankowości elektronicznej zawsze należy postępować zgodnie z polityką bezpieczeństwa opublikowaną przez bank i należy aktualizować wiedzę w tym zakresie.

VII. Hasło podstawowe bezpieczeństwo

Hasła są jednym z podstawowych sposobów, w jaki możemy udowodnić, kim jesteśmy. Używając ich logujemy się do poczty elektronicznej, bankowości on-line, dokonujemy zakupów w sieci i uzyskujemy dostęp do urządzeń, takich jak laptop lub smartfon. Można powiedzieć, że w wielu przypadkach hasła są niczym klucze do naszego królestwa.
W związku z tym, jeśli ktoś byłby w posiadaniu Twojego hasła, mógłby dokonać kradzieży Twojej tożsamości, transferu Twoich pieniędzy lub uzyskać dostęp do wszystkich Twoich prywatnych danych. Używanie silnych haseł jest niezbędne aby chronić swoją tożsamość i swoje informacje.
Cyberprzestępcy opracowali wyspecjalizowane programy, które coraz lepiej potrafią odgadnąć, a mówiąc inaczej "złamać", hasła. To oznacza, że mogą oni wykraść Twoje hasła jeśli są one słabe albo łatwe do odgadnięcia. Nigdy nie należy używać łatwo dostępnych informacji tworząc hasła. Do takich informacji należą na przykład data

urodzenia, imię zwierzątka lub cokolwiek, co można łatwo znaleźć na portalach społecznościowych lub wyszukać w Google. Zamiast tego, najlepszym sposobem na stworzenie silnego hasła jest użycie długiego hasła, które im więcej znaków zawiera, tym lepiej. Najlepiej zamiast używać jednego słowa, używać wielu słów, a nawet pełnych zdań. Tego typu hasło nazywa się z angielskiego passphrase i jest jednym z najsilniejszych jakich można użyć. Oto przykład jednego z nich:
Umówiłem się z nią na dziewiątą.
To wszystko czego potrzebujesz. Jeśli jest to wymagane, możesz sprawić że Twoje hasło stanie się jeszcze silniejsze dodając do niego symbole, wielkie litery lub cyfry, tak jak w przykładzie poniżej. Jest to szczególnie ważne, jeśli korzystasz z portali nie pozwalających używać wielu słów lub pełnych zdań jako hasła:
Um0w!lem$!3zni@n@9!.
Zwróć uwagę, jak w przykładzie została użyta wielka litera. Możesz również zastąpić niektóre litery cyframi lub symbolami, na przykład zastępując literę “a” symbolem “@”, literę “o” zerem, albo dodać znaki przestankowe, takie jak znak zapytania, kropkę czy nawet spację. Jeśli portal lub program ogranicza liczbę znaków w haśle, użyj maksymalnej dozwolonej liczby znaków.

Poza używaniem mocnych haseł, należy również ostrożnie się z nimi obchodzić. Posiadanie mocnego hasła nie pomoże, jeśli będzie można je łatwo wykraść lub skopiować.

Upewnij się że używasz różnych haseł do różnych kont. Na przykład, nigdy nie używaj tych samych haseł do usług w pracy czy do konta w banku co do haseł do kont osobistych, takich jak Facebook, YouTube czy Twitter. W ten sposób, jeśli jedno z haseł zostanie skompromitowane, pozostałe konta pozostaną nadal bezpieczne. Jeśli masz zbyt wiele haseł do zapamiętania, rozważ użycie menedżera haseł. Jest to specjalny program, który działa na komputerze lub urządzeniu przenośnym, który bezpiecznie przechowuje wszystkie Twoje hasła. Jedyne hasło, które trzeba zapamiętać to hasło do komputera i programu do zarządzania hasłami. Jeśli chcesz zastosować taki program do haseł używanych w pracy, skontaktuj się ze swoim przełożonym lub pomocą techniczną aby upewnić się czy korzystanie z menedżera haseł jest dozwolone w Twojej organizacji.

Nigdy nie udostępniaj swojego hasła innym osobom, także współpracownikom. Pamiętaj, że hasło jest tajemnicą, a jeśli ktoś je pozna, nie jest już bezpieczne. Jeżeli przypadkowo podzieliłeś się hasłem z kimś innym lub domyślasz się, że mogło być ono zostać złamane lub wykradzione, należy je natychmiast zmienić.

Nie należy korzystać z publicznych komputerów, takich jak te w hotelach lub w bibliotekach, aby logować się na konto do pracy lub do banku. Ponieważ każdy może korzystać z tych komputerów, mogą one być zainfekowane złośliwym oprogramowaniem, które przechwytuje wszystkie naciśnięcia klawiszy. Do kont w swojej pracy lub rachunków bankowych loguj się tylko z zaufanych komputerów lub urządzeń mobilnych, nad którymi masz kontrolę.

Uważaj na strony internetowe, które wymagają odpowiedzi na osobiste pytania. Pytania te są używane, jeśli zapomnisz hasła i trzeba będzie je zresetować. Sęk w tym, że odpowiedzi na te pytania można często znaleźć w Internecie czy nawet na Facebooku. Upewnij się, że jeśli odpowiadasz na osobiste pytania używasz tylko informacji, które nie są dostępne publicznie lub są to fikcyjne dane, celowo przez Ciebie zmyślone. Programy do zarządzania hasłami mogą pomóc także w trzymaniu bezpiecznie takich odpowiedzi, gdyż wiele z nich pozwala na przechowywanie dodatkowych informacji o kontach.

Wiele kont internetowych oferuje coś, co jest nazywane “dwuskładnikowym uwierzytelnianiem” lub “dwuetapową weryfikacją”. Jest to stosowane kiedy do logowania potrzebne jest więcej niż tylko jedno hasło, np. dodatkowo żądany jest kod przesyłany na smartfon. Użycie tej metody jest o wiele bardziej bezpieczne niż użycie samego hasła. Jeśli tylko jest to możliwe, należy zawsze korzystać z tych silniejszych metod uwierzytelniania.

Urządzenia mobilne często wymagają podania kodu PIN w celu ochrony dostępu do nich. Pamiętaj, że PIN jest niczym innym tylko kolejnym hasłem. Im Twój PIN jest dłuższy, tym jest bardziej bezpieczny. Niektóre urządzenia mobilne (np. iPhone) pozwolą Ci zmienić numer PIN na zwykłe literowe hasło.

I na koniec, zapamiętaj: jeśli przestajesz korzystać z konta, należy je zamknąć, usunąć lub wyłączyć.

VIII. Bezpieczne korzystanie z nowoczesnych usług sieciowych

Jeszcze kilka lat temu sieci domowe były stosunkowo proste, zazwyczaj nic ponad bezprzewodowy punkt dostępu i komputer lub dwa służące do surfowania po Internecie lub gier online. Jednak sieci domowe stają się coraz bardziej złożone. Nie tylko podłączamy do naszych sieci domowych znacznie większą liczbę urządzeń, ale także robimy z nimi znacznie więcej.

Sieć bezprzewodowa

Większość dzisiejszych sieci domowych opiera się na sieci bezprzewodowej (często nazywanej siecią Wi-Fi). To właśnie ona pozwala na podłączenie dowolnych urządzeń do Internetu, od laptopów i tabletów po konsole do gier i telewizory. Aby było to możliwe, sieć bezprzewodowa potrzebuje czegoś zwanego punktem dostępowym (ang. access point). Jest to urządzenie, które łączy się z routerem (może być też w niego wbudowane) i wysyła sygnał bezprzewodowy, z którym łączą się różne urządzenia. Kiedy twoje urządzenia połączą się z punktem dostępowym, mogą przez niego łączyć się z innymi urządzeniami z sieci domowej, jak również z Internetem. W efekcie bezprzewodowy punkt dostępu do sieci jest jednym z kluczowych elementów sieci domowej i bardzo zalecamy następujące kroki w celu jego zabezpieczenia:

Dla większości bezprzewodowych punktów dostępu domyślny login i hasło administratora są ogólnie znane i często nawet umieszczone w Internecie. Dlatego przede wszystkim należy je zmienić na takie, które znasz tylko Ty. Upewnij się, że jest to unikalne hasło i nie wykorzystałeś go już do żadnego innego konta.

Kolejną opcją którą należy skonfigurować to nazwa sieci bezprzewodowej (nazywana również SSID). Jest to nazwa, która wyświetli się na Twoich urządzeniach przy próbie połączenia się do lokalnej sieci bezprzewodowej. Nadaj swojej sieci niepowtarzalną nazwę, tak aby było łatwo ją zidentyfikować, ale pamiętaj, że nie powinna ona zawierać żadnych danych osobowych. Nie ma raczej większego sensu konfiguracja domowej sieci jako ukrytej (lub nie rozgłaszanej, ang. non-broadcast). Większość narzędzi do skanowania lub przeciętny atakujący może bardzo łatwo ją odkryć.

Następnym krokiem jest upewnienie się, że tylko osoby, które znasz i którym ufasz mogą się połączyć i korzystać z twojej sieci bezprzewodowej oraz, że te połączenia są szyfrowane. Chcesz przecież mieć pewność, że sąsiedzi lub obcy nie będą mogli połączyć

się albo monitorować twojej sieci. Można w prosty sposób zmniejszyć to ryzyko poprzez włączenie silnego zabezpieczenia w bezprzewodowym punkcie dostępu. Obecnie najlepszym rozwiązaniem jest korzystanie z mechanizmu zabezpieczeń WPA2. Włączając WPA2 sprawiasz, że aby ktoś mógł połączyć się z siecią musi podać hasło, a po uwierzytelnieniu wszystkie połączenia są szyfrowane. Upewnij się, że nie używasz starszych, przestarzałych metod zabezpieczeń, takich jak WEP lub że sieć nie ma żadnych zabezpieczeń, co jest nazywane inaczej siecią otwartą. Otwarta sieć pozwala każdemu połączyć się z nią bez uwierzytelniania.

Hasło którego osoby w twoim domu będą używać do łączenia się z siecią bezprzewodową powinno być silne, trudne do odgadnięcia i różnić się od hasła administratora. Najprawdopodobniej będzie wymagane podać je tylko raz dla każdego urządzenia ponieważ później zostanie ono w nim zapamiętane.

Wiele bezprzewodowych punktów dostępu obsługuje tzw. sieć dla gości (ang. guest network). Sieć dla gości pozwala odwiedzającym Cię połączyć się z bezprzewodowym punktem dostępu i uzyskać dostęp do Internetu, ale nie pozwala połączyć się z żadnym innym urządzeniem w sieci domowej. Jeśli dodasz sieć dla gości również należy włączyć dla niej WPA2 i ustanowić dla niej inne hasło.

Jeśli masz problem z zapamiętaniem różnych haseł, użyj menedżera haseł aby je bezpiecznie przechowywać.

Po skonfigurowaniu sieci bezprzewodowej zalecamy skonfigurować sieć domową tak, aby używać usługi oferowanej przez OpenDNS jako serwerów DNS (lub innej podobnej, np. Norton ConnectSafe for Home). Po wpisaniu w przeglądarce nazwy, dzięki DNS Twoja przeglądarka wie, z którym serwerem w Internecie ma się połączyć. Usługi takie jak OpenDNS identyfikują znane, zainfekowane strony internetowe i powstrzymają wszelkie urządzenia podłączone do domowej sieci bezprzewodowej przed przypadkowym odwiedzeniem takich stron. Ponadto usługi te często dają możliwość filtrowania i blokowania witryn budzących zastrzeżenia. To co sprawia, że to rozwiązanie to jest tak skuteczne to że nie ma konieczności instalowania żadnego oprogramowania na twoich urządzeniach, wystarczy jedynie wprowadzić zmianę w bezprzewodowym punkcie dostępu.

Warto też przygotować się do bezpiecznego działania w się w czasie podróży. Najprostszą i najbardziej efektywną metodą, która znacząco podniesie poziom naszego

bezpieczeństwa w czasie podróży jest wcześniejsze wykonanie kilku łatwych czynności: Aktualizacja systemu operacyjnego zarówno laptopa oraz smartfonu, a także aktualizacja wszystkich zainstalowanych w nich aplikacji. Zredukuje to możliwość powodzenia ataków wykorzystujących znane i załatane luki. Włącznie firewalla systemowego. Dzięki temu inne komputery z sieci nie będą mogły nieuprawnione połączyć się z naszym urządzeniem. Włączenie oprogramowania antywirusowego oraz zaktualizowanie bazy sygnatur. Można wówczas uniknąć przypadkowej infekcji komputera, gdy otrzymany email lub plik od osoby, co do której nie mamy 100% zaufania zawierał wirusa. Laptopy i smartfony są łatwym łupem dla potencjalnych złodziei. Dobrym nawykiem jest zabezpieczenie dostępu do konta w komputerze hasłem, a w smartfonie kodem PIN oraz włączenie automatycznego blokowania. Utrudni to złodziejowi dostęp do danych zapisanych w urządzeniu.

Dołączenie do urządzenia etykiety z danymi kontaktowymi właściciela daje szansę na jego

odzyskanie. Oferta nagrody jest zawsze dodatkową motywacją dla znalazcy.

W przypadku, gdy laptop lub smartfon zawiera prywatne lub poufne dane, dobrym zabezpieczeniem przed niepowołanym dostępem jest ich zaszyfrowanie. Przed wyjazdem sprawdź polityki bezpieczeństwa w Twojej firmie, aby dowiedzieć się jakiego oprogramowania najlepiej

do tego celu użyć.

Jeżeli opuszczając miejsce pracy uruchamiamy automatyczne powiadamianie o nieobecności, postarajmy się znaleźć współpracownika, który może posłużyć jako alternatywny kontakt. Dobrą praktyką jest także limitowanie odpowiedzi autorespondera jedynie do adresów znajdujących się w książce adresowej. Oprócz przygotowania sprzętu do podróży niemniej istotne jest zapoznanie się z potencjalnymi zagrożeniami, jakie mogą nas spotkać podczas korzystania z sieci w nieznanych nam miejscach. Publiczna sieć oferuje usługi dostępu do Internetu każdemu, bez względu na intencje. Takie sieci możemy najczęściej spotkać na lotniskach, w hotelach, restauracjach lub kafejkach w postaci otwartych sieci WiFi. Gdy używamy takiej sieci, nasza aktywność może być monitorowana przez innych. Dodatkowo, użytkownicy o złych zamiarach mogą ustanawiać własne sieci bezprzewodowe i zachęcać innych do ich używania przejmując jednocześnie przesyłane informacje. Zawsze gdy to możliwe używaj sieci WiFi, do których

jest pewność, że są udostępnianie przez znane i zaufane organizacje. Często nazwy takich sieci zawierają fragment nazwy hotelu, restauracji lub innej organizacji, np. operatora telekomunikacyjnego. Są one z reguły bezpieczniejsze niż sieci otwarte - nieznane i często wybierane tylko ze względu na darmowy dostęp. W przypadku, gdy to możliwe zawsze wybieraj sieci zapewniające szyfrowanie przesyłanych danych. W kolejności od szyfrowania najsilniejszego wyróżniamy sieci z szyfrowaniem WPA2, WPA oraz WEP. Niestety, nawet używając sieci z szyfrowaniem, nasze dane mogą zostać podsłuchane przez innych użytkowników tej samej sieci bezprzewodowej. Metodą, która temu zapobiega jest używanie dodatkowych szyfrowanych kanałów komunikacyjnych jak VPN (wirtualnie sieci prywatne) lub bezpiecznych protokołów takich jak HTTPS (SSL/TLS). Protokół HTTPS, używany przez wiele serwisów internetowych takich jak Google, Gmail, Twitter czy Facebook, zapewnia poufność przesyłanych danych. Przeglądarki internetowe z reguły w specjalny sposób zaznaczają, że jest on używany i nie ma obaw o to, że nasze informacje wpadną w niepowołane ręce lub zostaną zmodyfikowane bez naszej zgody. Wirtualna sieć prywatna ustanawia dodatkowy kanał komunikacyjny pomiędzy naszym komputerem a serwerem udostępniającym usługę VPN. Całość komunikacji jest szyfrowana podobnie jak w przypadku używania bezpiecznych protokołów SSL/TLS. Skontaktuj się ze swoim działem wsparcia IT i sprawdź czy Twoja organizacja umożliwia zdalny dostęp za pomocą technologii VPN. Istnieje też możliwość zakupu za niewielką opłatą usługi u prywatnych operatorów. Kolejną z metod jest użycie smartfonu jako bezprzewodowego punktu dostępowego. Skontaktuj się ze swoim operatorem telekomunikacyjnym w celu sprawdzenia, czy istnieje taka możliwość – zwykle wiąże się ona z dodatkowymi opłatami za transfer danych, zwłaszcza poza granicami kraju. Jeżeli smartfon nie posiada funkcji opisanej jako „osobisty punkt dostępowy WiFi" lub podobnej, często umożliwia obsługę skrzynki email oraz przeglądanie zasobów WWW. Jest to dobra alternatywa dla otwartych sieci WiFi, gdyż bezpieczeństwo przesyłanych danych jest zapewniane przez operatora telekomunikacyjnego.

Publiczne komputery, podobnie do publicznych sieci, mogą być używane przez każdego. Możemy je znaleźć w bibliotekach, hotelach oraz kafejkach często pozbawionych jakiegokolwiek nadzoru. Nie ma możliwości sprawdzenia kto używał danego komputera wcześniej i do jakich celów. Należy założyć, że może on być zarażony niebezpiecznym oprogramowaniem, a każda informacja jaką przesyłamy będzie przechwycona przez

osoby niepowołane. Przy korzystaniu z komputerów w tego typu miejscach należy bezwzględnie wystrzegać się podawania loginów i haseł do jakichkolwiek serwisów. W przypadku, gdy nie mamy wyboru i musimy dokonać operacji, która ujawnia nasze dane, po powrocie lub przy pierwszej nadarzającej się okazji skorzystania z bezpiecznego połączenia powinniśmy je zmienić. Komputery o otwartym dostępie mogą być swobodnie wykorzystywane do takich rzeczy jak sprawdzanie rozkładów lotów, czy wyszukiwanie ciekawych miejsc do zwiedzania w czasie podróży.