CYBERBEZPIECZEŃSTWO I CYBEROBRONA

instrukcja

dla osób w sytuacji zagrożenia

Lech Mikulski

1 października 2023 r.

Niniejsza publikacja została przygotowana i opublikowana staraniem niżej wymienionych.

Autor: Lech Mikulski

Korekta: Joanna Preizner

Kontakt: cyber@lechmikulski.com

Strona: www.lechmikulski.com

Data premiery: 1 października 2023 r.

UWAGA!

JEŻELI PODEJRZEWASZ,

ŻE

TWÓJ SMARTFON

JEST INWIGILOWANY,

ZANIM ZACZNIESZ CZYTAĆ DALEJ,

WŁĄCZ

TRYB SAMOLOTOWY

LUB

TRYB OFFLINE

SPIS TREŚCI

Szanowna Czytelniczko, Szanowny Czytelniku,

dziękuję, że sięgasz po tę publikację w sytuacji, w której się właśnie znajdujesz. Jest duża szansa, że ktoś uznał, iż dobrze będzie, jeżeli zapoznasz się z jej treścią. Możliwe też, że w skutek nagonki medialnej sam uznałem, że warto Ci ją przesłać, zapewne na Twój oficjalny adres e-mail.

Bardzo możliwe, że gdybyśmy spotkali się na sali wykładowej lub w innej sytuacji zawodowej, naturalnym byłoby używanie adekwatnych tytułów, lub przynajmniej zwracanie się per Pani / Pan. Nie wykluczam, że jeśli się kiedyś spotkamy, tak właśnie będzie, ale na potrzeby zwięzłego przekazania treści przyjąłem, że mogę się zwracać do Ciebie w sposób bezpośredni. Nie odbierz tego, proszę, jako brak szacunku – wynika to wyłącznie z chęci usprawnienia komunikacji i skupienia na treści.

Przyjmuję tu pewne założenia dotyczące tego kim jesteś, i potrzebnej Ci w tym momencie wiedzy. Zakładam, że jesteś osobą publiczną, lub zdarzyło Ci się ostatnio zaistnieć w przestrzeni publicznej, a może i medialnej.

Z dużym prawdopodobieństwem możesz być, jak sądzę, dziennikarką lub dziennikarzem, badaczką lub badaczem, autorką lub autorem książek, które z uwagi na swoją tematykę, rzetelność badawczą i niezgodność z wiodącą myślą partyjną są niewygodne dla rządzących.

A może jesteś lekarką lub lekarzem, którzy znają znaczenie słów *primum non nocere* i doświadczasz szykan, bo odmówiłaś/łeś podpisania tzw. klauzuli sumienia, albo pozwoliłaś/łeś sobie na publiczne skrytykowanie dowolnego wysoko postawionego polityka partii rządzącej.

Możesz też być odważną Kobietą lub zdeterminowanym Mężczyzną, dla których niezależnie od życia zawodowego udział w różnego typu wiecach, manifestacjach i protestach stały się w ostatnich latach obywatelskim obowiązkiem i codziennością. Jeżeli można Cię nazwać Aktywistką lub Aktywistą, to jestem pewien, że moje opracowanie powinno Cię zainteresować.

Podobnie będzie, jeśli praworządność i Konstytucja RP są dla Ciebie ważne, i z racji wykonywanego zawodu bronisz praw innych albo orzekasz – oczywiście, o ile nie zawieszono Cię za obronę wartości demokratycznych i polskiej racji stanu.

Przeczytaj ten tekst uważnie, jeżeli ze względu na transparent, którego treść nie spodobała się komuś ze służb mundurowych, zostałaś/łeś spisana/y przez Policję, wezwana/y na przesłuchanie i grozi Ci postawienie zarzutów, których konsekwencją może być pozbawienie wolności. (Tak było w przypadku piszącego te słowa, a zainteresowani znajdą tę historię na samym końcu, jako uzupełnienie wcześniejszych rozdziałów.)

Pisząc te słowa myślę też o polityczkach i politykach opozycji. Mam nadzieję, że jeśli działasz w opozycyjnej partii lub organizacji broniącej praw człowieka, to masz wsparcie specjalistów ds. Cybersecurity. Jeżeli nie – przeczytaj niniejszy e-book.

Te kilkadziesiąt stron to mój wyraz szacunku dla Ciebie i dla Twojej aktywności. To moje *dziękuję*, bo bardzo możliwe, że na co dzień korzystam z Twojej wiedzy, doświadczenia, profesjonalizmu, determinacji i odwagi. Dlatego właśnie chciałbym Ci podziękować tak, jak umiem – przekazując ten e-book oraz zawartą w nim wiedzę. Jeżeli dostajesz go e-mailem od kogoś ze znajomych – sprawdź na mojej stronie (www.lechmikulski.com), czy masz najnowszą wersję (nie wykluczam aktualizacji treści). Znajdziesz tę informację na dole okładki.

Szczególne podziękowanie zechce przyjąć ode mnie również anonimowy dla mnie Pan Mecenas, który 14 czerwca 2020 roku na Placu Nowym na krakowskim Kazimierzu nie dopuścił do zatrzymania mnie i mojej żony Joanny Preizner[1]. To o tyle symboliczne, że nasza milcząca manifestacja przeciwko nazywaniu przez władzę ideologią ludzi ze środowiska LGBT była dwuosobowa i prawdopodobnie była pierwszym tego rodzaju wystąpieniem w Polsce. Gdybyśmy wtedy zostali zatrzymani, policja mogłaby odnotować sukces w postaci zatrzymania wszystkich manifestantów protestujących przeciwko mowie nienawiści używanej przez polityków partii rządzącej, starających się zbić na wykluczaniu innych kapitał polityczny w trakcie prowadzonej wówczas kampanii wyborczej. Panie Mecenasie, serdecznie dziękuję – w swoim i żony imieniu. Mam nadzieję, że te słowa dotrą do Pana.

Zapraszam do lektury.

[1]Aleksander Gurgul, *Minister Gliński w Krakowie o LGBT: "Seksualność jest piękna, ale nie w przestrzeni publicznej"*, https://krakow.wyborcza.pl/krakow/7,44425,26031482,minister-glinski-w-krakowie-o-lgbt-seksualnosc-jest-piekna.html (dostęp: 23.09.2023).

Siostry Hakerki, Bracia Hakerzy,

jeżeli z uwagi na swoje doświadczenie ktoś z Was uzna, że trzeba w tej publikacji doprecyzować jakiś wątek, albo czegoś w niej brak – proszę o kontakt. Zakładam, że dzięki cyfrowemu wydaniu możliwe są korekty i uaktualnienia.

Obiecuję umieścić podziękowania w uaktualnionej wersji. To projekt Non-profit. Zamiast ponownie wychodzić na ulicę, postanowiłem podzielić się swoją wiedzą i wesprzeć innych, którym nie odpowiada świat organizowany nam przez prawicowych polityków i katolickich fanatyków.

Jeżeli dzięki Waszej wnikliwej lekturze i sugestiom wspólnie sprawimy, że zwykli ludzie będą bezpieczniejsi, to jakiś kawałek świata będzie lepszy. A to już dużo.

Manifest

Masz prawo do prywatności. Obejmuje to zachowanie plików, dokumentów, notatek i myśli tylko dla siebie. Masz prawo używać współczesnych narzędzi technicznych bez strachu, że ktoś będzie starał się wykraść Ci zapisywane za ich pomocą i znajdujące się na nich dane. Masz prawo decydować co, kiedy, jak i czy w ogóle zostanie upublicznione.

Masz prawo do tajemnicy zawodowej i do ochrony swoich źródeł, klientów czy pacjentów. Ufają Ci, dlatego masz nie tylko prawo bronić ich prywatności – masz też taki obowiązek.

Jeżeli coś ma swój cyfrowy odpowiednik, jest narażone na zdalny dostęp osób trzecich. Gdyby nie istniało w tej formie – nie mogłoby zostać wykradzione przez osoby niepowołane. Truizm? Utopia w XXI wieku? Miej to na uwadze zapisując dowolny cyfrowy plik.

Osoby zaangażowane w PRL w działalność opozycyjną często powtarzały:

Jeśli pomyślałeś – nie mów.

Jeśli powiedziałeś – nie pisz.

Jeśli napisałeś – nie podpisuj.

Jeśli podpisałeś – to się nie dziw.

W cyfrowym świecie jest jeszcze trudniej. Jeśli zapisałeś plik - nie udostępniaj. Jeśli udostępniasz – licz się z tym, że plik może zostać potencjalnie wykradziony. Nie ma znaczenia, czy prawo na to zezwala, czy nie. W sytuacji zainteresowania Tobą przez służby liczy się tylko to, czy dany plik da się pozyskać.

Założenia wstępne

Jeżeli zdarzyło Ci się przeczytać już jakąś publikację o Cyberbezpieczeństwie, to możliwe, że część zawartych tu informacji będzie Ci znana. Mogą pojawić się nazwy narzędzi, których być może już używasz. Potraktuj wówczas ten tekst jako propozycję pewnego spojrzenia na możliwości, jakie one wspólnie dają.

Zakładam, że trzeba zbudować jednorodny i przede wszystkim bezpieczny ekosystem, którego głównym zadaniem jest ochrona Ciebie i Twojej prywatności przed policją i innymi służbami, które z przekonaniem lub bez, przystępują do nadmiernej inwigilacji obywateli, chcąc przypodobać się rządzącym.

Chciałbym tu podkreślić, że nie uważam instytucji policji, służb specjalnych czy wywiadowczych za wcielenie wszelkiego zła. Jeżeli sytuacja tego wymaga, sam również wzywam odpowiednie służby i zdarzało mi się uzyskać potrzebną pomoc. Nie mam wątpliwości, że są one potrzebne, ale zamiast zająć się prawdziwą przestępczością czy obroną Państwa Polskiego przed atakiem zewnętrznym, w ostatnich latach przyczyniają się znacząco do ugruntowywania przewagi totalitarnej władzy nad obywatelem.

Bezkarność policjantów, którzy potrafią zaatakować gazem i pałkami teleskopowymi legalnie protestujące kobiety, złamać rękę podejrzanej podczas zatrzymania, przetrzymywać bez leków osobę w wieku senioralnym, czy domagać się rozebrania od bezbronnej kobiety, to coś, co nigdy nie powinno mieć miejsca. Nie mam wątpliwości, że w demokratycznym państwie policja powinna stać na straży prawa i sprawiedliwości, ale w Polsce te dwa słowa to nazwa partii, która jest synonimem terroru wobec kobiet, aktywistów i ludzi broniących praw człowieka. Stoi też za licznymi przypadkami łamania Konstytucji i prawa. Swoimi działaniami członkowie tej partii sprawili, że słowa wykorzystane w jej nazwie zostały pozbawione oryginalnego znaczenia.

Dlatego zakładam, że napisanie tej publikacji jest zasadne. Każdy powinien mieć możliwość samodzielnie zdecydować, co z cyfrowego życia pozostanie prywatne. Narzędzia i metody wspomniane na kolejnych stronach stają się niezbędne do zachowania wolności osobistej. Ich znajomość i stosowanie jest formą obrony przed przemocą i bezprawiem, których dopuszcza się państwo wobec swoich obywateli.

Przyjmuję, że powinno to zostać opisane w sposób przystępny i pozwalający na wykorzystanie również osobom nieobeznanym z techniką. Zabezpieczenie siebie, swoich danych i swoich działań w Internecie częściej będzie kwestią nawyków i świadomego używania narzędzi niż technicznej znajomości zasad ich działania.

Tym, co może odróżniać tę publikację od pozostałych z zakresu cyberbezpieczeństwa, jest inne umiejscowienie przeciwnika. Naszym zadaniem nie jest zabezpieczenie się przed śledzeniem przez tę czy inną korporację, reklamodawców czy serwis internetowy używający plików cookie. Haker, którym chyba najczęściej się nas straszy, nie jest złym wilkiem w tej bajce. Nasz przeciwnik ma dużo większe możliwości i w odróżnieniu od wymienionych – nie atakuje od frontu, a po cichu zakrada się tylnym wejściem (z ang. Backdoor).

Odwrócenie źródła zagrożenia sprawia, że musimy zapewnić sobie cyfrowe bezpieczeństwo w zupełnie inny sposób. Niezależnie od tego, jak dobrze zabezpieczymy dostęp do naszych danych od frontu, prawdziwe zagrożenie już czai się za tylnymi drzwiami. Nie naciśnie klamki, wejdzie „z buta”.

Twój przeciwnik

Twoim przeciwnikiem jest opresyjny aparat państwa. Tego samego, które utrzymujesz ze swoich podatków. Ma nad Tobą oczywistą przewagę, ale nie jesteś bez szans. Nastaw się, że służby nie będą Cię traktować z należytym szacunkiem, a niektórzy z ich pracowników będą w trakcie spotkania patrzeć na Ciebie z pogardą.

Twój przeciwnik nie śpi. Ma nieograniczony budżet na swoje działania i znaczne zasoby ludzkie, które zostaną przeciwko Tobie wykorzystane. Służby nie uważają Cię jednak za godnego siebie przeciwnika. Dzięki temu mogą łatwo popełnić błąd – upojone swoją wszechmocą, nie doceniają możliwości, które masz i które możesz wykorzystać, by się zabezpieczyć.

Każde zderzenie na linii „inwigilujące państwo vs. Obywatel" będzie miało swoją dynamikę i natężenie. Jeżeli właściwie rozpoznasz symptomy ataku, to nawet w trakcie jego trwania masz duże pole manewru.

Do pewnego stopnia Twój przeciwnik stara się ukryć swoje działania, stąd możliwe, że będzie Cię atakować w dość nietypowych porach. Jest to niedogodność, która wydłuża jego pracę, a Tobie daje czas potrzebny na obronę.

Twój przeciwnik nie wie też, czego szuka w Twoich danych. Potrzebuje czegokolwiek, co może zostać użyte przeciwko Tobie. Jeżeli wiesz, co może go interesować – należy zabezpieczyć to w pierwszej kolejności i zatrzeć ślady.

CZĘŚĆ I – KOD ŻÓŁTY

Stan zagrożenia

Stan zagrożenia to okres, w którym służby będą się Tobą interesować. To nie jest stan permanentny i przebiega z różnym natężeniem. Okresy najbardziej uciążliwych działań będą przeplatały się ze spokojniejszymi, w których będziesz przedmiotem znikomego lub żadnego zainteresowania służb. Po jakimś czasie, może jednak nastąpić ponowne, kontrolne sprawdzenie Ciebie i Twoich danych.

Trudno uważać się cały czas za cel inwigilacji. Nie dajmy się zwariować. Bez smartfonu, telefonu, e-maila czy korzystania z pełnego spektrum możliwości, które daje Internet jako sieć i jako technologia – niemożliwe jest normalne funkcjonowanie. Dlatego dla własnego bezpieczeństwa należy umieć określić, jak duże i jak realne niebezpieczeństwo nam grozi w danej chwili.

Porównując nasze poziomy bezpieczeństwa do kolorów świateł, możemy określić je w sposób następujący:

Kod zielony – sytuacja normalna, nie występuje zagrożenie, nie spodziewamy się naruszenia bezpieczeństwa naszych danych. Nasze e-maile nie są przedmiotem zainteresowania żadnych służb. Rozmowy nie są rejestrowane, a wiadomości tekstowe nie są przechwytywane. (Piszę to z polskiej perspektywy, np. z amerykańskiej wyglądałoby to inaczej.)

Ten poziom dotyczy większości osób, zwłaszcza jeżeli nie wyróżniają się szczególnie jakąś aktywnością publiczną.

Kod żółty – sytuacja zaczyna być niepokojąca. Z uwagi na planowany lub już odbyty udział w manifestacji, proteście, demonstracji, zaangażowaniu w działalność organizacji pozarządowych

lub opozycyjnych może się okazać, że nasze cyberbezpieczeństwo zostanie naruszone. Nasza komunikacja, w każdej formie, może stać się przedmiotem badania służb.

W przypadku szykowanej publikacji – postu, artykułu, książki itd., które mogą nie być zgodne z oficjalną narracją partii rządzącej lub ujawniają kolejne zakłamywanie przez nią rzeczywistości, również należy się liczyć z tym, że stopień zagrożenia cyberbezpieczeństwa wzrasta. To odpowiedni moment, by się przygotować na zmasowany atak.

Kod czerwony – z pewnością jesteśmy inwigilowani. Zagraża to osobie będącej celem oraz wszystkim, które się z nią kontaktują. Jakiś punkt zapalny wywołuje reakcję łańcuchową, a służby skupiają na Tobie uwagę. Aparat państwa zostaje wykorzystany przeciwko jednostce. Kluczowy staje się czas, a działania, które podejmiemy, decydują o tym, czy – a jeśli tak, jak bardzo – ucierpią nasza prywatność i nasze dane.

Pegasus – z uwagi na koszty śledzenia jednostki przy wykorzystaniu oprogramowania Pegasus, przypuszczalnie nie będzie to obecnie najczęściej stosowane narzędzie. Koszt śledzenia jednego numeru telefonicznego, jak podają źródła, może sięgać 100 000 $ (cena licencji za jeden numer telefoniczny).

Zgodnie z Informacjami podanymi przez FastCompany, wstępna opłata instalacyjna pobierana przez NSO wynosi $500,000, a zainstalowanie Pegasusa na 10 urządzeniach (Android lub iPhone) to koszt kolejnych $650,000[2]. Inwigilacja pięciu urządzeń BlackBerry ma kosztować $500,000, a pięciu użytkowników Symbiana – $300,000, jak podaje The Indian Express powołując się na dane z The New York Times z 2016 roku[3].

Zgodnie z informacjami TVN24, Polska miała wydać na zakup licencji Pegasusa 35 mln zł, płatnikiem miało być Centralne Biuro Antykorupcyjne (CBA)[4], a jak podaje Gazeta Wyborcza,

[2] DJ Pangburn, The Secretive Billion-Dollar Company Helping Governments Hack Our Phones, https://www.fastcompany.com/40469864/the-billion-dollar-company-helping-governments-hack-our-phones (dostęp: 30.09.2023). Potwierdzają te dane również inne źródła.
[3] Pranav Mukul , Anil Sasi, Cost of putting Pegasus in phones runs into crores, https://indianexpress.com/article/india/project-pegasus-cost-of-putting-pegasus-in-phones-runs-into-crores-7414323/ (dostęp: 30.09.2023).
[4] Reportaż wideo Leszka Dawidowicza, Czy Pegasus działa w Polsce i czy kupiło go CBA?, https://tvn24.pl/programy/czy-pegasus-dziala-w-polsce-ra964937-2311945 (dostęp: 30.09.2023).

zmieniając kwotę zakupu na 34 mln zł, środki te miały pochodzić z Funduszu Pomocy Pokrzywdzonym oraz Pomocy Postpenitencjarnej podlegającego Ministerstwu Sprawiedliwości[5].

Stąd musisz samodzielnie ocenić, czy z perspektywy rządzącej partii możesz być uważany za osobę tak zagrażającą ich bezpieczeństwu, że będą skłonni wydać tę kwotę z publicznych pieniędzy. Pegasus to oczywiście kod czerwony – można by dodać: permanentny.

Jeżeli rzeczywiście zakładasz, że to narzędzie jest używane przeciwko Tobie, mam nadzieję, że masz odpowiednie wsparcie.

Poziom Twojego zagrożenia będzie zależał od różnych czynników, które musisz samodzielnie ocenić. Przyjmij jednak, że jeżeli masz przeczucie, iż możesz być celem inwigilacji, bezpieczniej będzie uznać je za pewnik. Z dużym prawdopodobieństwem Twoje podejrzenie pojawia się z pewnym opóźnieniem. Dlatego zastanów się, czy w ostatnim czasie mogło mieć miejsce wydarzenie, które można uznać za punkt zapalny. Jeśli wiesz, że tak, to właśnie Twój kod zmienił kolor z ostrzegawczego żółtego na czerwony.

Jeżeli uważasz, że Twoja sytuacja ma Kod czerwony – sugestie, co należy zrobić, aby się bronić, znajdziesz w CZĘŚCI III - CYBEROBRONA na stronie 31.

[5] Autor: EF, CBA o Pegasusie: "Prowadzimy swoje działania w oparciu o przepisy polskiego prawa", https://wyborcza.pl/7,75398,25157818,cba-o-pegasusie-prowadzimy-swoje-dzialania-w-oparciu-o-przepisy.html (dostęp: 30.09.2023).

Sytuacja kryzysowa

Sytuacja kryzysowa to okres, w którym wiesz, że podlegasz inwigilacji. Jest krótszy niż stan zagrożenia. Trwa kilka dni do tygodnia. Sprawdzane są wtedy zdalnie Twoje skrzynki mailowe i chmury, kontrolowane są rozmowy telefoniczne. Początkowo możesz nie mieć tej świadomości, ale licz się z tym, jeżeli udało Ci się zwrócić na siebie uwagę policji lub służb.

Przykład: Jeżeli podczas prewencyjnego spisywania poproszono Cię o numer telefonu i adres e-mail, zapewne pod pozorem łatwiejszej i szybszej komunikacji z Tobą, to spodziewaj się, że nigdy nie dostaniesz e-maila z komendy, ale te, które masz w skrzynce zostaną pobrane i przeszukane. Numer telefonu zostanie wykorzystany do kontaktu, ale przede wszystkim do założenia podsłuchu. Cała operacja trwa kilka minut, dlatego możesz się tego spodziewać w ciągu kilku godzin od punktu zapalnego.

Jeżeli zostały fizycznie przejęte Twoje urządzenia – smartfon, tablet, komputer, dyski, pamięci przenośne itp. – masz pewność, że znajdujące się na nich dane oraz dane on-line również będą przedmiotem zainteresowania służb.

Punkt zapalny

Za punkt zapalny przyjmuję wydarzenie, które zapoczątkowuje działania służb przeciwko Tobie. To nie musi być udział w manifestacji - wystarczy celny, bolący ludzi władzy wpis w mediach społecznościowych. Nadmierne zainteresowanie nim może zwiastować nadchodzącą sytuację kryzysową.

Lawinę może tez uruchomić publikacja niewygodnego dla władzy tekstu. Oprócz medialnego dyskredytowania należy spodziewać się wtedy całej palety zakulisowych działań operacyjnych. Część z nich jest rozpoznawalna. Często ich uzupełnieniem będzie zmasowane zainteresowanie ze strony płatnych trolli. Zwróć, proszę, uwagę, czy wszystkie te symptomy pojawiają się równocześnie. Jeśli tak, to możesz mieć pewność, że właśnie ruszyła machina przeciwko Tobie.

CZĘŚĆ II – KOD CZERWONY

Inwigilacja

Proces inwigilacji jest totalny. Prowadzony jest wszelkimi dostępnymi metodami. Jeżeli policja/ służby poznały Twój numer telefonu i adres e-mail, w pierwszej kolejności będą prowadziły inwigilację właśnie w oparciu o nie. Oznacza to, że są one w pewnym sensie spalone – tak będą dalej nazywane.

Jeżeli z e-mailem powiązana jest dowolna chmura danych – są one w niebezpieczeństwie.

Przykład: Jeżeli używasz dysku Google oraz poczty Gmail, są one oczywiście ze sobą połączone. Jeżeli używasz innej chmury, ale adres poczty Gmail służy Ci za login, to ta chmura również może być widoczna / dostępna dla służb. Po adresie e-mail podanym policji możliwe jest połączenie Twojego konta w innym serwisie chmurowym z Tobą.

Podpowiedź 1: Jeżeli używasz swojego adresu e-mail jako loginu, a służby znają ten adres, zmień go na inny, niezwiązany z Tobą. Z dużym prawdopodobieństwem w bazie danych serwisu nadpisanie starego loginu nowym powinno usunąć dotychczasowy – przestanie on być przechowywany. Dzięki temu Twoje konto nie powinno zostać skojarzone z Tobą w razie wyszukiwania w bazie użytkownika o Twoim, jak już wiemy spalonym, adresie e-mail.

UWAGA! Wyjątkiem mogą tu być serwisy finansowe o rozbudowanej strukturze. Technicznie jest możliwe, by serwis przechowywał wcześniejsze loginy i hasła. Jeżeli widzisz, że serwis nie pozwala na użycie wcześniej wykorzystanych haseł, może mieć rozbudowaną bazę i przechowywać w niej usunięte przez użytkownika dane logowania. Jest to wykonalne, ale prostsze serwisy będą nadpisywać stare dane nowymi. Stąd proponowana zmiana sprawi, że dana chmura przestanie być kojarzona z Tobą poprzez Twój dotychczasowy, a obecnie spalony adres e-mail.

Podpowiedź 2: Mając dostęp do Twojego spalonego adresu e-mail służby są w stanie uzyskać dostęp do dowolnego serwisu, w którym masz ustawiony swój dotychczasowy e-mail jako służący do odzyskiwania zapomnianego hasła. Dlatego też im mniej serwisów będzie go wykorzystywać, tym lepiej.

Usuwanie spalonego adresu e-mail zacznij od tego, co należy zabezpieczyć w pierwszej kolejności – jeśli nie wiesz, czego mogą szukać służby, zacznij od portali społecznościowych. Pamiętaj, że przy zmianie np. hasła czy e-maila serwis zapewne prześle Ci na Twój spalony adres e-mail informację, że na Twoim koncie zaszła zmiana.

Po zmianie hasła znajdź e-mail z potwierdzeniem w swojej skrzynce mailowej, skasuj z niej i skasuj z kosza. Służby nadal będą mogły go odzyskać – do tego jeszcze wrócę. Na początku inwigilacji w pierwszej kolejności zostanie sprawdzona Twoja skrzynka mailowa, stąd jeśli e-maila nie ma w wiadomościach odebranych ani w koszu, służby nie wiedzą, że był. Nie zakładają, że wiesz o inwigilacji i że właśnie się zabezpieczasz.

Oprócz portali społecznościowych zabezpiecz w ten sam sposób wszystkie chmury, serwisy do zarządzania notatkami, zakładkami i w końcu hasłami (ważne!). Na koniec – portale związane z finansami. Służby i tak mają dostęp do Twoich kont bankowych, więc jest to symboliczne domknięcie procesu.

Proponowana kolejność wynika z tego, że portale społecznościowe stanowią kopalnię wiedzy. Wszystko, co w nich publikujesz, również po usunięciu, zostaje zachowane – do tego wątku jeszcze wrócę. Oczywiście należy się spodziewać, że da się znaleźć Twoje konto w serwisie, nazwijmy go roboczo, XYZ. Jeżeli będzie ono powiązane z Twoim e-mailem, służby mogą szybciej i łatwiej uzyskać do niego dostęp niż przez wystąpienie do firmy XYZ o przyznanie dostępu bez znajomości Twojego e-maila, powiązanego z danym kontem.

W nierównej walce ze służbami Twoim sprzymierzeńcem jest czas. Może się okazać, że przestaniesz być celem, zanim uzyskają dostęp do portalu XYZ. Trochę to przypomina sforę, która rzuca się na ofiarę, a odwołana odpuszcza. Dlatego ważne, by nie ułatwiać zadania przeciwnikowi. Jeżeli e-mail, który sprawdzają, nie jest powiązany z portalem XYZ, zyskujesz cenny czas. Mając dostęp do Twojego adresu e-mail, służby łatwo mogą uzyskać dostęp do szyfrowanych wiadomości na czacie, w tym prywatnych wiadomości przesyłanych przez użytkowników dowolnego serwisu.

Podsłuch rozmów telefonicznych

W zależności od konieczności może być prowadzony na różne sposoby. Możliwe jest podsłuchiwanie konkretnego numeru telefonicznego, konkretnej karty SIM, namierzanie konkretnego smartfonu (jako aparatu z numerem IMEI).

Pomijam tu zdalny podsłuch kierunkowy, bo wymaga on technicznie więcej zachodu niż przekierowanie Twoich wszystkich połączeń. Wiązałby się z wykorzystaniem dużych zasobów ludzkich i konieczności podążania za obiektem podsłuchu przez całą dobę. Zatem chociaż w filmach kryminalnych i sensacyjnych tajemnicza furgonetka śledząca podejrzanego może nadal robić wrażenie, w Twoim przypadku spodziewam się raczej przekierowania rozmów. (Tak też było i w moim.)

Numery telefonów są pozyskiwane nie tylko bezpośrednio, podczas spisania przez policję. Miej świadomość, że tak jak przestrzeń, w której się poruszamy, jest pokryta nadajnikami telefonii komórkowej, tak nasze przemieszczanie się jest odnotowywane. Dlaczego to jest ważne? Pokrycie w mieście będzie gęstsze, czyli dokładniejsze, niż poza miastem. Oznacza to, że dzięki logom nadajników da się zlokalizować wszystkie telefony, które znalazły się w danym obszarze o danej porze[6]. Każdy z numerów telefonów ma swojego przypisanego abonenta, dlatego ustalenie, kto znajdował się w danym miejscu np. na antyrządowej manifestacji, jest możliwe[7].

Dodatkowo, jeżeli jakaś aplikacja w naszym smartfonie wymaga włączonej lokalizacji, to w połączeniu z powyższym zostawiamy drugi ślad cyfrowy - dokładnie zaznaczoną trasę naszego przemieszczania się.

To nie wszystko. Przy okazji dużych manifestacji można też, tak jak to było w Warszawie, zobaczyć w pewnym ukryciu lub oddaleniu od trasy manifestacji specjalne SUV-y z

[6] Dobrze obrazuje to interaktywny projekt przygotowany przez The New York Times w 2019 roku. Charlie Warzel, Stuart A. Thompson, The Privacy Project, https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html (dostęp: 30.09.2023).

[7] Zob. Przemysław Malinowski, Chińska policja wykorzystuje dane z telefonów komórkowych do namierzania protestujących https://www.rp.pl/spoleczenstwo/art37536571-chinska-policja-wykorzystuje-dane-z-telefonow-komorkowych-do-namierzania-protestujacych (dostęp: 30.09.2023).
Marcin Maj, Idziesz na demonstrację (lub pasterkę)? Smartfona zostaw w domu, https://niebezpiecznik.pl/post/idziesz-na-demonstracje-smartfona-zostaw-w-domu/ (dostęp: 30.09.2023).

zamontowanym na pace obiektem przypominającym duży talerz satelitarny - tyle, że obustronnie wypukły. Z dużym prawdopodobieństwem widząc taki pojazd możemy się spodziewać namierzania, lub odwrotnie – prób zagłuszania komunikacji komórkowej. Jedno czy drugie – jest wymierzone przeciwko obywatelom.

Przypuszczenie trudne do zweryfikowania: Rozmowa prowadzona przez telefon komórkowy z zasady powinna być bezpieczna jako szyfrowana. Nasz głos powinien być na wejściu szyfrowany przez operatora telefonii komórkowej, w tej postaci przekazany dalej i następnie deszyfrowany przed przekazaniem odbiorcy. Zatem jeśli jeden numer telefonu łączy się z drugim numerem telefonu, pierwszym, co robią, jest wymiana kluczy szyfrowania. Byłoby to bezpieczne, gdyby nie fakt, że policja rozpoczynając podsłuch danego numeru, „wpina" się między rozmówców.

Niestety prawo zobowiązuje operatorów telefonii komórkowej do umożliwienia takiego działania. Stąd przekierowana rozmowa, jak można się domyślać, zostanie zdeszyfrowana dla strony trzeciej (podsłuchującej), a następnie ponownie zaszyfrowana i jako taka przekazana odbiorcy. Wydaje się to prawdopodobne, bo klucz szyfrujący jest znany operatorowi telefonii komórkowej (lub jest w jego posiadaniu), więc powinno to być technicznie możliwe.

Inną możliwością jest to, że klucz szyfrujący rozmówców jest na stałe udostępniany służbom i wtedy nie będzie ponownego szyfrowania po środku – nie będzie potrzebne. Z drugiej strony, byłoby to jednak trudniejsze do realizacji, bo każda rozmowa (zakładając, że pomiędzy różnymi abonentami) będzie odbywała się przy wykorzystaniu innego klucza. Dlatego hipoteza z ponownym szyfrowaniem po podsłuchaniu przez stronę trzecią może być bardziej trafna. Wyjaśniałoby to również, dlaczego podsłuchiwane rozmowy cechują się zauważalnym chwilowym opóźnieniem, które mogą zaobserwować rozmówcy. (Można wówczas odnieść wrażenie, że rozmówca odpowiada z opóźnieniem.)

Inwigilacja SMS-ów

Jeżeli rozmowy mogą być (i są) podsłuchiwane, to należy się również spodziewać, że SMS-y także są przechwytywane. SMS najlepiej porównać do pocztówki. Z założenia nie jest przechowywany przez sieć komórkową, lecz przesyłany przez infrastrukturę w postaci nieszyfrowanej. Standardowe SMS-y mają zostać zastąpione przez wiadomości w standardzie RCS, ale ich minusem, choć sama wiadomość ma być bezpieczniejsza, jest fakt, że takie wiadomości mają być przechowywane przez czas określony w latach (możliwe, że nawet 2-5 lat), również po ich skasowaniu przez nadawcę i odbiorcę.

Nie wykluczałbym też, że usunięty SMS nie może zostać odzyskany. Skasowany ze smartfonu jest odzyskiwalny. Nie mam wystarczającej wiedzy, by stwierdzić, czy z infrastruktury operatora jest w pełni usuwany po dostarczeniu. Zastanawiać mogą wszystkie dodatkowe informacje, które nawet po kilkuletnim okresie operator jest w stanie dostarczyć.

Będą to informacje z kim i o której godzinie osoba podsłuchiwana się kontaktowała. Ważne będzie, jak często ta komunikacja miała miejsce. Może być istotne, czy osoby komunikujące się ze sobą znajdują się w sprawdzanej lokalizacji. Na podstawie tych danych możliwe jest zwiększenie kręgu osób inwigilowanych, stworzenie profilu czy siatki kontaktów itp. W połączeniu z treścią wiadomości informacje te stanowią istotne dane. Również wielkość wiadomości w kb, czy w przypadku MMS-ów w MB, może okazać się istotna.

Inwigilacja E-maila

Zwykły e-mail nie jest bezpieczną formą komunikacji. W czasach, gdy został on wymyślony, nie zakładano istnienia wielu dzisiejszych zagrożeń. W swojej najprostszej postaci e-maile są widoczne dla każdego, zarówno w czasie przesyłania (w postaci tekstowej), jak i w czasie przechowywania na serwerze.

Najprościej pomyśleć o swoim adresie e-mail jak o folderze na dysku, tyle, że umieszczonym w chmurze. To, co znajduje się przed znakiem @, jest nazwą folderu. Każdy e-mail to plik tekstowy (.eml) w folderze.

Folder przechowuje dla nas firma hostingowa i przez pierwsze lata istnienia e-maila jego bezpieczeństwo opierało się na naszym zaufaniu do niej (w przypadku adresu e-mail we własnej domenie), lub do firmy oferującej „bezpłatne" miejsce na naszą prywatną korespondencję.

Z czasem e-maile uzyskały ochronę podczas przesyłania, ale nie podczas przechowywania, co oznacza, że e-mail jest dostępny dla osoby mającej dostęp do serwera, na którym się znajduje. Może nią być pracownik firmy hostingowej (lub oferującej usługę poczty), a także pracownik służb uzyskujący za ich pośrednictwem dostęp do konta inwigilowanej osoby.

Technicznie jest możliwe szyfrowanie konta każdego użytkownika, ale częściej stosowane będzie szyfrowanie całych dysków z e-mailami (różnych) klientów. Chociaż najpopularniejsze usługi poczty elektronicznej, w tym te początkowo bezpłatne, oferują w standardzie szyfrowanie e-maila, należy jednak mieć na uwadze, że dopóki klucz jest przechowywany przez firmę, która to oferuje, jest to jednoznaczne z możliwością deszyfrowania przez nią e-maili w razie nakazu udostępnienia ich służbom.

Może to też mieć związek z istniejącymi regulacjami prawnymi i współpracą pomiędzy wywiadami państw. Zainteresowani mogą znaleźć informacje dotyczące państw wchodzących w skład 5 Eyes Alliance, 9 Eyes Alliance i 14 Eyes Alliance[8], oraz państw z nimi stowarzyszonych. To oznacza, że poczta e-mail oferowana przez firmy funkcjonujące w krajach będących częścią

[8] Więcej na ten temat https://en.wikipedia.org/wiki/Five_Eyes (dostęp: 30.09.2023).

tych porozumień nigdy nie będzie bezpieczna. E-mail przechowywany w którymkolwiek z nich zawsze będzie dostępny dla służb.

Zwracają też uwagę doniesienia o fizycznym wtargnięciu przez służby do firm, które starały się zapewnić należytą ochronę e-maili klientów. Po fizycznym przejęciu serwerów firmy zostają zmuszone do zakończenia działalności[9].

O ile można zrozumieć i moralnie popierać działania wywiadów mające na celu zapobieżenie – przykładowo – rzeczywistym atakom terrorystycznym, handlowi ludźmi czy dystrybucji dziecięcej pornografii, to jednak stosowane obostrzenia prawne uderzają w głównej mierze w zwykłych obywateli i pozbawiają ich prawa do prywatności.

Korzystając z e-maila powinniśmy mieć na uwadze, że wbrew temu, co nam się wydaje, jest on ogólnodostępny. Jeżeli, dla naszej własnej wygody, oczekujemy, że nasze e-maile wyświetlają się nie tylko na komputerze, ale też w aplikacji na tablecie czy smartfonie, tym samym decydujemy, że będzie tu użyty protokół IMAP (ang. Internet Message Access Protocol). Przechowujemy wtedy korespondencję, często z kilkunastu lat, na zdalnym serwerze, do którego mamy dostęp. W razie zainteresowania ze strony służb lub fizycznego odebrania nam smartfonu podczas zatrzymania – mimowolnie gwarantujemy też ten dostęp innym.

Drugim protokołem, o odmiennym działaniu, będzie POP3. Ustawiając program pocztowy na komputerze (np. Thunderbird, Mailbird, czy Outlook) mamy możliwość rezygnacji z IMAP i wybrania POP3. Oznacza to, że nasze e-maile zostaną pobrane do programu mailowego i powinny zostać usunięte z serwera. Jeżeli nie ustawimy, by ich kopia została na serwerze, to zgodnie z założeniami tego protokołu e-maile w jedynej kopii powinny znajdować się na naszym komputerze (lub laptopie). Dla nas oznacza to tyle, że w pełni odpowiadamy za swoje e-maile – jeżeli stracimy komputer, to stracimy e-maile, bo ich kopii nie ma na serwerze.

---

[9] Przypuszczalnie to spotkało m.in. serwis https://ctemplar.com/ operujący z Islandii; więcej: https://restoreprivacy.com/email/reviews/ctemplar/ (dostęp: 30.09.2023). Co interesujące, podczas rozmowy przeprowadzonej z https://deepai.org/chat w dn. 21.05.2023, na moje dociekania o to, co mogło się stać z usługą, czat użył sformułowania „ctemplar.com was closed after their servers were seized by authorities due to a legal issue." Gdy próbowałem uzyskać jakieś informacje i podkreśliłem, że wyniki wyszukiwania zdają się być wyczyszczone, Chat stopniowo przestawał udzielać odpowiedzi, a następnie zaraportował, już raczej nie do mnie, a do obsługi czatu, jak myślę, „The user requested a link to an article on ctemplar.com seizure as Google provided no results." Po czym zakończył rozmowę, co nigdy wcześniej mnie nie spotkało. Inną interesującą usługą miał szansę być criptext.com, z pozoru działa, ale w trakcie pisania tego e-booka nie dało się założyć konta i trudno jednoznacznie stwierdzić, czy Mayer Mizrachi, jeden z twórców serwisu, przebywa nadal w areszcie. Więcej: https://es.wikipedia.org/wiki/Mayer_Mizrachi (dostęp: 30.09.2023).

Tyle w teorii, a w zależności od usługi, z której korzystamy (szczegóły powinny być opisane w polityce prywatności), nasze e-maile mogą być dodatkowo kopiowane, nawet jeśli zdecydujemy się na użycie protokołu POP3.

W praktyce oznacza to, że e-mail pobrany z serwera przy użyciu protokołu POP3 lub skasowany przy użyciu dowolnego urządzenia i przeprowadzeniu synchronizacji przez protokół IMAP – powinien zostać skasowany. Jednak mogą tu zajść wykluczające się terminy, w których zostanie to zrobione. Może to być natychmiast (mało prawdopodobne), w ciągu 30 dni lub w ciągu 90 dni. Jest to czas, w którym wszystkie kopie bezpieczeństwa serwerów powinny się oczyścić ze starych kopii. Stare kopie zapasowe (tzw. backupy) powinny zostać nadpisane przez nowe dane. Jednak tu sprawę komplikują, z naszego punktu widzenia, przepisy znane jako „data retention policy”[10]. Na ich podstawie firmy są zobowiązane do przechowywania naszej usuniętej korespondencji przez okres nawet 2 lat. To samo będzie dotyczyło każdego pliku, który skasowaliśmy z chmury. W niektórych przypadkach – np. danych finansowych - okres retencji wyniesie 7 lat!

Sytuację pogarsza fakt, że niektóre firmy zastrzegają sobie prawo do pozostawienia danych na swoich serwerach (możliwe, że po częściowej anonimizacji), przez okres uznany przez nie za „odpowiedni”. Informacje o tym można znaleźć w polityce prywatności usługi, z której korzystamy. Oznacza, to, że skasowany e-mail, chociaż przez nas nie może zostać już odzyskany, w tym samym okresie może zostać przekazany służbom, jeżeli tylko takie zapytanie firma otrzyma od odpowiedniej jednostki.

Jeżeli pozornie bezpieczna usługa e-mail ma siedzibę lub / i serwery umiejscowione w jednym z krajów wspomnianych powyżej aliansów, to nie ma znaczenia, jaki rodzaj zabezpieczeń oferuje. W sytuacji zainteresowania nami przez służby, żadne zabezpieczenia nie będą nas chronić.

Dotyczyć to może również ProtonMail, firmy, która podkreśla swoją swojej dbałość o bezpieczeństwo użytkowników. Tymczasem oprócz danych francuskiego aktywisty / aktywistki

[10] Więcej: https://en.wikipedia.org/wiki/Data_retention (dostęp: 30.09.2023).

posługującego się adresem jmm18@protonmail.com[11], w samym 2022 roku udostępniła „bezpieczne" dane z kont prawie 6000 użytkowników[12].

Jedynym, co – do pewnego stopnia – może zabezpieczyć korespondencję elektroniczną, jest samodzielne szyfrowanie przy wykorzystaniu kluczy szyfrujących np. PGP (z ang. Pretty Good Privacy) czy OpenPGP i inne. Ma to jednak tę wadę, że wszystkie korespondujące ze sobą osoby powinny być w stanie ich użyć. Musi się to odbyć za porozumieniem wszystkich stron – nie ma możliwości, by jedna osoba ustawiła szyfrowanie komunikacji e-mailowej dla swoich korespondentów. W razie przejęcia komputera z zapisanymi kluczami w programie pocztowym, cały trud szyfrowania nie będzie miał żadnego znaczenia.

[11] O sprawie szeroko pisały portale. Wersja aktywistów: Autor zbiorowy, *Récit policier de Sainte Marthe*, https://paris-luttes.info/recit-policier-de-sainte-marthe-15258?lang=fr (dostęp: 23.09.2023); Wyjaśnienia ze strony ProtonMail: Andy Yen, *Important clarifications regarding arrest of climate activist*, https://proton.me/blog/climate-activist-arrest (dostęp: 23.09.2023). Więcej: Sven Taylor, *ProtonMail Complied with 5,957 Data Requests in 2022 – Still Secure and Private?* (dostęp: 23.09.2023).

[12] Proton, Transparency report https://proton.me/legal/transparency (dostęp: 23.09.2023).

Komunikatory a inwigilacja

Mając w pamięci zagrożenia wynikające z inwigilacji rozmów telefonicznych, e-maili i wiadomości tekstowych, warto pomyśleć o używaniu komunikatorów. Temat ten powraca w wielu opracowaniach, dlatego ograniczę się tu tylko do wskazania kilku istotnych kwestii.

Jeżeli oprócz czynnego podsłuchu i inwigilacji naszej komunikacji zainstalowano nam na smartfonie program typu Pegasus, to używanie szyfrowanych komunikatorów nie uchroni prywatności naszej korespondencji[13]. Bardzo możliwe, że w trakcie ataku służb na naszą prywatność wykorzystane zostanie inne oprogramowanie typu keyloger, czyli zapisujące wciskane na telefonie klawisze (nawet te wyświetlane na ekranie). Na podstawie tego, co wciskamy, da się odtworzyć naszą szyfrowaną komunikację w bezpiecznym komunikatorze.

Może do tego dojść w sposób, któremu nie jesteśmy w stanie zapobiec – na telefon zostaje przesłana wiadomość zawierająca odpowiedni program szpiegujący (spyware), który przy naszym udziale – otwarcie SMS-a, kliknięcie w podejrzany link (opcjonalnie) – lub całkowicie bez niego (wówczas wystarczy samo otrzymanie wiadomości), może zainstalować program umożliwiający permanentną inwigilację naszego smartfonu. Wówczas wszystkie znajdujące się na nim dane (kontakty, wiadomości, e-maile, zdjęcia, pliki wideo, pliki audio i inne dokumenty) zostaną przesłane służbom.

Dlaczego w takim razie warto używać komunikatorów? Jeżeli naszym naturalnym kanałem komunikacji będzie Signal lub Viber (również oparty o protokół Signal), to otrzymanie niespodziewanej wiadomości SMS wzbudzi większą czujność. Da nam sygnał, że nadszedł czas na skasowanie wiadomości z komunikatorów, bo podejrzany SMS będzie jasną informacją, że ktoś się nami interesuje.

Inną zaletą szyfrowanych komunikatorów będzie możliwość prowadzenia rozmów głosowych lub wideo przez aplikację. W razie podsłuchu nałożonego na komunikację opartą o sieć telefonii komórkowej, rozmowa przez komunikator nie zostanie podsłuchana. Jedynie wtedy,

[13] Więcej: Michał Rysiek Woźniak, Pegasus: gorzej niż podsłuch. Umożliwia podrzucanie dowodów. Giertych, Wrzosek, Brejza, kto jeszcze..., https://oko.press/pegasus-gorzej-niz-podsluch-potrafi-tez-podrzucac-dowody (dostęp: 30.09.2023).

gdy korzystamy z danych mobilnych, dla służb będzie widoczne, że zużywamy dane internetowe.

Ilość danych wykorzystywanych do komunikacji audio lub audio i wideo w sposób oczywisty będzie większa niż przy komunikacji tekstowej (ewentualnie wzbogaconej o załączniki multimedialne). Widać to na miesięcznym zestawieniu operacji na koncie, które otrzymujemy od operatora telefonii komórkowej wraz z fakturą. Możemy zobaczyć, o której godzinie jaka liczba danych w kb została wykorzystana. Może być podane, ile danych zostało odebranych, a ile przesłanych. Jednak jeżeli nawet operator będzie w stanie ustalić, w jakim celu dane zostały użyte, to nie stanowi to dla nas zagrożenia. Tak jak każda strona, którą odwiedzamy, bez używania VPN lub przeglądarki TOR, będzie rejestrowana, tak samo, jeżeli korzystamy z aplikacji, przypuszczalnie może to być z nią kojarzone. Na smartfonie jesteśmy w stanie sprawdzić, ile danych lub baterii zużywa dana aplikacja, czyli informacje te są zbierane już na urządzeniu.

Jeżeli operator telefonii ustalałby szczegółowo, która aplikacja zużywa dane, to poza zaobserwowanym użyciem aplikacji, nie będzie miał dostępu do wykazu naszych rozmów czy wiadomości. Dlatego też komunikatory w aplikacjach będą bezpieczniejsze niż standardowa komunikacja przy użyciu wiadomości tekstowych i połączeń telefonicznych. Prawdopodobieństwo monitorowania wykorzystania aplikacji mogą sugerować pojawiające się specjalne oferty skierowane do użytkowników wybranych aplikacji lub ich określonych typów. Decydując się na użycie komunikatora należy sprawdzić w polityce prywatności, jak dany serwis obchodzi się z naszymi danymi. Komunikatory WhatsApp i Facebook Messenger, oba należące do Meta, będą miały inną politykę niż wspomniane Signal czy Viber. Jeżeli czytanie prawnych opisów nie należy do naszych ulubionych zajęć, wystarczające powinno się okazać użycie kombinacji Ctrl+F oraz osobno wpisanie fraz (np. delete, years, store, server), które powinny nam pozwolić szybko się zorientować, jak długo nasze dane są przechowywane.

Powinniśmy zachować czujność, jeśli w jednym miejscu pojawia się informacja, że dane są usuwane natychmiast lub np. po 30 dniach, a w innym miejscu, że dane są przechowywane przez czas zgodny z obowiązującym porządkiem prawnym. Należy się wówczas spodziewać, że chociaż skasujemy je na swoim urządzeniu, to pozostają one jednak w kopii przez 2-5-7 lat na serwerze. W 2023 roku na podstawie danych z czatu z 2022 roku, dostarczonego przez Meta,

zostały w USA skazane dwie kobiety Celeste Burgess[14] (córka) i Jessica Burgess[15] (matka) – odpowiednio za przeprowadzenie aborcji i pomoc w jej przeprowadzeniu oraz pozbycie się płodu[16]. W dostępnych dokumentach procesowych uwagę zwraca numer strony dokumentu zawierającego historię chatu przechowywanego przez Meta – str. 1404.

By uniknąć gromadzenia historii rozmów z wielu lat zdecydowanie lepiej wybrać komunikator, który kasuje rozmowy użytkowników. W Signal mamy możliwość ustawienia automatycznego czasu usuwania wiadomości.

Decydując się na skorzystanie z komunikatora zamiast innych kanałów komunikacji, powinniśmy zwrócić uwagę, że chociaż będzie on bezpieczniejszy, w dalszym ciągu nie gwarantuje nam pełnej prywatności. Zakładając konto łączymy je z numerem telefonu i adresem e-mail, a to oznacza, że nadal jesteśmy identyfikowalni.

Chcąc chronić swoją prywatność przed opresyjnym państwowym systemem inwigilacji, powinniśmy móc to zrobić i nie powinno to stanowić problemu. Musimy się jednak liczyć z tym, że cokolwiek prześlemy komunikatorem, może zostać użyte przeciwko nam. Chociaż ich twórcy podejmują starania, by stanowiły bezpieczną alternatywę komunikacyjną, żaden z nich nie jest w pełni bezpieczny. Zdecydowanie odradzam korzystanie z komunikatorów powstałych i operujących w krajach uznawanych za totalitarne lub słynące z inwigilacji.

Warto też zauważyć, że Signal i Viber oferują możliwość ręcznego usunięcia wysłanej wiadomości u siebie i u odbiorcy (pod warunkiem, że urządzenie odbiorcy jest w zasięgu Internetu). Część komunikatorów oferuje tylko usunięcie wiadomości u siebie. Również funkcja automatycznego usuwania wiadomości po upływie określonego czasu jest warta docenienia.

Decydując się na komunikator, warto też uwzględnić preferencje osób, z którymi mamy się kontaktować. Jeżeli zdecydujemy się np. na Signal, ale osoba, z którą chcemy wymieniać

[14] Andy Rose, *Nebraska woman charged with disposing of fetus following illegal abortion sentenced to 90 days in jail,* https://edition.cnn.com/2023/07/20/us/nebraska-teen-abortion-celeste-burgess/index.html (dostęp: 25.09.2023).
[15] Mitchell McCluskey, *A Nebraska mother who provided an illegal abortion for her daughter and helped dispose of the fetus gets 2 years in prison, report says,* https://edition.cnn.com/2023/09/23/us/nebraska-abortion-pill-jessica-burgess/index.html (dostęp: 25.09.2023).
[16] Jason Koebler, Anna Merlan, *This Is the Data Facebook Gave Police to Prosecute a Teenager for Abortion,* https://www.vice.com/en/article/n7zevd/this-is-the-data-facebook-gave-police-to-prosecute-a-teenager-for-abortion (dostęp: 25.09.2023).

wiadomości, nie używa go, nie jesteśmy w stanie skorzystać z tej bezpiecznej formy. Tak samo jak użytkownik Vibera nie będzie w stanie wysłać informacji do użytkownika Signala.

Jeżeli zależy nam na całkowicie anonimowej i szyfrowanej komunikacji, ciekawą alternatywą może okazać się Wire – dawniej komunikator, a obecnie narzędzie nastawione na komunikację profesjonalną. Podczas zakładania konta użytkownika możliwe jest podanie tylko e-maila, bez konieczności podawania numeru telefonu. Możemy, wykorzystując specjalnie w tym celu stworzony adres e-mail, oddzielić komunikację przez Wire od naszych innych narzędzi, kontaktów czy plików. Oczywiście ważne jest, żeby to był osobny e-mail, a nie alias do naszego głównego e-maila. Jeżeli nie zakładamy konieczności odzyskiwania hasła, możemy użyć e-mail tymczasowy wygenerowany np. przez „10 Minute Mail" - https://10minutemail.com/. Po 10 minutach adres zostanie bezpowrotnie skasowany.

CZĘŚĆ III - CYBEROBRONA

Cyberobrona

Przystępując do cyberobrony (z ang. Cyberdefence) powinniśmy nastawić się na stopniową i całościową obronę naszego cyfrowego życia oraz osób, które mogą próbować się z nami skontaktować w okresie, gdy podlegamy totalnej i permanentnej inwigilacji. Niestety, stanowimy potencjalne źródło zagrożenia – trochę to przypomina sytuację, gdy mając grypę możemy zarazić każdego, z kim mamy kontakt. Każda kontaktująca się z nami osoba może zostać wzięta „na celownik" - wszystko zależeć będzie od skali inwigilacji, której zostaniemy poddani.

Jeżeli korzystamy z pomocy asystenta / asystentki, oni również z pewnością szybko trafią w centrum zainteresowania służb jako osoby, przez które da się dostać do inwigilowanego człowieka.

Dlatego jedną z pierwszych czynności, które powinniśmy podjąć, powinno być ostrzeżenie ludzi, którzy mogą się chcieć z nami skontaktować. Jeżeli to możliwe, powinniśmy to zrobić z innego numeru telefonu niż zwykle (oczywiście z innego urządzenia) oraz z innego adresu e-mail. Powinniśmy przekazać, od kiedy przypuszczalnie jesteśmy inwigilowani, oraz czy i w jakim stopniu może to wpływać na cyfrowe bezpieczeństwo naszych bliskich, współpracowników czy znajomych. Możemy ustalić, że przez jakiś czas nie kontaktujemy się z daną osobą (np. do osobistego spotkania). To może też być o tyle istotne, że w razie spreparowania fałszywej wiadomości czy e-maila dana osoba będzie wiedzieć, że nie pochodzą one od nas.

Sugeruję skontaktowanie się tylko z wybranymi osobami – zajmuje to czas i uniemożliwia podjęcie innych działań. Jeżeli ktoś spoza naszego najbliższego kręgu podejmie próbę kontaktu – wówczas odwzajemnimy kontakt przez inny (bezpieczny) kanał komunikacji.

Zakładam, że stosunkowo prosto jest przygotować wiadomość tekstową lub e-mail, którą możemy przesłać do wybranych osób. Opcjonalnie możemy dodać link do artykułu lub innego

materiału – chociaż przyzwyczajanie bliskich do otwierania linków, które dostają z nieznanego im numeru telefonu lub z obcego e-maila, nie jest dobrym pomysłem.

W naszej wiadomości, wysłanej z nowego numeru telefonu, powinniśmy ustalić, w jaki sposób ktoś może potwierdzić, że został ostrzeżony, i że rozumie przekaz. Lepiej jest to określić, bo część osób może odpisać na wiadomość, a to oznacza, że ktokolwiek podający się za nas może zacząć się komunikować z kimś nam bliskim. Część osób może odpisać na inwigilowany numer lub przesłać na niego otrzymaną wiadomość z prośbą o potwierdzenie, że pochodzi od nas. Tym samym ujawnią niechcący, że wiemy o prowadzonych przeciwko nam czynnościach.

Dopóki nie dojdzie do osobistego spotkania albo rozmowy głosowej (chociaż oczywiście mam świadomość, że czyjś głos da się wygenerować za pomocą AI), osoba ostrzeżona powinna podchodzić z pewną ostrożnością do otrzymanych informacji. Dlatego najbezpieczniej poprosić o oddzwonienie na nowy numer – ten, z którego się kontaktujemy. Dzięki temu dajemy osobie bliskiej czas na zapoznanie się z treścią wiadomości, ewentualnego artykułu i wybranie momentu na kontakt. Z perspektywy osoby inwigilowanej pozwala to oszczędzić czas, bo nie musimy kilkukrotnie powtarzać tych samych informacji kolejnym osobom. Dzięki temu możemy się skupić na tym, co istotne.

Zanim rozpoczniemy cyberobronę, powinniśmy zdecydować, co chcemy osiągnąć. Jeżeli naszym celem jest ochrona naszych danych i odzyskanie możliwości komunikacji, to będziemy postępować tak, by udało się to jak najszybciej. Natomiast jeśli chcemy uchronić naszą prywatność, ale inwigilowane urządzenia zostawić jako dowód w późniejszej sprawie, to części z opisanych poniżej czynności nie będziemy mogli podjąć. Istotne wtedy będzie pozostawienie urządzeń w takim stanie, w jakim były w momencie ataku ze strony służb.

Zakładam jednak, że z przyczyn finansowych nie zawsze możemy sobie pozwolić na wymianę całego sprzętu elektronicznego, dlatego poniżej skupiam się na usunięciu zagrożenia i odzyskaniu sprzętu, co wiązać się będzie ze zniszczeniem potencjalnych dowodów.

Cyberobrona smartfonu

Z dużym prawdopodobieństwem smartfon będzie pierwszym obiektem ataku. Jest najbardziej osobisty – będzie zawierał najwięcej aktualnych informacji.

Wśród objawów inwigilacji smartfonu jest kilka, które mogą zostać łatwo zaobserwowane. Ich dostrzeżenie nie wymaga wiedzy technicznej. Kolejność losowa.

Smartfon zużywa szybciej baterię – intensywnie przesyła dane w tle, co ma wpływ na pobór energii z baterii urządzenia. Ponadto oprogramowanie szpiegowskie może powodować przegrzewanie się jakiegoś wybranego elementu w jego wnętrzu. Obudowa staje się wyczuwalnie cieplejsza w jednym miejscu. Należy jak najszybciej ponownie uruchomić urządzenie i rozważyć przełączenie w tryb samolotowy. Po przeprowadzonym restarcie może być zasadne czasowe całkowite wyłączenie, które pozwoli na schłodzenie się przegrzanych podzespołów.

Smartfon zużywa więcej Internetu niż zwykle – można to zaobserwować dzięki programom VPN, antywirusom lub wbudowanym funkcjom wybranych modeli smartfonów. W ustawieniach telefonu należy wyszukać „zużycie danych” i sprawdzić, czy jest większe niż było dotychczas. Zanim spanikujemy, warto się zastanowić, czy sami nie jesteśmy tego przyczyną.

Smartfon rozładowuje się przez noc – jeżeli smartfon będzie miał pobierane dane w dużych ilościach, z dużym prawdopodobieństwem będzie się to odbywało w nocy. Dlatego, jeżeli naładowany telefon jest całkowicie rozładowany po nocy, należy się zainteresować, jaka jest przyczyna.

Smartfon dzwoni i się rozłącza – na wyświetlaczu, na jeden dzwonek, wyświetla się jakiś numer, często zastrzeżony. Może to być też błyśnięcie ekranu – widać, że ktoś dzwoni, ale zanim usłyszymy dzwonek, rozmówca się rozłącza. Numer może nie być widoczny w historii połączeń.

Smartfon dzwoni sam do siebie – Twój smartfon leży koło Ciebie, widzisz, że dzwoni, a na ekranie wyświetla się Twój własny numer telefonu jako osoby dzwoniącej. Ma to na celu wybudzenie telefonu i połączenie ze stacją bazową, by z dokładnością do kilku metrów ustalić, gdzie aparat się znajduje. W ten sposób sprawdza się też, czy urządzenie pozostaje aktywne.

Dwa smartfony dzwoniące do siebie – to przykład kuriozalny, słyszałem o takiej sytuacji tylko raz. Dwie osoby siedzą koło siebie – powiedzmy Alice i Bob (używając przykładowych imion typowych dla literatury z zakresu cyberbezpieczeństwa). Na stole leżą ich smartfony, których właściciele nie dotykają. W tym samym momencie obydwa urządzenia dzwonią. Na telefonie Boba widać, że dzwoni do niego Alice. Na telefonie Alice widać, że dzwoni do niej Bob. Obydwa telefony przestają dzwonić równocześnie. Jak można się domyślać, może to służyć sprawdzeniu, czy obie osoby znajdują się w jednej lokalizacji.

Włączona lokalizacja telefonu – jeżeli po którejkolwiek z powyższych sytuacji w telefonie jest włączona jego lokalizacja, a wcześniej była wyłączona, to jest to kolejne potencjalne potwierdzenie naszego przypuszczenia o byciu inwigilowanym.

Przesunięcie czasowe - w trakcie rozmowy telefonicznej, tak jak było wspomniane wcześniej, da się zauważyć lekkie opóźnienie. Rozmówcy słyszą się, nie muszą występować zakłócenia. Jednak gdy jedna osoba kończy mówić i byłoby naturalne, że druga jej odpowie, a to nie następuje, należy zachować czujność. Może dojść do sytuacji, w której mamy wrażenie, że obydwie osoby w którymś momencie zaczynają mówić równolegle. Z powodu wspomnianego przesunięcia, nie słysząc odpowiedzi, rozmówca upewnia się, że jest słyszany, parafrazuje, dopytuje. W tym momencie druga osoba już mówi, ale zaczyna słyszeć kolejne kwestie i przerywa wypowiedź. Skutkiem tego obaj rozmówcy albo mówią równocześnie, albo obaj milczą, a rozmowa traci naturalny rytm.

Słowa „klucze” (z ang. trigers) – konkretne słowa, wyzwalające ustawioną reakcję filtrów. W rozmowie padają słowa, po których następuje zakłócenie rozmowy oraz zauważalne jej opóźnienie. Przykładowe słowa: policja, protest, manifestacja, prawnik, przesłuchanie itp. (te były użyte przeciwko autorowi). Po pojawieniu się słowa „klucza” w rozmowie, jest ona stopniowo zakłócana, aż zostaje rozłączona. Im częściej pojawiają się te słowa, tym zakłóceń jest więcej. Po rozłączeniu rozmowy i ponownej próbie połączenia z rozmówcą nie da się nawiązać połączenia. Może pojawić się komunikat o błędzie sieci, ale nie musi. Połączenia nie da się nawiązać – natychmiast, bez wstępnych dzwonków, włączona zostaje poczta głosowa osoby, do której staramy się zadzwonić. Celem tego działania może być próba zmuszenia, by ktoś nagrał informację, która później potencjalnie może zostać użyta przeciwko niemu. Na pewno zaś skutkuje to poczuciem niepewności, zagubienia, powoduje stres i lęk. Jest skuteczną

formą zastraszania i może być narzędziem izolacji osoby obserwowanej od wspierających ją ludzi.

Nie twierdzę, że wszystkie te symptomy wystąpią razem. Każdy z nich jest alarmujący i powinien wzbudzać czujność. Jeżeli chcemy mieć pewność, czy telefon jest na podsłuchu, to powinniśmy zbadać tzw. logi. To pliki przypominające pliki tekstowe z rozszerzeniem .log (zamiast np. rozszerzenia .docx typowego dla dokumentów tekstowych).

Jeżeli pliki zawierające logi nie są widoczne po podpięciu smartfonu do komputera z Windowsem, to na pewno są widoczne po pobraniu wszystkich danych urządzenia w zip przy użyciu Chromebooka (komputer z systemem Chrome OS) lub dowolnej dystrybucji Linuxa[17]. W logach zapisywane są wszystkie istotne zdarzenia, np. włączenie i wyłączenie telefonu, a w związku z tym – połączenie ze stacją nadawczą. Swój ślad zostawią też podsłuchy ustawione na numer telefonu i przypuszczalnie te na numer IMEI urządzenia[18].

Większość z nas nie potrzebuje jednak technicznie analizować tego, co działo się ze smartfonem, lecz chce pozbyć się zagrożenia. Zasugerowałem już wcześniej, by przełączyć smartfon w tryb offline (tryb samolotowy). Wynikało to z faktu, że większość wspomnianych powyżej naruszeń prywatności jest możliwa tylko wtedy, gdy smartfon jest podłączony do sieci, a że ta publikacja ma postać cyfrową, liczę się z tym, że może być czytana na inwigilowanym smartfonie.

Należy mieć świadomość, że nawet w trybie samolotowym smartfon w jakimś stopniu pozostaje aktywny. Nadal może być namierzany, ale pobieranie danych czy podsłuch nie powinny być możliwe. Na wszelki wypadek nie powinniśmy jednak prowadzić istotnych rozmów w jego pobliżu.

Sugerowane jest wożenie inwigilowanego smartfonu np. w bagażniku na normalnej trasie – będzie wyglądało, że nadal jest w ruchu, a trasa dom-praca-dom i tak na pewno jest służbom znana. Dzięki temu zabiegowi dłużej utrzymujemy przeciwnika w przekonaniu, że nie wiemy o prowadzonych przeciwko nam działaniom.

[17] Przykładowe logi z inwigilowanego telefonu zamieszczam na końcu publikacji z uwagi na ich długość.
[18] To pierwsze można zobaczyć w przykładowym logu na końcu, to drugie stanowi hipotezę, której nie mam jak zweryfikować.

Część oprogramowania używanego przez służby działa na zasadzie nawiązania połączenia przy wykorzystaniu Internetu i przesyłu danych. Można spotkać się z opiniami, że trzykrotne zrestartowanie telefonu powinno rozłączyć przynajmniej część programów (w tym podobno Pegasus). Przytrzymujemy przycisk włączenia smartfonu i wybieramy na ekranie „uruchom ponownie". Robimy to trzy razy nie czekając, aż smartfon w pełni się włączy i połączy z siecią. Jeżeli ta metoda działa, a wydaje się to prawdopodobne – służby będą musiały ponownie nawiązywać połączenie z Twoim smartfonem. Możliwe, że będzie to z ich strony wymagało zainicjowania nowego połączenia – ponowne przesłanie linku czy oprogramowania. Nie jestem w stanie tego zweryfikować, ale jeżeli inwigilacja prowadzona jest przy użyciu programu, to wydaje się możliwe, że kilkukrotne odcięcie od sieci będzie stanowiło utrudnienie działań operacyjnych.

Pamiętaj, że „wyłączenie smartfonu" i „ponowne uruchomienie" nie oznaczają tego samego. Bardzo podobnie działa komputer. Jeżeli wyłączamy smartfon lub laptop, to system przygotowuje sobie plik pamięci, w którym zapisuje różne ustawienia – w tym również informacje, które programy miały niedokończone zadania. Jeżeli po wyłączeniu urządzenia włączamy je ponownie, to w oparciu o zapisany zrzut pamięci urządzenie przywraca przerwane uprzednio procesy. Jeżeli natomiast decydujemy się na ponowne uruchomienie, to czyścimy pamięć wykonywanych operacji. Kilkukrotne ponowne uruchomienie smartfonu odpowiada tzw. twardemu resetowi komputera. Przypuszczalnie pozwala to oczyścić pamięć oraz zablokować pewne niepożądane procesy.

Dla pewności, po przeprowadzeniu opisanych w poprzednim akapicie działań, możemy przełączyć smartfon w tryb samolotowy i wówczas przystąpić do ratowania naszych danych. Jeżeli okaże się, że podpięcie smartfonu do komputera i prowadzenie poniższych operacji jest w tym trybie niemożliwe, należy wrócić do trybu online.

Zanim podłączymy smartfon do komputera, powinniśmy ocenić ryzyko, z jakim się to wiąże. Możliwe, że oprogramowanie, które możemy mieć na smartfonie, spróbuje przejść na komputer. Powinniśmy więc liczyć się z tym, że stwarza to zagrożenie dla kolejnego urządzenia. Dla zachowania minimum bezpieczeństwa, zanim połączymy urządzenia ze sobą, należy zaktualizować ręcznie antywirusa (osobno program i bazę wirusów), a także wykonać kopię danych z laptopa na dysku zewnętrznym. Dane kopiujemy, nie przenosimy. Zadaniem operacji

jest zrobienie kopii bezpieczeństwa, a nie posiadanie jedynej kopii na zewnętrznym dysku[19]. Powinniśmy pamiętać też o folderach typu „pulpit", „moje dokumenty", „pliki pobrane" – często osoba w sytuacji stresowej pamięta o plikach w utworzonych przez siebie folderach, a zapomina o używanych przez siebie folderach, które zostały utworzone przez system.

Te kroki są konieczne, jeżeli pracujemy na komputerze z Windows[20], ale jeśli mamy taką możliwość – a zwłaszcza czas i chęci – to warto zainfekowany telefon podpiąć do dystrybucji live Linuxa, najlepiej Tails, lub do Chromebooka[21]. Zestawienie ze sobą Tails, znanego ze skrajnej dbałości o prywatność użytkowników, z Chromebookiem wyposażonym w ChromeOS od Google, kojarzonego raczej z dbałością o dostęp do danych użytkowników, może wydać się absurdalne. Jeżeli dodamy do tego jeszcze współpracę Google ze służbami państw i udostępnianie im danych użytkowników,[22] może to wywołać konsternację. Obydwa te systemy mają tę zaletę, że – z odmiennych powodów – będą odporne na oprogramowanie mogące zainstalować się na komputerze podczas przesyłania naszych danych. Tails jako wersja live po wyłączeniu komputera nie zapisuje niczego, w tym żadnego programu. Ponadto jest to Linux, zatem bez zgody użytkownika żaden program nie może się sam zainstalować na komputerze. Natomiast Chromebook z uwagi na to, że jest przewidziany dla niedoświadczonego użytkownika, często dla dziecka, ma domyślnie zablokowane różne ustawienia, dzięki czemu jest bezpieczniejszy niż komputer z Windows. Zainstalowanie czegokolwiek wymaga korzystania z repozytorium zweryfikowanych programów lub pisania kodu. Innymi słowy – nic się samo bez wiedzy i uwagi użytkownika nie może zainstalować. Ponadto, jeżeli skorzystamy z trybu gościa, to podobnie jak w Tails, po wyłączeniu komputera po naszej aktywności nie zostanie żaden ślad.

Niezależnie od tego, czy zdecydujemy się pracować na komputerze z Windows, Tails czy ChromeOS, po podpięciu smartfonu do komputera powinniśmy skopiować nasze pliki –

[19] Wskazówki dotyczące bezpiecznego przechowywania i kopiowania plików można znaleźć na końcu publikacji, w dziale Dodatki.
[20] Nie znam środowiska Mac OS, przypuszczam, że te same zalecenia będą dobre również w przypadku korzystania z komputera firmy Apple.
[21] Więcej o Tails i Chromebook w dalszej części publikacji.
[22] Szczegóły dostępne na stronie https://transparencyreport.google.com/user-data/overview (dostęp: 30.09.2023). W 2022 roku dotyczyło to ponad 800 tys. kont użytkowników na świecie, w tym ponad 13 tys. kont użytkowników z Polski.

zwłaszcza zdjęcia i wideo znajdujące się w folderze DCIM. Jeżeli używamy karty pamięci, trzeba też pamiętać o skopiowaniu danych z pamięci wewnętrznej urządzenia i z karty pamięci.

Dla wygody możemy dane ze smartfonu skopiować na osobny pendrive lub dysk zewnętrzny. Pozwoli to na ich oddzielenie od pozostałych danych oraz proste przenoszenie między urządzeniami. Pendrive lub dysk zewnętrzny powinniśmy w całości profilaktycznie przeskanować antywirusem przy pierwszym wpięciu do gniazda USB komputera z antywirusem.

Po skopiowaniu danych upewnijmy się, że są. Zainicjujmy kopiowanie jeszcze raz – jeżeli wszystko prawidłowo się skopiowało, zostanie wyświetlony komunikat informujący, że pliki, które (ponownie) próbujemy skopiować, znajdują się już we wskazanej lokalizacji.

Czas kopiowania zależy od rozmiaru danych. Android wymusza pracę jednozadaniową. Nie mamy możliwości równoczesnego włączenia kilku procesów kopiowania z różnych lokalizacji.

Po skopiowaniu wszystkiego, co uznaliśmy za potrzebne, odłączamy smartfon od komputera. Jeżeli na komputerze widzimy pliki, otwierają się i zakładamy, że wszystko zostało zgrane, należy sformatować kartę pamięci – w urządzeniu lub po jej wyjęciu w komputerze. W razie problemów lub wątpliwości warto skorzystać z tutoriali na YouTube lub czyjejś pomocy. W zależności od wielu czynników proces może różnie przebiegać, stąd trudno go jednoznacznie opisać. Formatowanie kasuje wszystkie dane na karcie. Nie należy go robić, jeśli nie skopiowaliśmy ich wcześniej na komputer czy pendrive.

Podczas kolejnych czynności karta nie powinna znajdować się w smartfonie. Zabezpieczamy się tym samym przed ewentualnością jej zawirusowania, gdy będziemy usuwać jego skutki ze smartfonu.

Przygotowujemy się do przeprowadzenia wyczyszczenia smartfonu poprzez przywrócenie ustawień fabrycznych urządzenia. Jeżeli to zrobimy, wszystkie nasze dane, w tym wiadomości i zdjęcia, zostaną bezpowrotnie usunięte. Jeśli chcemy je zachować, powinniśmy wykonać kopię zapasową.

W smartfonie wybieramy „Ustawienia” (ikonka koła zębatego) i wyszukujemy „konto kopii zapasowej”. Wyświetli się nasze obecne konto w serwisie Google. Jeżeli zakładamy, że służby znają ten adres e-mail, powinniśmy utworzyć nowe konto, niezawierające naszego imienia,

nazwiska czy innych danych, które mogą nas identyfikować. To ma być konto, które będzie znajdowało się wyłącznie na smartfonie. Powinno mieć również inne hasło niż nasze dotychczasowe konto. Wybieramy „utwórz nowe konto" i tworzymy czyste konto.

Z aplikacji Google wybieramy Google One (ikona „1"), klikamy w zdjęcie profilowe i wybieramy nowo utworzone konto, lub, jeśli wolimy (i chyba zależnie od wersji Androida), tutaj też możemy utworzyć nowe konto – opcja „Dodaj kolejne konto".

Po jego wybraniu znajdujemy się, zgodnie z opisem, w „miejscu na dane i inne funkcje Google One". Znajdujemy „tworzenie kopii" – kafel po lewej stronie, a po jego naciśnięciu, na środku znajdziemy belkę „utwórz kopię zapasową teraz". Po jej kliknięciu na kolejnej stronie na dole znajdziemy belkę „Zarządzaj kopią zapasową". Możemy tu odznaczyć zdjęcia – kopia wykona się szybciej i Google nie uzyska dostępu do naszych wszystkich zdjęć, a kopię zdjęć mamy już zrobioną na laptopie lub pendrive. Warto też uaktywnić „Rób kopie zapasowe korzystając z mobilnej transmisji danych". Po kliknięciu na dole na „Utwórz kopię zapasową teraz", kopia zostanie utworzona.

Ten proces trochę potrwa, bo smartfon przesyła właśnie Twoje dane do chmury. Wyświetla pulsujący pasek postępu i informację „Tworzę kopię zapasową…".

Gdy proces zostanie ukończony, wyświetli się komunikat „Kopia twoich danych została utworzona". Dla pewności możemy zalogować się na nowe konto Google na komputerze, jeżeli tylko nie jest zainfekowany, i w usłudze Google One możemy zobaczyć, że nasza kopia rzeczywiście tam jest.

Po weryfikacji wybieramy na smartfonie „Ustawienia" (ikonka koła zębatego) i wyszukujemy w wyszukiwarce na górze „Przywrócenie ustawień fabrycznych". Gdy uruchomimy tę funkcję, smartfon zostanie wyczyszczony z naszych prywatnych danych oraz usunie wszystkie aplikacje, w tym te, które są używane do szpiegowania nas.

Po ponownym uruchomieniu i zalogowaniu się na nasze nowe konto, pośród pojawiających się opcji do wyboru będzie możliwość przywrócenia danych z naszej kopii. Jeśli ją wybierzemy, to na smartfonie pojawią się znów nasze smsy, kontakty i aplikacje – powinna być możliwość zdecydowania, które mają zostać ponownie zainstalowane.

Uwaga! Jeśli w SMS-ach, które zostały przywrócone, był wcześniej SMS np. z dziwnym linkiem, który mógł zainicjować inwigilację, to on również został przywrócony. Jeśli tak się stało, należy go znaleźć i usunąć, unikając aktywacji linku. Do indywidualnej decyzji pozostawiam ponowne wykonanie powyżej opisanych czynności.

Opisana procedura zajmuje kilka godzin i pozwala na odzyskanie smartfonu i oferowanych przez niego funkcji. Pozwala też na powrót do komunikacji głosowej, chociaż należy się liczyć z tym, że za jakiś czas służby będą chciały wrócić do inwigilowanej osoby.

Jeżeli chcemy wzmocnić nasze bezpieczeństwo, to warto się zastanowić, czy przynajmniej na jakiś czas nie kupić numeru na kartę, u innego operatora niż dotychczasowy, i tylko tego numeru używać w odzyskanym smartfonie, zapewne głównie do korzystania z Internetu lub komunikatora Signal.

Dotychczasową kartę SIM warto wymienić u operatora – koszt to 30 - 60 zł. Dzięki temu, jeżeli podsłuch był ustawiony nie na numer, ale na kartę SIM, a tak wskazują logi, to wymieniając kartę SIM pozbywamy się ogona.

***** ***

Kolejnym wzmocnieniem może być użycie tradycyjnego telefonu, takiego z klawiszami, który nie ma żadnych aplikacji, ani nie pozwala na podpięcie go do komputera – jego system jest na tyle „prymitywny”, że z dużym prawdopodobieństwem zabezpieczy swoją ograniczoną funkcjonalnością urządzenie przed próbą zainstalowania oprogramowania przystosowanego do nowych urządzeń, pracujących w nowym systemie. Z dużym prawdopodobieństwem tradycyjny telefon nie pracuje w oparciu o Android, stąd aplikacje pisane z myślą o tym systemie nie będą stanowiły dla niego zagrożenia.

Te pozornie proste telefony, pozbawione funkcji smartfonów, są również na tyle przystępne cenowo, że można kupić je za gotówkę w sklepie (by nie rejestrować transakcji na karcie bankowej). To ma też tę zaletę, że podczas zakupu smartfonu w salonie telefonii komórkowej numer IMEI jest rejestrowany w bazie firmy, dzięki czemu staje się dostępny dla służb wraz z naszymi pozostałymi danymi, a to zwiększa możliwość prowadzenia inwigilacji.

Te proste telefony, oprócz długiego czasu rozmów, oferują też możliwość zabezpieczenia wszystkiego kodem PIN, nie pozwalają na podpięcie do komputera i zapewniają możliwość bardzo szybkiego i łatwego przywrócenia ustawień fabrycznych. Ponadto, jeżeli nie użyjemy karty pamięci (niektóre modele to umożliwiają), to w razie przejęcia tego telefonu podczas zatrzymania służby nie będą miały z niego wielkiego pożytku. Nie są w stanie zmusić nikogo do odblokowania odciskiem palca, bo on nie ma takiej funkcji, ani nie mogą odblokować go przystawiając telefon do twarzy przesłuchiwanego. Jeżeli kasujemy na bieżąco SMS-y, tradycyjne telefony nie mają żadnych danych, które służby mogłyby chcieć pozyskać. Zależnie od sytuacji, w której jesteśmy, możemy też szybko skasować wszystkie kontakty.

***** ***

Cyberobrona tabletu

Tablet, chociaż czasem bywa porównywany do dużego smartfonu, przeważnie jednak używany jest do innych celów i w inny sposób. Dlatego warto przyjrzeć mu się osobno. Oczywiście wszystkie wskazówki dotyczące przygotowania kopii danych, przywrócenia ustawień fabrycznych czy zmiany konta będą podobne, dlatego nie będą tu powtarzane.

Z uwagi na to, jak korzystamy z tabletu, jest bardzo prawdopodobne, że stanowi on w głównej mierze narzędzie dostępu do treści w Internecie. W związku z tą nadrzędną funkcją nie będzie zawierał tylu osobistych informacji co smartfon. Dzięki temu możemy łatwiej go zabezpieczyć i częściej przywracać do stanu początkowego. Możliwe, że jeśli używamy go do multimediów, sprawdzenia poczty czy czytania on-line, nie będzie nawet konieczne wykonywanie kopii zapasowej, a po przywróceniu ustawień fabrycznych wystarczy, że zalogujemy się na konto poczty e-mail i będziemy mogli korzystać z urządzenia tak, jak potrzebujemy.

Z uwagi na brak SMS-ów szansa na zainfekowanie tabletu jest mniejsza. Oczywiście może mieć aplikację do obsługi wiadomości tekstowych, ale ponieważ nie jest to główna funkcja tabletu, łatwiej zachować czujność w momencie otrzymania podejrzanej wiadomości.

Jeżeli tablet obsługuje karty SIM, możemy wymieniać dostawcę Internetu tak często, jak tego potrzebujemy. Możemy zdecydować, czy będziemy korzystać z jednej firmy - wówczas ryzyko inwigilacji wzrasta - czy co miesiąc wybierzemy usługi innej firmy. Jeżeli nawet będziemy rejestrować kartę u kolejnego operatora, zgodnie z wymogami przepisów, to jej znalezienie będzie wymagało więcej zachodu ze strony służb.

Ponadto, zwłaszcza w okresie, kiedy wiemy, że służby szczególnie się nami interesują, możemy używać nierejestrowanych karty SIM. Przynajmniej część z dostępnych na rynku oferuje jeszcze przed rejestracją możliwość użycia np. 1 GB danych przez tydzień, co kosztuje około 5-30 zł. Jeżeli zdecydujemy się na to rozwiązanie, po wykorzystaniu karty możemy ją zarejestrować i doładować, ale jeśli dbamy o prywatność, możemy z niej zrezygnować i kupić kolejną u innego operatora. To nie jest duży pakiet danych, ale do obsługi e-maila czy Signal w zupełności wystarczy. Nawet jeśli zdecydujemy się przenieść aplikacje do mediów społecznościowych wyłącznie na tablet i zrezygnujemy z ich używania na smartfonie, dostępna liczba danych powinna okazać się wystarczająca do ich normalnego używania.

Dla zwiększenia niewykrywalności za kartę SIM należy zapłacić gotówką. Transakcje bezgotówkowe są z zasady mniej bezpieczne, gdy zależy nam na zachowaniu prywatności i anonimowości. Teoretycznie jest możliwe: połączenie numeru karty SIM, numeru paragonu, numeru transakcji kartowej i tym sposobem odkrycie danych osobowych kupującego, będącego właścicielem karty bankowej. Jednak chcąc uniknąć paranoi trzeba przyznać, że zajmie to więcej czasu i nie spodziewam się, by każdy zakup karty SIM, która nie została zarejestrowana, miał być rozpracowywany w ten sposób. Jest też prawdopodobne, że gdy te dane zostaną ustalone, osoba inwigilowana będzie już w tym czasie używać kolejnej karty. Niemniej, dla pewności i swojego poczucia spokoju, jeśli tylko to jest możliwe, lepiej zapłacić gotówką.

Jeżeli uznamy to za zasadne, możemy na tablecie ustawić różnego typu zabezpieczenia. Aby to zrobić, warto szczegółowo przejrzeć jego ustawienia (ikona koła zębatego). Wchodząc w menu z pewnością znajdziemy opcję blokady ekranu poprzez wzór graficzny lub PIN cyfrowy. Warto przejrzeć kolejno dostępne opcje, chociaż zapewne większość użytkowników tego nie robi.

Możemy między innymi zdecydować, czy chcemy by na wyłączonym ekranie pojawiały się jakiekolwiek powiadomienia. Czasem przez niektóre z nich da się wejść do aplikacji, mogą też zdradzać, z jakich usług i firm korzystamy. Powiadomienie z banku ujawni, gdzie znajduje się nasz rachunek, który może zostać prześwietlony. Aplikacja do obsługi e-maila może zdradzić, w jakiej usłudze mamy pocztę, a to może ją narazić na sprawdzenie itd. Dlatego warto rozważyć wyłączenie powiadomień na ekranie blokady.

Zabezpieczając urządzenie możemy zdecydować też, czy na ekranie blokady (gdy tablet jest zablokowany) można dodawać nowego użytkownika, czy nie (co sugerowane). Dzięki zablokowaniu tej funkcji osoba niepowołana nie jest w stanie dodać konta i dostać się do naszych danych i aplikacji. Jest możliwe, że każdy użytkownik będzie miał własny wygląd ustawień, ale może się też zdarzyć, że wszyscy mają dostęp np. do pobranych plików. Tym samym może to zdradzać, czym się ostatnio zajmowaliśmy. Stwarza to też drugie, poważniejsze zagrożenie. Jeżeli tablet zostanie podpięty do komputera, to gdy jest w pełni zablokowany nie powinno dać się dostać do jego danych. Jeżeli jednak będzie możliwe dodanie konta nowego użytkownika na ekranie blokady, to po odblokowaniu tabletu przy jego użyciu możliwe jest udzielenie dostępu do wszystkich plików znajdujących się na urządzeniu poprzez komputer. Dlatego warto zadbać o zabezpieczenie tabletu zaczynając od ustawień blokady ekranu.

Jeżeli korzystamy z komplementarnego antywirusa z pakietem oprogramowania zabezpieczającego (np. AVG, BitDefender) możliwe jest również zablokowanie dodatkowym pinem wybranych przez nas aplikacji. Oferują to również niektóre wersje kompilacji systemu. Dzięki temu możemy dodać dodatkową linię obrony naszych danych.

W ustawieniach tabletu (lub antywirusa) możemy zdecydować, czy chcemy by jednorazowe odblokowanie chronionej aplikacji odblokowywało też wszystkie inne chronione, czy wolimy każdorazowo wpisywać pin, osobno w każdej z nich (Ustawienia -> Blokowanie aplikacji -> Odblokuj wszystkie aplikacje jednocześnie). Ustawienia te mogą się różnić w zależności od modelu i wersji systemu, ale warto zwrócić uwagę na te możliwości.

Nasza ważna aplikacja może być chroniona pinem (hasłem) tabletu, pinem do wrażliwych aplikacji (systemowym lub narzucanym przez antywirusa) oraz hasłem samej aplikacji. Część z nich będzie dodatkowo oferowała dwustopniowe logowanie z przesłaniem kodu na adres e-mail lub na wskazany numer telefonu. Chociaż obydwa mogą zostać łatwo przechwycone, opisany wyżej cały ciąg zabezpieczeń utrudnia dostęp do aplikacji, którą w ten sposób chronimy.

By zwiększyć nasze bezpieczeństwo korzystania z Internetu możemy rozważyć używanie przeglądarki TOR i / lub zdecydować się na usługę VPN, która dodatkowo może chronić dane przesyłane i pobierane przez aplikację. Warto mieć jednak świadomość, że część VPN zapisuje nasze wyszukiwania (tzw. logi), stąd trzeba sprawdzić w polityce prywatności, czy są one przechowywane. Może to być zaskakujące, ale niektóre z nich nie tylko zbierają nasze dane wyszukiwania, lecz również przechowują je przez minimum okres 2 lat i zobowiązują się do ich udostępniania służbom, zaś dane finansowe powiązane z naszymi danymi osobowymi są przechowywane nawet 7 lub 10 lat.

Z założenia VPN powinien tunelować (osłaniać) nasz ruch internetowy przed dostawcami Internetu i przed odwiedzanymi przez nas stronami. W pierwszym przypadku dostawca powinien widzieć, że korzystamy z VPN, ale nie powinien widzieć, jakie strony odwiedzamy. Natomiast chroniąc nas przed zbieraniem danych przez odwiedzane przez nas serwisy, VPN powinien dawać możliwość wyboru tymczasowego numeru IP, który wskazuje na fałszywą lokalizację, ukrywając tym samym naszą prawdziwą. Uzupełnieniem tej funkcjonalności może być moduł „anti track”, część pakietu oprogramowania towarzyszącego antywirusowi, która

poprzez zmianę naszego indywidualnego tzw. odcisku sprawia, że śledzenie naszej aktywności, zwłaszcza przy użyciu plików cookies, jest mocno ograniczone.

VPN wbudowany w przeglądarkę oferują Opera[23] (darmowe oraz płatne oferowane przez firmę zewnętrzną[24]) oraz Brave[25] (płatne, w oparciu o Guardian[26]). Natomiast myśląc o płatnym VPN warto przejrzeć politykę prywatności i sprawdzić, czy i jakie dane są zbierane, oraz jak długo są przechowywane. Warto zwrócić uwagę na rejestry aktywności (tzw. logi), co serwis pod tymi pojęciami rozumie i jak tych danych używa. Nie bez znaczenia jest przetwarzanie i przechowywanie danych (data retention) – klienta (np. płatnicze) i powstałych w wyniku korzystania z Internetu, powiązanych z logami.

Jeżeli odpowiada nam cena i kraj, z którego pochodzi dana usługa, warto uważniej przyjrzeć się temu, jak serwis określa swoją politykę prywatności (Privacy policy).

Niektóre obietnice składane przez serwisy brzmią wręcz mało wiarygodnie – np. obietnica anonimizacji danych osobowych, przy jednoczesnym ich przechowywaniu przez lata. Nie mamy możliwości sprawdzić, co to oznacza, a może równie dobrze oznaczać możliwość cofnięcia tego procesu na żądanie służb. Stąd, chociaż VPN zwiększa bezpieczeństwo, sam w sobie też może być dodatkowym czynnikiem ryzyka. Dlatego szczególnie te serwisy, które deklarują, że nie przechowują logów, mogą być bardziej przydatne.

Kilka wybranych usług VPN kładących nacisk na politykę braku logów (w różnym stopniu), kolejność alfabetyczna:

AVG Secure VPN - https://www.avg.com/pl-pl/secure-vpn[27] Dostępny osobno lub jako część pakietu AVG Ultimate.

Cyberghost VPN – https://www.cyberghostvpn.com/[28] (Należy do Kape Technologies)[29].

[23] https://www.opera.com/pl/features/free-vpn Polityka prywatności https://legal.opera.com/privacy/ (dostęp: 29.09.2023).
[24] Nazwa tej firmy nie jest ujawniona. Stan na 29.09.2023.
[25] https://brave.com/pl/firewall-vpn/ (dostęp: 29.09.2023).
[26] https://guardianapp.com/, Polityka prywatności https://guardianapp.com/privacy-policy/ (dostęp: 29.09.2023).
[27] Polityka prywatności https://www.avg.com/en-ww/vpn-policy#pc (dostęp: 29.09.2023).
[28] Polityka prywatności https://www.cyberghostvpn.com/pl_PL/privacypolicy (dostęp: 29.09.2023).
[29] https://www.kape.com/our-brands/ (dostęp: 29.09.2023).

ExpressVPN - https://www.expressvpn.com/[30] (Należy do Kape Technologies)[31].

Mullvad VPN – https://mullvad.net/ Przejrzysta polityka braku logów[32]. Zwraca uwagę możliwość anonimowej płatności za usługę gotówką.

Nord VPN – https://nordvpn.com/[33].

Surfshark VPN –https://surfshark.com/[34].

Decydując się na usługę VPN lepiej unikać porównywarek. Wiele serwisów rekomenduje usługi jednego większego dostawcy, które sprzedawane są pod różnymi markami. Stąd pozornie obiektywne recenzje i zestawienia mogą sugerować nam wybór między usługami VPN jednej firmy. Serwisy, których zadaniem jest zarobienie na linkach afiliacyjnych, raczej również nie powinny być brane pod uwagę przy podejmowaniu decyzji. Z uwagi na specyfikę usługi konieczne będzie, niestety, zagłębianie się w politykę prywatności.

Zaczynając od podobieństw pomiędzy smartfonem a tabletem, warto na koniec dostrzec, że część z nich nie będzie obsługiwać kart SIM. Tablet, który korzysta wyłącznie z WI-FI, powinien być bezpieczniejszy niż ten ze slotem na kartę SIM. Urządzenie jej pozbawione jest trudniejsze do zidentyfikowania. Będziemy używać go korzystając najczęściej z domowego routera, który też sam w sobie ma często wbudowane różne zabezpieczenia. Dodatkowo, możemy łączyć urządzenie z siecią tylko w momencie, gdy go używamy. Gdy odłączymy je od WI-Fi, jest niewidoczne i nienamierzalne.

Nie jest to w pełni wygodne, ale teoretycznie jest możliwe, by włączać urządzenie o wybranej porze, pobrać aktualizacje systemu, oprogramowania i pakietu bezpieczeństwa, a po zrobieniu tego pobrać wiadomości czy e-maile. Po udzieleniu odpowiedzi urządzenie można ponownie wyłączyć. Jest to dosyć nietypowe rozwiązanie, ale zwiększa bezpieczeństwo.

Oczywiście z tak okrojonego tabletu możemy również korzystać udostępniając Internet z przenośnego routera lub bezpośrednio ze swojego smartfonu. Większość urządzeń oferuje taką możliwość.

[30] Polityka prywatności https://www.expressvpn.com/pl/privacy-policy (dostęp: 29.09.2023).
[31] Więcej: https://www.kape.com/our-brands/ (dostęp: 29.09.2023).
[32] No-logging of user activity policy https://mullvad.net/pl/help/no-logging-data-policy/ (dostęp: 29.09.2023).
[33] Polityka prywatności https://my.nordaccount.com/pl/legal/privacy-policy/nordvpn/ (dostęp: 29.09.2023).
[34] Polityka prywatności https://surfshark.com/pl/privacy (dostęp: 29.09.2023).

Cyberobrona komputera

Stosunkowo najprostszym do obrony i umożliwiającym bezpieczne używanie jest laptop lub komputer stacjonarny. Zakładam, że w przypadku większości czytelników systemem operacyjnym jest Windows. Użytkownicy innych systemów będą mniej podatni na atak (lub będą wiedzieli, jak postąpić).

Jeżeli używamy (podobnie jak to było sugerowane w przypadku korzystania z tabletu) pakietu antywirusowego, VPN, przeglądarki TOR do zadań specjalnych, a na co dzień jednej z bezpiecznych przeglądarek, np. Brave, Chrome, Firefox lub Opery, to w dużej mierze już dbamy o bezpieczeństwo naszego komputera.

Jeżeli jednak zakładamy, że mógł on zostać zawirusowany, powinniśmy podjąć działania potwierdzające nasze podejrzenie, uratować dane i wyeliminować zagrożenie. Przede wszystkim nie wolno wówczas podpinać do komputera zewnętrznych nośników danych, które mogą nie być jeszcze zainfekowane. Jeżeli, w skrajnym przypadku, komputer padł ofiarą ransomware i jego dane zostały zaszyfrowane, a ktoś domaga się od nas okupu, to podpięcie czegokolwiek do komputera (np. dysku z kopią danych) sprawi, że również wszystko, co znajduje się na zewnętrznym urządzeniu, zostanie bezpowrotnie utracone. Dlatego spodziewając się wirusa, nie podpinamy żadnego dysku lub pendrive'a do komputera.

By zweryfikować nasze przypuszczenie warto zastanowić się, kiedy i w jaki sposób mogło dojść do zainfekowania. Przesłanie wirusa jest oczywiście możliwe i dawniej stanowiło prawdziwą zmorę, ale obecnie program antywirusowy, wykraczający swym zakresem działania poza tradycyjną nazwę, powinien sobie poradzić z zagrożeniem. Przeważnie e-mail lub niebezpieczna strona zostaną zablokowane jeszcze zanim zdążą nam zaszkodzić. Dużo częściej może dojść do zainfekowania komputera przez przeniesienie wirusa na pendrivie lub dysku zewnętrznym, których np. używamy w pracy na publicznym komputerze i podpinamy również do komputera domowego.

Jeżeli zakładamy, że komputer został zawirusowany, powinniśmy w pierwszej kolejności przeskanować go posiadanym antywirusem. Zanim zaczniemy, należy osobno i ręcznie zaktualizować program oraz jego bazę wirusów. Obydwie aktualizacje przeważnie można włączyć klikając prawym przyciskiem myszy na ikonę antywirusa znajdującą się koło zegara..

Jeżeli aktualizacje pobierają się normalnie i nie widzimy żadnych odstępstw od normy, możemy mieć nadzieję, że nasze przypuszczenie jest błędne. Bardzo często szkodliwe oprogramowanie będzie blokowało w pierwszej kolejności antywirus i uniemożliwiało jego aktualizację.

Przeprowadzamy pełne skanowanie komputera (lub najpierw szybkie, a później ponownie pełne). W zależności od programu, typu plików i ich rozmiaru całość operacji może potrwać od kilkunastu minut do kilku godzin.

Jeżeli skanowanie nic nie wykaże, a nadal coś nas niepokoi w sposobie działania komputera (np. spowalnia, zawiesza się, przegrzewa lub rzęzi) możemy dla pewności przeprowadzić skanowanie skanerem on-line. Przykładowe programy, kolejność alfabetyczna:

ESET online scanner – https://www.eset.com/pl/home/online-scanner/

F-secure online scanner –https://www.f-secure.com/en/online-scanner

mks_vir – https://mks-vir.pl/skaner-online/ Ponadto jeżeli przypuszczamy, że jakiś konkretny plik może zawierać szkodliwe oprogramowanie, lub wskaże nam go antywirus, możemy przesłać go, poprzez przeciągnięcie pliku między oknami komputera, na stronę Virus Total[35]. Wystarczy otworzyć przeglądarkę na stronie serwisu i z komputera przeciągnąć podejrzany plik. Dostępny tu system sprawdzi w oparciu o kilkanaście silników antywirusowych, czy zgłaszany przez nas plik jest bezpieczny. Wynik analizy zostanie wyświetlony od razu po jej ukończeniu w przeglądarce.

Jeżeli mamy wirusa (używając potocznego określenia), można usunąć go programem antywirusowym, ale znacznie lepiej przeinstalować system. Nawet po usunięciu zainfekowanego pliku lub oprogramowania może się okazać, że jakieś pozostałości wirusa nadal są gdzieś ukryte.

Gdy zależy nam na czasie, przeinstalowanie systemu i zainstalowanie używanych przez nas programów jest szybsze niż próba zwalczenia wirusa. Jest też bezpieczniejsze i skuteczniejsze, gdy wybierzemy opcję usunięcia danych i zainstalowania systemu od nowa na całym dysku.

Niektórym czytelnikom może się to wydawać trudne i przekraczające ich możliwości, ale warto rozważyć taką metodę rozwiązania problemu. Całkowite usunięcie danych, programów,

[35] https://www.virustotal.com/gui/home/upload (dostęp: 29.09.2023).

sformatowanie dysku i instalacja systemu mogą zająć około 30 minut. Walka z wirusem to godziny, a najczęściej 3-4 dni, które potrzebujemy, by komputer wrócił do pełnej sprawności i użyteczności.

Część osób może zdecydować się na skorzystanie z funkcji przywracania systemu oferowanej przez sam system. Jeżeli umożliwia ona odświeżenie systemu, ale pozwala zachować na dysku pliki użytkownika, jest możliwe, że pośród nich zostanie również szkodliwe oprogramowanie lub zainfekowany plik.

Jeżeli cokolwiek z zaproponowanej poniżej listy czynności nie powiedzie się, możemy udać się do serwisu komputerowego, który przeinstaluje system dla nas.

Aby przygotować się do przeinstalowania systemu musimy stwierdzić, czy możemy skasować pliki na dysku, czy potrzebujemy je odzyskać, bo nie mamy kopii (niestety nie wszyscy mają nawyk robienia kopii danych).

Pobranie danych z zawirusowanego komputera możemy zrobić na dwa sposoby – przy użyciu Tails[36] (metoda bezpieczna, szczegóły w dodatku o Tails) lub w Windows – prostsze, ale mniej bezpieczne, bo to w tym środowisku jest wirus[37].

Podczas wszystkich czynności ratunkowych laptop powinien być cały czas podpięty do zasilania sieciowego.

Aby odzyskać nasze dane potrzebujemy dysk lub pendrive – w zależności od wielkości danych, które mamy pobrać. Powinno to być puste urządzenie, na którym nie mamy innych danych. Podpinamy je do komputera ze szkodliwym oprogramowaniem, dlatego należy się liczyć, że gdyby znajdowały się na nim inne dane, to je również moglibyśmy utracić.

Metoda I (bezpieczna)

Wyłączamy komputer, podpinamy pendrive z systemem Tails i uruchamiamy komputer. Gdy na ekranie pojawiają się opcje bootowania, wciskamy zgodnie z informacją na ekranie wskazany

[36] https://tails.net/ (dostęp: 29.09.2023).

[37] Terminu „wirus" używam tu w potocznym znaczeniu, nie precyzuję, czy mamy do czynienia z malware, spyware, ransomware, adaware czy keylogerem. Ogólnie jako wirus traktuję szkodliwe oprogramowanie zainstalowane bez wiedzy i woli użytkownika w celu wyrządzenia mu szkody.

klawisz (najczęściej Esc, F2, F10, lub F12). Z wyświetlonego menu wybieramy „Boot Menu” i strzałkami i Enterem wybieramy pendrive z zainstalowanym Tails. Powinien być tak opisany, że będziemy wiedzieć, że to na pewno on (możliwe, że jest jedynym widocznym „USB drive”). Potwierdzamy enterem nasz wybór i system się włącza. Na pierwszym oknie, które się pojawia, mamy możliwość wybrać klawiaturę (jest polski), język (nie ma polskiego) oraz ustawić hasło (password). Ustawiamy hasło – pozwoli nam na dostęp do plików na komputerze. Zatwierdzamy wybór i system się uruchamia.

Podpinamy zewnętrzny nośnik i kopiujemy pliki. Skróty znane z Windows będą działać – kopiuj (Ctrl+C) i wklej (Ctrl+V). Odradzam wytnij (Ctrl+X), bo jeśli w trakcie kopiowania coś się stanie, to możemy stracić plik, który w momencie awarii był przenoszony w nowe miejsce.

Lepiej uważnie kopiować swoje foldery. Warto spojrzeć, czy nie pojawiło się w nich coś, czego sobie nie przypominamy. Jeśli tak, może warto to pominąć. Nie kopiujemy wszystkiego poprzez skrót „zaznacz wszystko” (Ctrl+A), a jedynie znane nam pliki.

Ta metoda jest bezpieczna, bo wirus z Windows nie będzie działała w środowisku Linux, a dodatkowo w Tails nie da się zainstalować nic bez zatwierdzenia ustawionym przez użytkownika hasłem. Ponadto w momencie wyłączenia komputera wszystkie zmiany w instalacji Tails na pendrivie zostają usunięte.

Po zakończeniu kopiowania wyłączamy komputer, wypinamy pendrive i możemy zainstalować nową wersję Windows.

Metoda II (mniej bezpieczna)

Pracujemy podobnie jak w Tails, ale ze świadomością, że komputer, na którym to robimy, jest zainfekowany. Do włączonego komputera podpinamy pusty pendrive lub dysk i podobnie jak powyżej kopiujemy pliki. Po ukończeniu wyłączamy komputer i wyciągamy pendrive z danymi. Może być potencjalnie zainfekowany, dlatego nie podpinamy go do żadnego innego komputera.

Uwagi przed instalacją

Przy kopiowaniu plików należy pamiętać o folderach systemowych, z których korzystamy: Moje dokumenty, Pulpit, Pobrane itp.

Należy zapisać klucz do Windowsa – na dolnym pasku klikamy prawym przyciskiem myszy ikonę systemu (cztery niebieskie kwadraty). Wybieramy z opcji „System". Alternatywnie: wciskamy na klawiaturze klawisz „Win" (z ikoną Windowsa) i w polu wyszukiwania wpisujemy „System".

Z wyświetlonej strony zapisujemy „Identyfikator produktu" i „Identyfikator urządzenia". Dla pewności możemy zrobić zdjęcie widocznego ekranu. W przypadku Windowsa 11 bardzo możliwe, że system sam przeniesie te dane i nie będzie konieczne ich przepisywanie.

Wybieramy ikonę Windowsa na ekranie lub na klawiaturze. W pole wyszukiwania wpisujemy „Opcje odzyskiwania". Na widocznym polu wybieramy „Resetuj ten komputer". Wybieramy, czy chcemy zachować pliki, czy je usunąć i od nowa zainstalować system. Następnie postępujemy zgodnie z wyświetlonymi wskazówkami. System zostanie przeinstalowany, a cała operacja zajmie przynajmniej 30 minut. Wraz z instalowaniem używanych przez nas programów powinno to zająć mniej niż 4 godziny, w zależności od tego, ile programów używamy.

Bardziej zaawansowani użytkownicy mogą zdecydować się na przygotowanie własnego pendrive'a instalacyjnego używając Balena Etcher[38] i obrazu ISO systemu pobranego ze strony Microsoft[39]. Pendrive instalacyjny należy przygotować na innym niż zawirusowany komputerze. Po uruchomieniu pendrive'a z Windows, może być konieczne włączenie go w „Boot menu", podobnie jak to było opisane powyżej w przypadku Tails.

Po przeinstalowaniu systemu jako pierwszy instalujemy pakiet antywirusowy i aktualizujemy go wraz z używaną przez niego bazą wirusów. Podpinamy pendrive z plikami, które odzyskaliśmy, i zanim cokolwiek z niego otworzymy, skanujemy cały nośnik przy użyciu antywirusa, w możliwie pełny sposób. Dla pewności powinniśmy go również przeskanować

[38] https://etcher.balena.io/ (dostęp: 29.09.2023).
[39] https://www.microsoft.com/software-download/windows11 (dostęp: 29.09.2023).

wybranym skanerem online. Jeżeli skanowania nic nie wykażą, możemy skopiować nasze uratowane pliki na komputer.

Jeżeli którykolwiek plik okaże się zawirusowany, należy go usunąć. Niestety czasem są straty, jest jednak duża szansa na to, że uda się ich uniknąć.

Cała operacja dobiegła końca. Dzięki przeinstalowaniu systemu nie mamy złośliwego oprogramowania na komputerze.

Jeżeli w trakcie spotkania ze służbami, ktokolwiek z funkcjonariuszy miał kontakt z naszym laptopem / komputerem, albo zostały nam one odebrane na jakiś czas, bezwzględnie należy przeinstalować system zgodnie z wcześniejszymi sugestiami. Fizyczny dostęp do komputera to najprostsza i najskuteczniejsza metoda zainfekowania go. Jeżeli służby uznają to za celowe, wyłączą antywirusa, zainstalują oprogramowanie szpiegujące (np. typu spyware, keyloger), włączą ponownie antywirusa i zwrócą komputer. Operacja ta zajmie kilka minut, a w stresie możemy nie zauważyć, że na chwilę został wpięty pendrive do gniazda USB.

Każde zajęcie sprzętu powinno być traktowane jako zagrożenie. Służby nie odbierają laptopa obywatelowi z troski o niego, ale by mu zaszkodzić. Dlatego po odzyskaniu sprzętu niezwłocznie należy przeinstalować system. Jeżeli nasza prywatność została tak głęboko naruszona, można się spodziewać eskalacji. Bezpieczniej będzie również nie prowadzić rozmów w jego pobliżu – przynajmniej do czasu rozpoczęcia instalacji systemu.

Są też znane przypadki umieszczania podsłuchów w obudowach laptopów. Jeśli tylko możemy, warto po odzyskaniu komputera zdjąć obudowę i sprawdzić, czy nie pojawiło się coś nowego wśród podzespołów komputera. Zapewne nie będzie zamocowane na stałe, a prowizorycznie przyklejone.

CZĘŚĆ IV – DODATKI

Tails

Wszelkie informacje o systemie Tails można znaleźć na stronie projektu [40], dlatego powtarzanie ich tutaj nie ma sensu. Jego zalety są tam najlepiej opisane, a jeśli czytelniczka / czytelnik nie posługują się biegle językiem angielskim, to przy użyciu Google Translate[41] możemy przetłumaczyć dowolną stronę, której link wkleimy w oknie formularza.

Aby przygotować swoją kopię systemu potrzebujemy:

- Pendrive, najlepiej 16 GB lub więcej;

- komputer, który nie jest zainfekowany (najlepiej rozpocząć przygotowania od przeskanowania komputera antywirusem);

- Program Balena Etcher[42];

- Plik ISO pobrany z działu Install[43] - wybieramy plik zgodnie z ikoną systemu, którego używamy.

Postępujemy zgodnie z zamieszczoną obrazkową instrukcją – w programie Balena Etcher wskazujemy plik ISO z systemem, co można porównać do dodania załącznika do e-maila.

Następnie program automatycznie wykrywa pendrive, na którym może zainstalować system. Proces jest całkowicie bezpieczny i nie uszkodzi naszego systemu. Balena Etcher oznacza nawet wykrzyknikiem dysk systemowy i pilnuje, by nic na nim nie instalować.

Po wybraniu pendrive inicjujemy proces instalacji systemu. Trwa to kilka minut i kończy się sprawdzeniem, czy zainstalowana wersja jest prawidłowa. Wszystko to odbywa się automatycznie. Gdy proces się zakończy, zostaniemy zapytani, czy chcemy przygotować kolejną kopię.

---

[40] https://tails.net/ (dostęp: 30.09.2023).
[41] https://translate.google.pl/?hl=pl&sl=auto&tl=pl&op=websites (dostęp: 30.09.2023).
[42] https://etcher.balena.io/ (dostęp: 29.09.2023).
[43] https://tails.net/install/windows/index.en.html Jeżeli używamy systemu Windows, potrzebujemy tej wersji. (dostęp: 30.09.2023).

Jeżeli wystąpi jakiś błąd – cały proces należy powtórzyć, ewentualnie można zmienić pendrive. Starszy może nie być odpowiedni, ale z nowym modelem nie będzie problemu.

Nasza wersja systemu jest zainstalowana tylko i wyłącznie na pendrive. Może zostać użyta na większości komputerów z dostępem do BIOS – konieczne jest, tak jak to było wspomniane powyżej, ponowne uruchomienie komputera. Gdy na ekranie pojawiają się opcje bootowania, wciskamy zgodnie z informacją na ekranie wskazany klawisz (najczęściej Esc, F2, F10, lub F12). Z wyświetlonego menu wybieramy „Boot Menu", i strzałkami oraz Enterem wybieramy pendrive z zainstalowanym Tails.

Tails będzie działał na komputerach z Windows w wersji 64-bit. Nie będzie działał, jeżeli Twój komputer ma ponad 10 lat i wersję systemu 32-bit. Nie działa też na komputerach Mac z procesorami M.1 i M.2 oraz na Chromebookach. Podobno nie działa również na dotykowych Microsoft Surface. Możliwe, że Windows 11 w wersji S również będzie blokował dostęp do BIOS.

Największą zaletą Tails jest jego bezpieczeństwo. Po jego użyciu i wyłączeniu komputera, wszystko, co robimy, zostanie usunięte. Dopóki pracujemy używając Tails, wszystkie nasze działania pozostają w pamięci podręcznej, a w momencie wyłączenia komputera bezpowrotnie znikają.

Zalety są oczywiste – możemy używać przeglądarki Tor[44], sprawdzić pocztę online lub używając Thunderbird. Przeważnie wystarczy wpisać swój adres e-mail i hasło, a znany nam zapewne program pocztowy pokaże zawartość naszej skrzynki mailowej.

Dowolny plik lub załącznik, który pobierzemy, jeśli tylko nie przeniesiemy go na dysk komputera lub pendrive, zostanie usunięty w chwili wyłączenia komputera. Mamy dostępny pełny pakiet Libre Office. Możemy się zapoznać z dokumentami, a jeśli to bezpieczne i konieczne, możemy skopiować pliki używając „Files" (z górnego menu wybieramy -> Applications -> Accessories -> Files). Aby to zrobić, będziemy musieli wpisać hasło, które ustawiliśmy przy włączaniu Tails.

Minusem dla niektórych będzie to, że przy każdym uruchomieniu systemu trzeba będzie wpisać hasło do sieci Wi-Fi. To pewna niedogodność, ale mamy też dzięki temu możliwość popracować spokojnie offline.

[44] https://www.torproject.org/ (dostęp: 30.09.2023).

Może czasem się zdarzyć, że na niektórych laptopach pojawia się czarny ekran. Trwa to kilka sekund i należy wówczas poczekać. Możliwe, że ma to związek z chwilowym spadkiem napięcia na gnieździe USB, a po jego powrocie do normalnego poziomu system znów działa.

System poinformuje nas, gdy będzie można go zaktualizować – jest to możliwe z poziomu systemu, ale powoduje zajęcie dodatkowego miejsca na pendrivie. Dlatego warto czasem przygotować pendrive od nowa, tak jak to było opisane powyżej.

System oferuje też funkcję „persistent storage" (stałego schowka), w którym możemy przechowywać pliki lub np. hasła z KeePass. Włączenie tej funkcji przy starcie systemu (tylko wtedy jest to możliwe) stanowi zagrożenie dla bezpieczeństwa, i jeżeli chcemy mieć pewność, że system usuwa wszystkie ślady naszej aktywności, nie należy włączać tej funkcji. Domyślnie jest wyłączona i jest to w pełni uzasadnione. Posiadanie samego systemu na pendrivie sprawia, że możemy łatwo i szybko zastąpić go nową wersją, a jeśli nawet zgubimy pendrive lub zostanie on przejęty, to nie ma na nim naszych osobistych danych.

Tails z uwagi na naszkicowany sposób działania (bo możliwości ma dużo większe) może też pozwolić osobom, które otrzymują załączniki od wielu różnych i często nieznanych ludzi, na ich bezpieczne otwarcie. Żaden załącznik otwarty w Tails nie może zainfekować komputera. Bez zgody użytkownika nie jest to możliwe.

Chromebook

Tails nie wymaga zakupu nowego komputera. Jeżeli jednak wolimy gotowe rozwiązania, to można zastanowić się nad Chromebookiem, pod warunkiem jednak, że będziemy w stanie używać go w bezpieczny sposób. ChromeOS[45] jest super bezpiecznym i świetnie zaprojektowanym systemem. Wygoda używania go jest większa niż w przypadku innych systemów. Komputery są lekkie i pracują przez wiele godzin. Znacznie dłużej niż standardowe komputery z Windows. To możliwe dzięki temu, że system od Google jest bardzo lekki i na pewno nie jest obciążający dla komputera.

Chromebooka możemy używać w dwóch trybach – z logowaniem na konto Google i bez niego, w trybie gościa. Jeżeli zdecydujemy się na logowanie, to w komfortowy sposób będziemy mogli skorzystać z tego, co oferuje pakiet usług Google. Ma to jednak tę wadę, że w razie przejęcia komputera przez służby, chociaż możemy nie być zalogowani, od razu widać, jakiego konta używamy, i wszystko, co na nim się znajduje, zostanie przypuszczalnie w niedługim okresie udostępnione służbom, które o to wystąpią.

Natomiast druga opcja – wykorzystanie trybu gościa – tak jak było nieco wcześniej wspomniane, nie zapisuje naszej aktywności na urządzeniu. Podobnie jak w przypadku Tails, w momencie wyłączenia urządzenia historia zostanie wykasowana.

Jeżeli założymy, że mamy konto, na którym nie przechowujemy nic istotnego, możemy je traktować jako stałe konto, które po włączeniu Chromebooka będzie widoczne. Natomiast inne konto, które będzie się wiązało z naszą pracą i ujawnienie danych z niego może być niebezpieczne, nie powinno nigdy być zalogowane na stałe.

W przeciwieństwie do Tails raz zapisane dane logowania do Wi-Fi są dostępne dla wszystkich użytkowników, w tym i dla niezalogowanego konta gościa. Zanim zdecydujemy się na Chromebook (bo możliwe, że nie jest on odpowiedni dla każdego), należy zapoznać się z zasadami aktualizacji. Z założenia mają one być dostępne dla danego modelu aż przez 10 lat od momentu jego produkcji. Dlatego warto przed ewentualnym zakupem sprawdzić tzw. „Auto

[45] https://www.google.com/intl/pl_pl/chromebook/chrome-os/ (dostęp: 30.09.2023).

Update Policy”[46] i upewnić się, że ten komputer, który nas interesuje, ma przed sobą długie lata aktualizacji. Wiele poleasingowych Chromebooków, bardzo przystępnych cenowo, jest już po końcu aktualizacji (EAU – End of Auto Update).

[46] https://support.google.com/chrome/a/answer/6220366?sjid=100756204796581149-EU (dostęp: 30.09.2023).

Jak inwigilowana lekarka ma leczyć pacjentów

Na koniec skrajny przykład. Do gabinetu lekarki weszły służby i przejęły dokumentację medyczną pacjentów. Były to działania bezprawne, a po niedługim czasie dokumentacja została zwrócona.

Czysto teoretycznie - gdyby dane wrażliwe były przechowywane w formie elektronicznej, na specjalnej platformie, której nazwa jest nieznana służbom, byłyby bezpieczne. Mam na myśli oprogramowanie oferowane do zarządzania danymi pacjentów operujące w odpowiednio zabezpieczonej chmurze, do której opłacany jest dostęp w postaci abonamentu, z którego mogą skorzystać lekarze.

Dodatkowym zabezpieczeniem w korzystaniu z takiej platformy może być komputer z Tails i przeglądarką TOR lub Chromebook w trybie gościa. W sytuacji wtargnięcia służb do kliniki, komputer z Tails można wyłączyć w niecałe 10 sekund. Aby to zrobić, przytrzymujemy włącznik komputera do momentu jego wyłączenia. Przeprowadzamy w ten sposób twardy reset i kasujemy wszystko, co było otwarte. Przejęty komputer nie zawiera materiałów, które mogłyby być użyte przeciwko nam. Jednocześnie dane pacjentów są bezpiecznie chronione hasłem, w nieznanym służbom serwisie. Może nawet logowanie do niego zabezpiecza przesłanie kodu na e-mail lub telefon (tzw. 2FA – Two Factor Autentication), albo klucz typu YubiKey[47]?

A jakie możliwości daje Chrombook w podobnej sytuacji? Używamy go jako gość, zauważamy nielegalne wtargnięcie. Wciskamy przycisk wyłącznika i trzymamy aż do zgaszenia. Po kilku sekundach Chromebook się wyłącza, zamykając wszystko, czego używaliśmy, i całkowicie kasując historię.

Jeżeli jednak z jakiegoś powodu byliśmy zalogowani na koncie, to po wylogowaniu – dostępne również przez chwilowe przytrzymanie przycisku wyłącznika – możemy zresetować urządzenie do ustawień fabrycznych. Aby to zrobić, przyciskamy równocześnie klawisze Ctrl + Alt + Shift + R. Gdy wyświetli się taka możliwość, wybieramy „reset”. W ciągu 20-30 sekund jesteśmy w stanie przywrócić Chromebooka do ustawień fabrycznych, jednocześnie usuwając wszystkie konta, hasła do Wi-Fi czy historię naszej aktywności.

[47] https://www.yubico.com/ (dostęp: 30.09.2023).

Aby ułatwić sobie działanie w sytuacji stresowej, warto oznakować kolorem te klawisze, których mamy użyć (np. pisakiem, naklejką). W spokojnych warunkach warto przećwiczyć czynności, które być może będziemy musieli przeprowadzić w sytuacji dużego stresu. Dlaczego nie można zrobić tego samego w przypadku komputera z Windows? Można go wyłączyć, ale cała historia naszej działalności, po ponownym włączeniu będzie dostępna.

Bezpieczne przechowywanie i kopiowanie plików

Z uwagi na liczbę plików, z którymi mamy do czynienia, konieczne jest standardowe postępowanie, by zminimalizować ryzyko ich utraty. Proces zabezpieczania plików powinien być również na tyle prosty, by nie zniechęcał do podjęcia takiego działania.

Oryginały i kopie

Z założenia należy robić kopie swoich plików. Pozwala to uniknąć ich utraty w razie awarii dysku.

Oryginały

Najczęściej oryginały plików będą się znajdowały bezpośrednio na dysku laptopa / komputera. Rzadziej na dysku zewnętrznym. To są pliki, których używamy na co dzień.

Kopie

Kopia bezpieczeństwa powinna być aktualizowana w określonych interwałach czasowych. Przy użytku „domowym" powinno wystarczyć raz na miesiąc, najlepiej w określony dzień. Można wówczas ustawić sobie przypomnienie w kalendarzu (np. 1 dnia miesiąca).

Decydując, jak często chcemy robić kopie, warto rozważyć, co jesteśmy w stanie stracić, jeśli nasz główny dysk się zepsuje w okresie między wykonywaniem kopii danych. W razie awarii tracimy wszystko, co zostało zapisane na dysku w ciągu np. miesiąca. Dlatego też warto po zakończeniu pracy nad ważnym projektem lub zapisaniu czegoś istotnego robić nadprogramową kopię.

Aby uniknąć żmudnego porównywania i wyszukiwania plików, warto wyrobić sobie nawyk kopiowania w jedną stronę – z dysku laptopa na dysk zewnętrzny. Nigdy w drugą stronę.
Podczas kopiowania zawsze wybieramy opcję nadpisania starszych plików nowszymi. Dlatego ważny jest kierunek kopiowania – z dysku laptopa na dysk zewnętrzny.

Dysk zewnętrzny nie służy do pracy, ani do codziennego użytku - jest tylko archiwum, do którego kopiujemy oryginały plików z dysku głównego. Gdy dysk laptopa ulegnie awarii,

możemy wtedy jednorazowo skopiować wszystko z dysku zewnętrznego na nowy laptop i w ten sposób odzyskać dane.

Z uwagi na to, że układ subfolderów w folderze może się zmieniać, a pliki edytowalne (np. tekstowe) będą edytowane, dobrze raz na czas skasować kopię (cały folder) i w jego miejsce zrobić nową kopię.

Dysk twardy

Żaden dysk twardy nie jest wieczny. Nawet dysk w okresie gwarancyjnym może ulec uszkodzeniu.

Mając oryginały plików na jednym dysku (np. laptopa), a kopie na innym, jesteśmy bezpieczniejsi. Przezorni bardzo istotne materiały trzymają w dwóch kopiach, na osobnych dyskach zewnętrznych, najlepiej różnych producentów albo przynajmniej z różnych serii produkcyjnych. W warunkach domowych dysk z oryginałami i dysk z kopiami powinny wystarczyć. Niektórzy oprócz kopii na dysku robią też kopię w chmurze, przy czym nie powinna to być kopia wykonywana w oparciu o folder z oryginalnymi plikami. Dla bezpieczeństwa tworzymy folder „kopia danych" i tylko do niego dajemy uprawnienia chmurze. Dzięki temu, jeśli będzie to konieczne, możemy szybko odciąć chmurę od naszych plików na dysku. Chmura pobierze pliki tylko z tego folderu i je usunie, stąd nie ma ryzyka, że każdy plik będzie zajmował podwójnie miejsce na dysku twardym.

Ponadto, najważniejsze pliki można kopiować na pendrive, który nosimy przy sobie.

Na nowym dysku twardym warto zapisać w nazwie dysku oraz w pliku tekstowym, do kiedy ma gwarancję. Od momentu pierwszego użycia (zakupu) są to przeważnie 2 lub 3 lata.

Przykładowa nazwa dysku:
KOPIE_PLIKOW_do_05_2024
(Dysk użyty po raz pierwszy w maju 2022, gwarancja 2 lata)

Informacja w pliku txt np. o nazwie „INFO_o_dysku"
„dysk używam od 30.10.2022

gwarancja 2 lata (do 30.10.2024)”

Gdy dobiega końca okres gwarancyjny, dane powinny zostać skopiowane na nowy dysk, a dysk po gwarancji może stać się dodatkową kopią bezpieczeństwa. Dysk po gwarancji nie powinien być główną kopią danych, bo w razie awarii dysku laptopa, awaria kopii jest również możliwa.

Trwałość danych

Trwałość plików determinuje trwałość nośnika, na jakim są zapisane, oraz ich format.

Pendrive – długa trwałość (pamięć flash), na pewno kilkanaście lat.
Wyjątek stanowią pendrive’y płaskie o kształcie karty kredytowej – duża awaryjność mechaniczna.

Dysk SSD – również pamięć flash, przypuszczalnie kilkanaście lat. Nowa technologia, niesprawdzona.

Dysk HDD – standardowy dysk 2.5 cala lub 3.5 cala (taki jak w laptopie lub komputerze).
Trwałość do 2-3 lat. Zdarzają się z gwarancją na 5 lat. W razie upadku, zwłaszcza podczas pracy, wszystkie dane mogą zostać natychmiast bezpowrotnie utracone.

Płyty DVD – dane bezpieczne do 5 lat. Powyżej tego okresu możliwa utrata, chociaż często udaje się odczytać dane z płyt kilkunastoletnich.

Płyty CD – Bezpieczeństwo podobne jak płyt DVD, chociaż niektórzy twierdzą, że mniejsze.

Przechowywanie danych w chmurze (Dropbox, Google Drive, One drive i inne) lub usługi **typu cloud storage** (pCloud, MyAirBridge, WeTransfer).
Dane są przechowywane tak długo, jak długo istnieje firma, która świadczy taką usługę. Nie wiadomo, kto ma do nich dostęp, ani gdzie są przechowywane.
Bardzo ograniczona możliwość pobrania wszystkich danych w razie potrzeby.
Zdarzają się awarie i uszkodzenia plików.

Format plików

Przeważnie w okresie ok. 7-10 lat zmieniają się formaty plików. Po jakimś czasie pliki starsze mogą okazać się nieczytelne, stąd, jeśli to możliwe, warto pliki zapisywać ponownie w nowych formatach. Pliki tekstowe warto również mieć w kopii w .pdf. W razie utraty danych i odzyskiwania plików, pdf-y są w 100 % odzyskiwalne, a pliki .docx, .doc lub .odt bardzo często nie, lub tylko częściowo.

Nazwy folderów i plików

W nazwach folderów i plików nie używamy polskich znaków. Jeśli w nazwach podajemy datę powstania wersji, lepiej zrobić to na początku pliku, przy czym data powinna być zapisana w następujący sposób: 2018_08_02_nazwa_pliku
Wtedy pliki układają się według daty powstania.

W nazwach plików i folderów używamy łącznika (podkreślnika) pomiędzy słowami:
np. Zdjecia_z_wakacji

Jeśli w nazwach plików używamy rzeczowników w Mianowniku, łatwiej jest je wyszukać:
np. zdjecia_wakacje_Grecja_2023

Wpisując w wyszukiwarkę którekolwiek z tych słów, znajdziemy bez problemu właściwe pliki.

Dlaczego podkreślnik? Jeśli będziemy konwertować folder do pliku .zip, eksportować go do chmury, czy otwierać folder spod Windows na Mac lub pod Linuxem, nazwy folderów i plików nie ulegną zmianie. Unikniemy „zsunięcia" słów w np. „Zdjeciazwakacji" czy „zdjeciawakacjeGrecja2023".

Symptomy awarii

Jeżeli dysk twardy w laptopie zaczyna buczeć, pracować nierówno lub wyraźnie się przegrzewa, powinniśmy niezwłocznie skopiować wszystkie dane. Jeśli zdarza się, że dysk się „zwiesza" (zacina), jego żywotność z pewnością dobiega końca. W sytuacji ewakuacji danych lepiej robić to folderami, niż jednocześnie ewakuować wszystko – bardziej to obciąży dysk i szybciej może on przestać pracować.

Uwagi końcowe

Planując zabezpieczenie swoich danych trzeba wiedzieć, przed czym chcemy się uchronić. Wiedząc, co traktujemy jako zagrożenie dla naszych danych, łatwiej się zabezpieczyć przed ich utratą.

Zanim zaczniemy kopiować pliki, przed podpięciem zewnętrznego nośnika powinniśmy przeskanować laptop programem antywirusowym – najlepiej zainstalowanym i on-line (np. mks_vir, F-secure). Jeśli laptop będzie zawirusowany, unikniemy wtedy ryzyka utraty kopii danych. Jeśli jest czysty, możemy zrobić nową kopię danych.

Logi z inwigilowanego smartfonu

Poniżej zamieszczam pismo, które przesłałem do operatora telefonii komórkowej wraz z wybranymi wówczas logami. Pogrubienia w tekście własne.

***** ***

Szanowni Państwo,

W trakcie rozmowy z numerem +48 XXX XXX XXX w dniu 19 marca 2023 pomiędzy godziną 16:58:57 a 17:30:06 wystąpiły problemy i zakłócenia połączenia, a następnie połączenie zostało przerwane. Dwie ostatnie próby ponownego nawiązania połączenia skutkowały natychmiastowym przełączeniem na pocztę, tak jakby bez sygnału.

Godziny połączeń podaję poniżej za wykazem widocznym w XXXXXX.

W telefonie znalazłem w logach takie informacje, które pokrywają się czasowo z tą rozmową (jest przesunięcie o godzinę pomiędzy informacjami widocznymi w serwisie XXXXXX w stosunku do czasu np. wysłania wiadomości widocznego w telefonie).

LV:I, TM: 2023-03-19 18:00:44, TAG: ##XLogger##, MSG: com.miui.cloudservice.sysbase.service.SimStateMonitorService::recheckSIMStatus@SimStateMonitorService.java:109, thread:2--**Broadcast removed.**

LV:I, TM: 2023-03-19 18:00:48, TAG: ##XLogger##, MSG: com.miui.cloudservice.sysbase.service.SimStateMonitorService::recheckSIMStatus@SimStateMonitorService.java:109, thread:2--**Broadcast removed.**

LV:I, TM: 2023-03-19 18:03:29, TAG: ##XLogger##, MSG: com.miui.cloudservice.sysbase.receiver.TelephonyStateChangeReceiver::onReceive@TelephonyStateChangeReceiver.java:18, thread:2--Intent { act=miui.android.intent.action.SIM_STATE_CHANGED flg=0x5000010 cmp=com.miui.cloudservice.sysbase/.receiver.TelephonyStateChangeReceiver (has extras) }

EXTRAS: ['android.telephony.extra.SUBSCRIPTION_INDEX' => '2' 'slot_id' => '1' 'subscription_id' => '2' 'phone_id' => '1' 'phoneName' => 'Phone' 'reason' => 'null' **'rebroadcastOnUnlock' => 'true' 'ss' => 'LOADED'** 'phone' => '1' 'subscription' => '2']

LV:I, TM: 2023-03-19 18:03:29, TAG: ##XLogger##, MSG: com.miui.cloudservice.sysbase.service.SimStateMonitorService::recheckSIMStatus@SimStateMonitorService.java:125, thread:2--**Broadcast inserted.**

LV:I, TM: 2023-03-19 18:03:29, TAG: ##XLogger##, MSG: com.miui.cloudservice.sysbase.service.SimStateMonitorService::recheckSIMStatus@SimStateMonitorService.java:125, thread:2--**Broadcast inserted.**

LV:I, TM: 2023-03-19 18:03:29, TAG: ##XLogger##, MSG: com.miui.cloudservice.sysbase.service.SimStateMonitorService::recheckSimId@SimStateMonitorService.java:211, thread:2--**Broadcast SIMID ready.**

LV:I, TM: 2023-03-22 09:14:15, TAG: ##XLogger##, MSG: com.miui.cloudservice.sysbase.service.SimStateMonitorService::recheckSIMStatus@SimStateMonitorService.java:109, thread:2--**Broadcast removed.**

Plik z logami obejmuje okres od 2021-09-24 09:36:17 do 2023-03-23 23:50:14

Rebroadcast wystąpił tylko w okresie od 2023-03-19 18:00:44 do 2023-03-22 09:14:15, a wszystkie logi z 18 marca 2023 są usunięte.

20 marca wymieniłem kartę SIM na nową i zmieniłem aparat telefoniczny.

Czy słusznie przypuszczam, że tamto połączenie oraz mój telefon w tym okresie mogły być podsłuchiwane przez policję lub służby specjalne?

Podejrzenie powyższego ma związek z moim udziałem w manifestacji i spisaniem danych, wraz z numerem telefonu, przez policję.

Z poważaniem

Lech Mikulski

***** ***

Po kilku dniach odebrałem telefon od operatora telefonii komórkowej. Zostałem poproszony o nakreślenie sytuacji. Gdy zapytałem, czy moje przypuszczenia mogą być zasadne, w odpowiedzi usłyszałem zdanie, które mniej więcej mogło mieć następujące brzmienie.

„Oczywiście zweryfikujemy pana zgłoszenie, ale zapewne pan wie, że jeżeli pana przypuszczenia się potwierdzą, nie będziemy mogli panu udzielić odpowiedzi".

Do dziś jej nie uzyskałem.

Autor i jego historia

Lech Mikulski (ur. 1979) – Wykładowca akademicki. Reżyser filmowy, producent i kierownik produkcji. Specjalizuje się w realizacji filmów dokumentalnych oraz filmów krótkometrażowych. Fotograf, były dziennikarz mediów lokalnych.

Jego filmy pokazywane były na festiwalach i targach filmowych w Polsce i w Europie. Autor filmu dokumentalnego „Nie pogubić się" prezentowanego w telewizji Kino Polska oraz „Morze twoimi oczami" emitowanego w TVP 2.

Ostatnie lata spędził, wspólnie z żoną Joanną Preizner, na protestach w obronie demokracji, praw kobiet i praw osób LGBTQ.

***** ***

Bezpośrednią przyczyną napisania niniejszej publikacji była **sytuacja opisana w artykule autorstwa Pani Redaktor Angeliki Pitoń, opublikowanym w Gazecie Wyborczej, zatytułowanym *Autor transparentu zarekwirowanego na Manifie odpowie za znieważenie narodu lub państwa polskiego? Sprawa w prokuraturze***[48].

Artykuł jest dostępny pod adresem:

https://krakow.wyborcza.pl/krakow/7,44425,29589158,autor-transparentu-f-ck-poland-odpowie-za-zniewazenie-narodu.html?_ga=2.94906908.1800874350.1679773494-1408104321.1679773492

Oboje z żoną wydaliśmy w związku z tą sytuacją oświadczenie, które znajduje się na kolejnej stronie.

[48] Angelika Pitoń, *Autor transparentu zarekwirowanego na Manifie odpowie za znieważenie narodu lub państwa polskiego? Sprawa w prokuraturze* https://krakow.wyborcza.pl/krakow/7,44425,29589158,autor-transparentu-f-ck-poland-odpowie-za-zniewazenie-narodu.html?_ga=2.94906908.1800874350.1679773494-1408104321.1679773492 (dostęp: 01.10.2023).

Oświadczenie Joanny Preizner i Lecha Mikulskiego

“Solidarność naszą bronią!” – powtarzamy w trakcie demonstracji przeciw łamaniu praw człowieka przez Polskę. Mamy konstytucyjne prawo do protestu wobec zła. Mamy prawo do wolności słowa i prawo do zgromadzeń. Mamy prawo do dokonywania wyborów, które uznajemy dla nas za najlepsze. Mamy prawo bronić własnych przekonań. Wierzymy, że choć różnimy się od siebie, wszyscy jesteśmy równi. Jesteśmy głęboko przekonani, że nie wolno być obojętnym. Ten, kto nie reaguje na zło, jest za nie moralnie odpowiedzialny tak samo jak ten, kto się zła dopuszcza.

Nie jest naszym celem atakowanie kogokolwiek, a forma, jaką wybraliśmy dla naszego protestu, jest właściwa wobec ogromu zła, przeciwko któremu występujemy, i odzwierciedla nasze emocje i uczucia z nim związane.

18 marca 2023 roku razem z kilkuset innymi osobami wzięliśmy udział w krakowskiej Manifie. Po pokojowej demonstracji rozpoczął się marsz i wówczas nieumundurowani policjanci nas otoczyli. Zostaliśmy oddzieleni od grupy i odprowadzeni na bok, gdzie czekały już radiowozy i około 20 funkcjonariuszy. Powodem był plakat formatu A4 trzymany przez Lecha Mikulskiego, na którym z jednej strony widniało hasło „Women’s rights = human rights” (Prawa kobiet prawami człowieka), a z drugiej „Fuck Poland for breaking human rights” (Pieprzyć Polskę za łamanie praw człowieka). Plakat został zatrzymany przez policję. Dziś, 28 marca 2023 roku, L. Mikulski stawił się w charakterze świadka na przesłuchaniu w sprawie podejrzenia o „znieważenie RP”, czyli o popełnienie przestępstwa z artykułu 133 Kodeksu Karnego, za co grozi do trzech lat pozbawienia wolności. W obecności swojej prawniczki złożył wyjaśnienia.

Motywacje naszego protestu są następujące:

1. Kobiety w Polsce mają ograniczone prawo do podejmowania decyzji dotyczących swojego zdrowia i życia. Nie mają prawa do aborcji, nie otrzymują odpowiedniej opieki lekarskiej.
2. Kobiety są zmuszane do rodzenia śmiertelnie lub poważnie chorych dzieci, po czym pozostawiane są bez wsparcia ze strony państwa.
3. Kobiety otrzymują niższą płacę za tę samą pracę co mężczyźni i mają mniejszą szansę na awans zawodowy niż oni.

4. Kobiety i dzieci nie są wystarczająco chronione przez prawo i powołane do tego instytucje, gdy spotykają się z różnymi formami przemocy seksualnej, ekonomicznej, psychicznej i fizycznej.
5. Na granicy polsko-białoruskiej od półtora roku, łamiąc prawo, polskie służby wypychają uchodźców – dorosłych i dzieci - szukających w Polsce pomocy i/lub azylu. Ci, którzy próbują im tej pomocy udzielić, są przez państwo szykanowani i zastraszani.
6. Członkowie społeczności LGBTIQA+ spotykają się z legitymizowanymi przez polskie władze i kościół katolicki (świadomie używamy małych liter w pisowni nazwy tej instytucji) atakami i mową nienawiści. Nie mają równych praw i nie czują się w Polsce bezpiecznie. Wielu z nich żyje w nieustającym lęku lub decyduje się na emigrację. Niektórzy popełniają samobójstwa.

Jako polscy obywatele nie zgadzamy się na to. Nasze państwo – jedyne, jakie mamy i jedyne, za które czujemy się odpowiedzialni – nie czyni tego w naszym imieniu. Mamy prawo, żeby się temu przeciwstawić i korzystając z wolności słowa mówić o tym w takiej formie, jaką uznamy za właściwą.

Joanna Preizner

Lech Mikulski