10 rad podnoszących bezpieczeństwo komputera od Niebezpiecznik.pl

Oto zestaw czynności, których wykonanie powinno podnieść ogólne bezpieczeństwo Twojego prywatnego komputera, telefonu lub tabletu. Wykonaj je, a utrudnisz hakerom/cyberprzestępcom kradzież twoich prywatnych danych zarówno z dysków twoich urządzeń jak i z serwisów internetowych, na których masz konta.

Porady kierowane są do "przeciętnego Kowalskiego", ale część z nich może wymagać pewnego obycia z komputerem. W razie niejasności poproś znajomego informatyka o pomoc w konfiguracji.

Akcja	Opis neutralizowanego ataku	UWAGI i przydatne programy
1. Zaszyfruj *cały* dysk twardy (tzw. *full disk encryption*)	Chroni przed nieuprawnionym dostępem do danych, np. na skutek kradzieży lub w sytuacji w której zostawiłeś sprzęt bez opieki w hotelowym pokoju, schodząc na śniadanie (tzw. atak Evil Maid).	Programy: - TrueCrypt dla Windows (http://www.truecrypt.org/ projekt przechodzi pewne niezrozumiałe zmiany, został nagle zamknięty przez developerów, zaleca się korzystanie z innego oprogramowania lub pozostanie przy wersji 7.1.a) - FileVault2 dla Mac OS X (wbudowany w system, w zakładce "Security & Privacy" w systemowych preferencjach). Po skonfigurowaniu FileVaulta uruchom terminal i wydaj polecenie: `sudo pmset -a hibernatemode 25 destroyfvkeyonstandby 1` które będzie kasowało klucz z pamięci podczas hibernacji laptopa, chroniąc przed atakami Evil Maid i Cold Boot. - BitLocker dla Windows (wbudowany w system) - dm-crypt dla Linuksa (wbudowany w większość dystrybucji) Niezależnie od szyfrowania, warto wykonywać **regularny backup (tzw. kopię zapasową)**, ponieważ w przypadku szyfrowanych dysków, zmiana/błąd jednego bitu może uniemożliwić dostęp do wszystkich danych. Niektóre z dysków twardych wspierają szyfrowanie na poziomie kontrolera (co nie wymaga instalacji dodatkowego oprogramowania, a odpowiedniej konfiguracji, tj. ustawienia hasła w BIOS). Oczywiście to czy ufać algorytmom danego producenta pozostawiamy do oceny samemu użytkownikowi -- pytanie kluczowe: czy lepiej, aby do danych miał dostęp producent czy złodziej?

2. Regularnie aktualizuj oprogramowanie	Chroni przed większością ataków masowych, typu: - otwarcie złośliwego pliku PDF, - wejście na złośliwą stronę internetową Każde popularne oprogramowanie posiada błędy bezpieczeństwa (tzw. dziury). Są one odnajdowane i łatane na bieżąco. Aby je eliminować należy regularnie aplikować aktualizacje, inaczej powalamy każdemu gimnazjaliście korzystającemu z tzw. "programów do hackowania" (np. metasploita) na przejęcie naszego komputera	Włącz automatyczną aktualizację w każdym z programów, z których korzystasz na komputerze (zwłaszcza w przeglądarce internetowej) Jeśli musisz "ręcznie" ściągnąć aktualizację, ściagaj ją ze strony producenta po HTTPS (w przeciwnym razie, ktoś kto jest na trasie twojego połączenia, mógłby podmienić ściągane dane na złośliwe). Przydatne programy: - Windows: PSI (Personal Security Inspector) http://secunia.com/products/consumer/psi/ - Linux: apt-get update && apt-get upgrade - Mac OS X: Ustawienia -> Aktualizacje Od czasu do czasu warto także przejrzeć uprawnienia, jakie nadałeś zewnętrznym aplikacjom na swoich kontach: - Facebooka: https://www.facebook.com/settings?tab=applications - Google: https://accounts.google.com/b/0/IssuedAuthSubTokens?hl=en
3. Stosuj unikatowe hasła, czyli różne do każdego z serwisów/usług **...i włącz 2 factor authentication (dwuskładnikowe uwierzytelnienie)**	Chroni przed nieuprawnionym dostępem do Twoich danych (kont w serwisach internetowych). Najczęściej atakujący zdobywają dostęp do twojego konta w serwisie X, dzięki temu, że udało im się włamać na serwis Y, w którym także miałeś zarejestrowane konto na ten sam adres e-mail/login. Ponieważ serwis Y był od dawna zapomniany (np. studenckie forum) i zarządzany przez niekompetentną osobę, w momencie ataku pracował pod kontrolą nieaktualnego oprogramowania. Dzięki temu, atakujący wykorzustując znany od dawna błąd, wykradli z niego bazę danych. W bazie znajdowało się twoje	Atakujący są w stanie sprawdzać ponad 5 milionów haseł na sekundę. Dlatego aby opóźnić złamanie hasła, hasło powinno być: - **niesłownikowe** (hasła: qwerty, qazwsx, albo kasia123 lub defibrylator nie są dobre, ponieważ znajdują się w słownikach służących do łamania haseł. Te słowniki zawierają wszystkie poprawne słowa z j. polskiego, angielskiego, itp, oraz popularne kombinacje "123456", a także wersje powyższych słów pisane od tyłu, na przemian małymi i dużymi literami, a także z przyrostkami (ang. suffix): "123", "098", "111", "000", "123!", "1!" itp. na końcu). - **nieszablonowe** (nie twórz ich według szablonu. np. *MojeTajneHasloDoAllegro* - bo w przypadku wycieku haseł z Allegro, atakujący domyśli się, że twoje hasło do Facebooka to zapewne *MojeTajneHasloDoFacebooka*) - **długie i skomplikowane** (im dłuższe hasło i im więcej znaków posiada, tym dłużej zajmie atakującemu jego łamanie). *(te same porady dotyczą także odpowiedzi na pytania "przypominające hasło")*

	hasło, niestety takie same jak do serwisu X. *Do czego prowadzą tego typu ataki -- przeczytaj: http://niebezpiecznik.pl/post/od-wycieku-prawie-20-000-hasel-do-wrzucania-nagich-zdjec-ofiar-na-facebooka/* Inną przyczyną włamań na konta jest obejście formularza logowania poprzez formularz "resetu" hasła. Z tego powodu nie ustawiaj pytania "przypominającego hasło" na "Ulubiony kolor" z odpowiedzią "Czarny", gdyż jest to bardzo łatwe do odgadnięcia. **Dwuskładnikowe uwierzytelnienie** ochroni twoje konto, w przypadku przejęcie Twojego hasła (np. po logowaniu się do Facebooka na komputerze kolegi, w hotelu, itp.). Atakujący aby mieć dostęp do Twojego konta potrzebuje także twojego telefonu (a miejmy nadzieję, że nie zostawiłeś go przy cudzym komputerze, na którym wpisałeś hasło ;).	**Hasła twórz i zapisuj w managerze haseł** (np. KeePass, który jest dostępny dla Windows/Linux/Mac/iOS/Android). Dzięki temu musisz pamiętać tylko jedno hasło - do managera. Resztą zajmie się on. **Dwuskładnikowe uwierzytelnienie można włączyć w:** - Facebooku http://niebezpiecznik.pl/post/facebook-wprowadza-nowe-zabezpieczenia/ - Google GMail http://niebezpiecznik.pl/post/google-wprowadza-dwuskladnikowe-uwierzytelnienie/ - Dropbox - Twitter http://niebezpiecznik.pl/post/twittera-nowe-i-trzeba-przyznac-ciekawe-podejscie-do-dwuskladnikowego-uwierzytelniania/ - Evernote ...oraz innych serwisach, być może te, z których korzystasz już je mają -- sprawdź to ...i włącz! ***UWAGA!*** *Upewnij się, że wiesz jak się zalogować za pomocą specjalnych kodów awaryjnych, na wypadek gdybyś stracił dostęp do swojego telefonu. Wydrukuj je i przechowuj w bezpiecznym miejscu.*
4. Podnieś bezpieczeństwo przeglądarki Firefox i Google Chrome	Podsłuchaniem twojego ruchu internetowego i kradzieżą tożsamości/danych	Przeglądarka internetowa to zapewne program w którym spędzasz najwięcej czasu, dlatego: 1. Upewnij się, że nie korzystasz z przeglądarki innej niż Google Chrome (albo jej zoptymalizowanego odpowiednika) lub Firefox lub Opera ;) *Zaletą Google Chrome jest sandboxing (separacja), minimalizujący skutki ataków, ale wadą przekazywane pewnych statystyk do Google (co można ograniczyć w ustawieniach lub wykorzystać klon przeglądarki Google Chrome zorientowany na prywatność, np. SRWare Iron lub Chromium, która domyślnie nie wysyła statystyk i raportów o błędach).* 2. Wyłącz wtyczkę Java (oraz inne których nie potrzebujesz, a zapewne nie potrzebujesz niczego poza Flashem)

		2. Włącz funkcję "click-2-play" dla wtyczek. Dzięki temu, żaden aplet Flasha na stronie nie wystartuje sam z siebie (nawet te "niewidzialne" 1x1 px). Aby aktywować np. aplet filmiku na YouTube, będziesz musiał najpierw w niego kliknąć Dla Chrome: Ustawienia → Pokaż ustawienia zaawansowane... → Ustawienia treści → Wtyczki → Kliknij, by uruchomić Instrukcje dla innych przeglądarek 3. Zainstaluj przydatne rozszerzenia, zwłaszcza te: - **NoScript** (blokada JS dla Fx) - **NoScripts** (blokada JS dla Chrome) - **HTTPS Everywhere** (wymusza szyfrowane połączenia, jeśli są możliwe) 4. Jeśli prywatność jest dla Ciebie równie ważna co bezpieczeństwo, skonfiguruj ciasteczka w tryb "**No third party cookies**" - ochroni to Twoją prywatność przed trackingiem reklamowym (por. http://niebezpiecznik.pl/post/grozne-ciasteczka-flashowe/)
5. Korzystaj z VPN, łącząc się z nieswoją siecią (Wi-Fi)	Chroni przed podsłuchaniem twoich danych. W przypadku darmowych hotspotów (np. w Starbucks, McDonalds, itp.) oraz sieci z szyfrowaniem WEP -- każdy inny użytkownik sieci widzi cały twój ruch internetowy. Jeśli nie korzystasz z szyfrowanych protokołów, będzie można Cię podsłuchać i np. przechwycić np. twoje hasła. Atakujący może także celowo podstawić fałszywą, niezaszyfrowaną sieć o nazwie (SSID) takiej jak sieć, do której wcześniej się łączyłeś. Twój komputer połączy się z nią automatycznie, co pozwoli na podsłuch połączenia przez atakującego.	Wszelkie błędy certyfikatów wyskakujące podczas połączenia lub komunikaty informujące o zmianie odcisku/fingerprinta klucza traktuj jako atak MITM i nie akceptuj takiego połączenia. Włączaj np. firmowy VPN korzystając z niezaufanych sieci Wi-Fi (hotele, lotniska, biura klienta). Jeśli nie masz firmowego VPN-a, możesz kupić tego typu usługę za grosze lub stworzyć ją samemu. Bardzo prosty VPN możesz zrobić sam przy pomocy dowolnego serwera VPS z SSH (polecamy Digitalocean jako najtańszy hosting VPS-ów, z gotowymi obrazami, dyskami SSD i wysokimi limitami, za 5USD na miesiąc w rozliczeniu sekundowym - obecnie podanie kodu **2MO512** lub **10TOSHIP** przy rejestracji, po podaniu danych płatniczych dodaje 10USD na koncie, czyli 2 miesiące zabawy). Jeśli już masz gdzieś konto SSH, zaloguj się do niego w ten sposób: `ssh login@serwer -D 9090` a następnie w przeglądarce ustaw SOCKS proxy na port 9090. **Uwaga**! Dalej można przechwycić twój ruch generowany przez inne niż przeglądarka

		oprogamowanie zainstalowane na twoim komputerze (systemowe SOCKS proxy rozwiąże problem - por. http://superuser.com/questions/319516/how-to-force-any-program-to-use-socks a potem wydaj polecenie: "netsh winhttp import proxy source=ie"). Dodatkowo warto zdawać sobie sprawę, że ruch jest szyfrowany jedynie do serwera SSH -- jeśli więc ktoś podsłuchuje serwer SSH, na wyjściu będzie w stanie podejrzeć twoje niezaszyfrowane połączenia (dlatego korzystaj tam gdzie to możliwe z szyfrowanych protokołów, tj. np. HTTPS). Alternatywą do VPN-a jest także sieć TOR (https://www.torproject.org/) - ale podobnie jak z serwerami VPN/SSH -- na wyjściu z tej sieci niezaszyfrowany ruch kierowany do serwera docelowego może zostać przechwycony.
6. Korzystaj z firewalla	Chroni przed zwiększaniem powierzchni ataku poprzez wystawienie "wszystkim" usług z Twojego komputera (np. domyślnie włączonego w Windows udostępniania plików przez protokół SMB)	Ustaw blokadę wszystkich połączeń przychodzących do Twojego komputera. Nie utrudnia Ci to korzystania z komputera, pod warunkiem, że nie jesteś serwerem WWW, lub nie udostępniasz innej usługi innym internautom - ale jeśli to robisz, to zapewne wiesz na jakim porcie działa usługa i będziesz w stanie założyć odpowiednią regułę na firewallu. GUI do firewalla na Mac OS X: http://www.hanynet.com/icefloor/ Rozważ instalację oprogramowania, które będzie także limitowało ruch wychodzący z twojego komputera. Dla Mac OS X będzie to **LittleSnitch,** w przypadku Windowsa interaktwne limitowanie ruchu wychodzącego umożliwia program **ZoneAlarm**
7. Korzystaj z antywirusa i konta z ograniczonym uprawnieniami (nie admina)	Antywirus chroni przed znanymi wirusami, a korzystanie z konta bez przywilejów administratorskich nie pozwoli złośliwemu oprogramowaniu na całkowite przejęcie systemu.	Antywirusy da się obejść i jest to stosunkowo proste zadanie. Nie mniej jednak warto z nich korzystać, bo doskonale odsiewają znane (tj. stare) i masowe zagrożenia. Nie trzeba kupować antywirusa - wiele z firm ma wersje bezpłatne i są one równie (nie)skuteczne co ich "płatne" odpowiedniki. Rozważ instalację dodatkowych narzędzi chroniących przed złośliwym oprogramowaniem, takich jak: - **Bit9**, jako alternatywę do antywirusa, polegającą na whitelistingu programów - **EMET** (unieszkodli wiele exploitów, jeśli już dotrą na Twój system)

		Nie korzystaj z konta administratora do pracy na co dzień. Załóż osobne konto.
8. Zastanów się, co umieszczasz w sieci	Chroni przed kompromitacją, wyciekiem poufnych danych	Wszystko co umieszczasz w internecie lub wysyłasz e-mailem nawet do 1 wybranej osoby, traktuj jako **publicznie dostępne. Zawsze. Dla wszystkich**. Skrzynka e-mail twojego zaufanego odbiorcy może zostać upubliczniona na skutek ataku. Prywatna galeria zdjęć na Facebooku może nagle stać się dostępna dla każdego internauty na skutek czasowego błędu w serwisie. Takie sytuacje miały już miejsce (por. http://niebezpiecznik.pl/post/dziura-w-facebooku-ujawnia-prywatne-zdjecia-uzytkownikow/). Wszystko co umieszczasz w internecie, ma dużą szansę zostać tam na zawsze, czy tego chcesz, czy nie, por. http://archive.org
9. Załóż hasło na BIOS	Chroni przed kradzieżą sprzętu/danych Atakujący nie odpali Twojego komputera z LiveCD/USB i nie uzyska dostępu do niezaszyfrowanych części dysku, obchodząc uwierzytelnienie (utrudni mu to także nadpisanie MBR dysku z poziomu zewnętrznego systemu)	Dysk zawsze można wymontować fizycznie, i jeśli jest niezaszyfrowany (patrz pkt. 1), to klops. W komputerach Mac brak jest BIOS-u ale można ustawić “startup password” Pamiętaj! Hasło na BIOS często można zresetować (np. zworką) lub podać domyślne hasło producenta, jeśli ma się dostęp fizyczny do płyty głównej. O ile nie da się przed dostępem fizycznym zabezpieczyć skutecznie, to warto to wykrywać - najprostszą metodą będzie korzystanie z lakieru do paznokci. Ochronę fizyczną mogą także podnieść odpowiednie akcesoria.
10. Pamiętaj że jeśli wybrałeś brak szyfrowania całego dysku twardego to patrz punkt 1.	Nic nie chroni cię w przypadku kradzieży przed - wyciekiem twoich poufnych danych, - kradzieżą tożsamości, - kompromitacją poprzez opublikowanie np. twoich prywatnych zdjęć na twoim Facebooku, itp.	Możesz jednak odzyskać sprzęt, namierzając złodzieja… o ile przed kradzieżą zainstalowałeś na swoim komputerze/telefonie oprogramowanie typu “przyjazny trojan”, a urządzenie nie zostało przez złodzieja wyłączone: - **http://preyproject.com/** (Windows, Mac, Linux, Android, iOS) - **FindMyiPhone** (pozwala również na odnajdywanie Macbooka, iPada) - https://icloud.com - **Android Device Manager** Pomimo ustalenia przybliżonego miejsca przechowywania sprzętu do "namierzenia złodzieja", i "odzyskania sprzętu" droga może być długa i wyboista. Zawsze jednak można spróbować wymuszenia usunięcia danych.

		Uwaga! Dobrze zabezpiecz dostęp do kont zarządzających ww. programami. Warto mieć świadomość, że w przypadku ich przejęcia skutki mogą być tragiczne, por. http://niebezpiecznik.pl/post/jak-amazon-pomogl-zhackowac-apple/
