FUNDACJA PANOPTYKON

ODZYSKAJ KONTROLĘ NAD INFORMACJĄ

Samouczek dla dziennikarzy i nie tylko

Opracowanie:

Anna Obem

Współpraca:

Beata Biel
Wojtek Bogusz
Katarzyna Szymielewicz

Fundacja Panoptykon
Warszawa 2017

SPIS TREŚCI

WSTĘP

Publikując w 2014 r. fragmenty nagrań z tzw. afery taśmowej, redakcja tygodnika „Wprost" z pewnością liczyła się z tym, że prędzej czy później sprawą zainteresują się służby, które będą chciały wiedzieć, jak te informacje do niej trafiły. Ale przeszukanie to tylko jedna – i bynajmniej nie najpowszechniejsza – droga odkrycia cennych informacji.

Ochrona informacji ma fundamentalne znaczenie w pracy dziennikarza, nie tylko z przyczyn prawnych, ale też ze względu na jego wiarygodność i komfort pracy. W tym kontekście warto spojrzeć na problem bezpiecznego zarządzania informacją o wiele szerzej niż tylko przez pryzmat zabezpieczenia nośników czy redakcji. Równie ważne – i częściej spotykane – zagrożenia związane są z codzienną aktywnością dziennikarza w sieci i poza nią.

Do bezpiecznego zarządzania informacją nie wystarczy jednak kilka aplikacji zainstalowanych na komputerze czy telefonie. Przede wszystkim przyjrzyj się temu, jak na co dzień korzystasz z sieci i urządzeń, jak przechowujesz informacje i jak się nimi dzielisz. Jeśli na przykład zamieszczasz na swoim profilu na Facebooku kontrowersyjne wpisy, miej świadomość, że bynajmniej nie poruszasz się w sferze prywatnej. Abstrahując od tego, czy redakcja ma prawo wyciągnąć konsekwencje służbowe z wypowiedzi, która pojawiła się na prywatnym – przynajmniej teoretycznie – profilu dziennikarza (jak zadecydował sąd w sprawie zwolnionej z RDC Ewy Wanat – niekoniecznie), warto liczyć się z faktem, że informacja raz opublikowana w sieci będzie poza kontrolą.

Konieczne może się okazać zrewidowanie niektórych nawyków. Szyfrowanie e-maili czy SMS-ów pomoże zabezpieczyć informacje, ale tylko pod warunkiem, że jednocześnie dbasz o podstawy bezpieczeństwa, np. zmianę haseł czy kontrolowanie, kto ma dostęp do usług i informacji. Zaś lekceważenie tej sfery może skończyć się np. tak, jak w przypadku radiowej Jedynki: jej szefowie do dziś nie wiedzą, kto zamieścił na facebookowej stronie radia mem szydzący z prezydenta Andrzeja Dudy.

W cyfrowej rzeczywistości sposoby korzystania z informacji, przechowywania jej i dzielenia się nią zmieniają się dynamicznie. Podobnie jest z zagrożeniami. Dlatego nie da się stworzyć gotowej instrukcji, której przestrzeganie zagwarantuje bezpieczeństwo informacji w każdym kontekście i która nie zdezaktualizuje się wraz z rozwojem nowych technik i narzędzi do komunikacji (oraz zmianami w przepisach). O wiele lepszą inwestycją czasu i energii będzie rozwijanie kompetencji, np. umiejętności oceny ryzyka w konkretnej sytuacji i dopasowania do niej najlepszego rozwiązania.

W tym samouczku staramy się wprowadzić w to, jak to robić. Wyjaśniamy, jakie podstawowe zasady bezpieczeństwa należy zachować na co dzień, i pomagamy samodzielnie radzić sobie z zagrożeniami, a przede wszystkim je przewidywać i minimalizować. Nie zamierzamy zniechęcać do korzystania z Internetu i nowych technologii, a jedynie pomóc odzyskać maksymalną kontrolę nad informacją i komunikacją.

Niniejszy samouczek został podzielony na cztery części. Na początku przedstawiamy czynniki, jakie warto wziąć pod uwagę przy **analizie ryzyka** (w szczególności to, z jakim rodzajem przetwarzanych informacji mamy do czynienia i kto może mieć do nich dostęp). W pozostałych – praktycznych – częściach koncentrujemy się na: **podstawowych zasadach bezpieczeństwa**, **ochronie źródeł dziennikarskich** oraz **świadomym zarządzaniu cyfrowym „ja"**.

I. ANALIZA RYZYKA

Jakie informacje trzeba chronić?

Nie każda informacja musi być chroniona w takim samym stopniu, jednak odpowiedzialna ocena stopnia poufności informacji na początku może być trudna. Dlatego lepiej przesadzić ze środkami ostrożności niż je zaniedbać.

Rodzaje informacji

- **Informacja publiczna** to taka, którą publikujemy. Należy pamiętać, że informacja prywatna opublikowana w sieci (np. na Facebooku czy Twitterze) staje się informacją publicznie dostępną. W przypadku informacji publicznej pojawia się ryzyko zniekształcenia, zmanipulowania lub przypisania jej osobie, która nie była autorem.
- **Informacja poufna** to przede wszystkim dane osobowe informatorów, ale też inne informacje, które – jeśli trafią w niepowołane ręce – mogą komuś zaszkodzić, niosąc za sobą negatywne konsekwencje dla jego życia lub pracy.
- **Informacja prywatna** to każda informacja, która dotyczy sfery pozazawodowej. Chociaż sama w sobie nie musi być kompromitująca, może być wykorzystana np. do podważenia czyjejś wiarygodności zawodowej. Wrażliwość informacji prywatnej jest niedoceniania – wiele osób nie zdaje sobie sprawy, że publikując np. na portalach społecznościowych informacje o sobie i swoich bliskich, czyni z nich informacje publiczne, narażając się na negatywne konsekwencje.

Wygoda albo bezpieczeństwo? Pozorny dylemat

Zainteresowanie narzędziami zwiększającymi bezpieczeństwo informacji przychodzi falami. Na przykład po ujawnieniu przez Edwarda Snowdena informacji o amerykańskich programach inwigilacji skokowo wzrosła liczba użytkowników nieśledzącej wyszukiwarki DuckDuckGo. Po przyjęciu przez polskie władze ustawy inwigilacyjnej pojawił się boom na takie rozwiązania jak VPN, Tor czy Signal. Z czasem jednak to zainteresowanie spadło – być może dlatego, że – na pierwszy rzut oka – korzystanie z bezpiecznych narzędzi komunikacyjnych wydaje się trudniejsze czy mniej komfortowe. Ale ten dylemat jest pozorny – na rynku dostępnych jest wiele narzędzi, które są i bezpieczne, i wygodne. Najlepszy przykład to komunikator Signal (alternatywa dla SMS-ów) i szyfrowany wideo-czat meet.jit.si (alternatywa dla komunikatorów komercyjnych, np. Skype'a) – oba są proste w użyciu i nie wymagają ani nakładów finansowych, ani czasowych.

Warto też pamiętać, że nie każda informacja wymaga jednakowej ochrony. Zastanów się:

- jakie informacje są prywatne i wymagają zwiększonej ochrony,
- jakie są na tyle wrażliwe, że trzeba zastosować najwyższe środki ostrożności.

W wielu przypadkach wystarczy przestrzeganie prostych zasad higieny. Np. aktualizowanie oprogramowania czy okresowa zmiana haseł – nie wiążą się z większym wysiłkiem, szczególnie jeśli te zasady staną się elementem codziennej rutyny. Dodatkowa korzyść: dbasz nie tylko o informację, ale też np. o finanse, bo lepiej chronisz swoje prywatne konto bankowe. Zmiany można wprowadzać stopniowo i wybierać rozwiązania adekwatne do potrzeb i możliwości. Wtedy okaże się, że nie jest to wcale takie trudne.

Ocena zagrożeń

Zastanów się, jakim zagrożeniom poddana jest posiadana przez Ciebie informacja, jak również informacja o Tobie. Przeanalizuj, w jaki sposób informacja może trafić w niepowołane ręce i jak zabezpieczyć się na wypadek, gdyby do tego doszło. Pomocne pytania diagnostyczne:

Gdzie znajduje się informacja? Kto ma do niej dostęp? Z jakich urządzeń korzystasz w ciągu dnia: komputera stacjonarnego, laptopa, tabletu, smartfona? Jak chronisz informację (fizycznie i cyfrowo)? Jak się łączysz z Internetem? Czy masz kopie informacji? Czy nie jest ich zbyt wiele? Czy są dobrze zabezpieczone?

Dostęp do wrażliwej informacji/wrażliwego kanału komunikacji przez niezabezpieczone sieci bezprzewodowe zwiększa zagrożenie utratą kontroli. Informację trudniej jest chronić na urządzeniach mobilnych. Posiadając kopie zapasowe, zmniejszasz ryzyko utraty informacji, ale jednocześnie zwiększasz ryzyko utraty kontroli nad nią.

Jak chronisz swoje konta? Czy przestrzegasz podstawowych zasad bezpieczeństwa?

Zaawansowane zabezpieczenia, np. szyfrowanie komunikacji, mają sens tylko wtedy, gdy równocześnie dbasz o podstawowe zasady bezpieczeństwa: zabezpieczasz silnymi hasłami komputer i usługi, z których korzystasz, aktualizujesz system operacyjny i wszystkie programy (aplikacje), fizycznie chronisz urządzenie.

Kto może uzyskać dostęp do Twojego urządzenia? Jaką stosujesz procedurę dzielenia się informacją z innymi osobami? Jak chronisz tożsamość swoją i informatorów?

Im więcej osób ma dostęp do informacji (przełożeni, rodzina, koledzy z redakcji), tym większe ryzyko, że ona wycieknie. Ale jednocześnie sytuacja, kiedy tylko Ty wiesz o wrażliwej informacji, może być niebezpieczna.

Czy w każdej sytuacji i z każdego urządzenia musisz mieć dostęp do wszystkich informacji?

Może dotyczy to tylko niektórych informacji? Korzyść z dostępu do danych z różnych urządzeń jest taka, że w przypadku zgubienia, zniszczenia czy kradzieży sprzętu nie tracisz bezpowrotnie informacji. Jednak jest wiele zagrożeń:

- większa liczba urządzeń z dostępem do informacji zwiększa ryzyko wycieku,
- telefony są powiązane z dostawcą usługi (operatorem komórkowym),
- informacje przechowywane na komputerze można lepiej zabezpieczyć niż te na telefonie czy tablecie (systemy operacyjne są lepiej przetestowane pod kątem różnych zagrożeń);
- małe, przenośne urządzenia są też bardziej podatne na fizyczne zagrożenia (kradzież, uszkodzenie, zgubienie).

Nie wszystkim zdarzeniom jesteś w stanie zapobiec, ale możesz przygotować się na ich ewentualne wystąpienie. Zastanów się:

Czy działasz zgodnie z prawem?

To podstawa. Jeśli łamiesz prawo, posiadana przez Ciebie informacja może trafić w ręce służb w związku z prowadzonym śledztwem i trudno będzie Ci jej bronić w oparciu o prawo ochrony tajemnicy dziennikarskiej.

Co się stanie, jeśli posiadane przeze Ciebie informacje lub informacje o Tobie trafią w niepowołane ręce?

Możesz zapobiec niektórym negatywnym konsekwencjom, np. ograniczając zakres informacji, jakie publikujesz, lub liczbę osób i urządzeń, które mają dostęp do wrażliwych informacji. Uważaj: informacja o korzystaniu przez Ciebie z jakiejś usługi czy aplikacji to też informacja o Tobie.

W jaki sposób chronisz posiadane przez siebie informacje?

Możesz utrudnić osobom nieuprawnionym dostęp do informacji, np. szyfrując je mocnym hasłem.

Jednak przede wszystkim – biegle opanuj możliwości ochrony informacji i komunikacji, zachowaj rozsądek i dobieraj środki ostrożności do konkretnej sytuacji.

Szczególne ryzyka związane z telefonem

Operator telekomunikacyjny – czyli sieć komórkowa – zbiera szereg informacji o aktywności użytkowników telefonów, w tym tzw. metadane. Są to **dane telekomunikacyjne**:

- dane abonenckie: m.in. imię, nazwisko, adres zamieszkania właściciela numeru;
- wykaz połączeń: informacja, z jakimi numerami, kiedy, jak często i jak długo się łączysz;
- dane geolokalizacyjne: informacja o tym, jak się przemieszczasz;

a jeśli korzystasz z telefonu z dostępem do Internetu, także **dane internetowe**, czyli:

- historia Twojej aktywności w sieci, np. strony, jakie odwiedzasz;
- metadane dotyczące komunikacji przez Internet, np. dotyczące adresatów wysłanych e-maili lub wiadomości przekazywanych przez popularne komunikatory.

Operator ma też dostęp do połączeń głosowych i SMS-ów. Ma kontrolę nad częścią ustawień telefonu (np. ma techniczną możliwość zmieniania ustawienia połączeń telefonicznych i internetowych, przechwytywania lub zmieniania telefonicznych połączeń głosowych i SMS-ów, monitorowania lub zmieniania połączeń internetowych przeprowadzanych poprzez operatora).

Prawo pozwala służbom na dostęp do danych telekomunikacyjnych i internetowych (z wyjątkiem treści komunikacji) bez kontroli sądu. Dane te pozwalają szczegółowo poznać codzienne rutyny użytkownika, ułatwiając np. odkrycie tożsamości informatorów.

Smartfon – w przeciwieństwie do klasycznego telefonu komórkowego – dostarcza też bardzo wielu informacji producentom aplikacji w nim zainstalowanych. To kolejny kanał, przez który mogą one dostać się w niepowołane ręce. Co więcej, telefony trudniej jest chronić przed złośliwym oprogramowaniem niż komputery, łatwiej też je utracić. Konkretne porady, jak zabezpieczyć telefon, znajdziesz w następnym rozdziale.

Szczególne ryzyka związane z przetwarzaniem danych w chmurze

Korzystanie z chmury ma swoje zalety:

- możesz dać dostęp do informacji innym osobom lub wraz z nimi pracować nad materiałem, od razu widząc rezultaty;

- może być się bezpieczniejsze, np. gdy podróżujesz i obawiasz się utraty danych lub przeszukania (dzięki chmurze nie nosisz wrażliwej informacji przy sobie).

Jednak w kontekście ochrony informacji, te cechy chmury zazwyczaj są raczej wadą niż zaletą:

- tracisz kontrolę nad tym, kto ma dostęp do informacji – udostępniasz ją właścicielom i administratorom chmury;
- właściciel/administrator chmury ma wgląd w Twoją sieć kontaktów – wie, kto zamieszcza i ściąga pliki.

W niektórych sytuacjach chmura może też utrudnić dostęp do informacji, np. w razie ograniczonego dostępu do Internetu lub awarii serwisu.

II. ABC BEZPIECZNEGO ZARZĄDZANIA INFORMACJĄ

Kilka mitów o bezpieczeństwie

Nie jestem dziennikarzem śledczym, więc nie ma powodu, by ktokolwiek chciał mieć dostęp do moich urządzeń i posiadanych przeze mnie informacji.

Każdy z nas posiada informacje, które powinien chronić. Nie muszą to być dane informatorów, a choćby informacje dotyczące sfery prywatnej, np. dotyczące konta w banku, zdrowia, bliskich, adres zamieszkania, termin planowanego urlopu. Wyciek takich informacji stanowi zagrożenie nie tylko dla życia prywatnego (kradzież czy próba wyłudzenia), ale też zawodowego, bo można wykorzystać je do szantażu czy ukraść dziennikarzowi temat.

Mój komputer jest bezpieczny, bo jest chroniony hasłem.

Ustawienie silnego hasła w komputerze jest punktem wyjścia do zadbania o bezpieczeństwo, bo utrudnia dostęp do informacji osobom niepowołanym. Ale nie jest to ochrona wystarczająca. Hasło można obejść, dostając się do dysku niezależnie od systemu operacyjnego (np. wymontować dysk i zajrzeć do niego lub zarazić komputer oprogramowaniem szpiegującym). Dlatego trzeba podjąć dodatkowe działania, opisane w dalszej części tego rozdziału.

Korzystanie z trybu incognito w przeglądarce zapewnia anonimowość.

Tryb incognito (tryb prywatny) zapobiega zapisywaniu historii odwiedzanych stron w przeglądarce oraz plików *cookie*. W rezultacie inna osoba korzystająca z tego samego urządzenia nie będzie widziała, jakie strony były odwiedzane. Tryb prywatny często używany jest do odwiedzania stron dla dorosłych (stąd potoczne określenie: „tryb porno"). Tryb incognito nie blokuje jednak przekazywania informacji o Twojej aktywności w sieci dostawcy usług internetowych, właścicielom stron, które odwiedzasz, ani administratorowi sieci (jeśli korzystasz z sieci firmowej, może zobaczyć je pracodawca). Korzystając z przeglądarek internetowych, zawsze zostawiasz po sobie ślad.

Informacja zamieszczona na prywatnym profilu na Facebooku jest prywatna.

Zamieszczając informację w sieci, tracisz nad nią kontrolę. Nawet jeśli przeczyta ją tylko jedna osoba, może ją skopiować i rozpowszechnić. Tak działa Internet. Wiele portali bynajmniej nie obiecuje prywatności, ale nie daj się oszukać tym, które to robią, np. Snapchatowi. Wiadomość znika z ekranu, ale nie z serwerów. A dzięki funkcji „zrzut ekranu" (*print screen*) odbiorca może ją

zachować na swoim urządzeniu na dłużej i rozpowszechnić. Jedyna recepta, by zachować kontrolę nad informacją, to jej nie przesyłać. To nie do zastosowania w 100%, ale warto się zastanowić, zanim wrzuci się do sieci informacje naprawdę wrażliwe. A jeśli już to robisz – zastosuj szyfrowanie „od końca do końca" (end-to-end encryption, np. szyfrowanie e-maila za pomocą PGP/GPG), zwiększając w ten sposób kontrolę nad tym, kto widzi jej treść. Ale uwaga – szyfrowanie nie ukrywa metadanych, czyli tego, kto z kim i kiedy się komunikuje.

Przechowywanie wrażliwej informacji w chmurze jest bezpieczne.

Do wszelkich informacji zgromadzonych w chmurze dostęp ma lub łatwo może uzyskać:

- dostawca wirtualnego serwera (chmury),
- organy państwa (policja, skarbówka, służby specjalne).

Firma dla własnych celów może te informacje analizować i przetwarzać (np. w celach marketingowych), a usunięcie danych z serwera najczęściej jest odwracalne (przynajmniej dla administratora). A zgodnie z regulaminem większości serwisów dane „usunięte" przez użytkowników nie znikają automatycznie z serwerów firmy i mogą być przechowywane jeszcze przez wiele miesięcy i udostępniane organom państwa np. w celu zwalczania nadużyć podatkowych czy rozstrzygania sporów cywilnych.

Dobre praktyki

Bezpieczny warsztat pracy

Bezpieczny warsztat pracy to przede wszystkim bezpieczna redakcja. Kluczowe zasady:

- oddzielenie pokoju spotkań od pokoju pracy, np. kolegia redakcyjne powinny być organizowane w odseparowanym pomieszczeniu, z zamykanymi oknami i drzwiami, żeby utrudnić podsłuchanie toczących się tam rozmów czy założenie urządzenia podsłuchowego; dostęp do tych miejsc powinny mieć tylko osoby zaufane;
- zamykanie serwerowni na klucz, który posiadają tylko uprawnione osoby; routery nie powinny znajdować się w miejscu ogólnodostępnym; zabezpieczenie kabli w sposób, który uniemożliwia podpięcie się do sieci osobom nieuprawnionym; niezabezpieczony, plączący się pod nogami kabel to również ryzyko spięcia – a więc zniszczenia sprzętu i utracenia danych;
- regularne sprawdzanie gniazdek (przełączników, listew...) pod względem tego, czy nie umieszczono w nich podsłuchu; zepsute gniazdko może też spowodować spięcie elektryczne, co niesie za sobą ryzyko zniszczenia sprzętu lub utraty danych;
- zabezpieczenie sieci bezprzewodowej mocnym i często zmienianym kluczem (hasłem) WPA/WPA2;
- jeden komputer – jeden użytkownik (należy unikać współdzielenia sprzętu);
- ograniczenie dostępu do wspólnego dysku; blokowanie dostępu do wszystkich zasobów po zakończeniu współpracy z daną osobą;
- przynajmniej jeden komputer w redakcji bez podłączenia do Internetu – może się przydać do odczytania informacji poufnych z nośników danych.

Powyższe zasady warto też zastosować w domu, jeśli jest to Twoje podstawowe miejsce pracy.

Zabezpieczenie urządzenia

Pracując z danymi wrażliwymi, upewnij się, że korzystasz z bezpiecznego urządzenia. Tego warunku nie spełnia urządzenie, które zostało zarekwirowane przez służby, a potem oddane. Lista

zasad, których należy przestrzegać, jest długa, ale wprowadzenie ich w życie nie powinno nastręczać większych trudności.

Ochrona fizyczna:

- wychodząc z pokoju, zabezpieczaj komputer hasłem; nie zostawiaj otwartej torebki (torby, teczki) ani nośników danych leżących na wierzchu;
- po pracy zabieraj laptopa ze sobą, nie zostawiaj go w redakcji, a komputer stacjonarny – wyłączaj;
- zamykaj szuflady biurka, szafki i pokój na klucz, nie zostawiaj klucza w drzwiach;
- w podróży unikaj zostawiania urządzenia w pokoju bez opieki – jeśli nie ma innego wyjścia, postaraj się stworzyć takie warunki, żeby wiadomo było, czy ktoś miał do niego dostęp.

Podstawowa ochrona cyfrowa:

- zabezpiecz urządzenie hasłem – hasło powinno być trudne do odgadnięcia, okresowo zmieniane i bezpieczne przechowywane; używaj różnych haseł do różnych usług – możesz skorzystać z programu do zarządzania hasłami (KeePassX);
- używaj aktualnego oprogramowania i programu antywirusowego; aktualizuj je; instaluj tylko oprogramowanie, któremu ufasz (i z zaufanego źródła) i które jest Ci niezbędne – niektóre programy zwiększają ryzyko, np. Java, Flash, Quick Time, czytnik PDF-ów; odinstaluj zbędne oprogramowanie;
- otwieraj załączniki do e-maili i wiadomości tekstowych tylko od znanych Ci i zaufanych nadawców (możesz też bezpiecznie otwierać je za pomocą specjalnego systemu operacyjnego, np. Qubes-OS.org, lub odpowiednio zabezpieczonej domyślnej przeglądarki, np. Firefox z wtyczką NoScript); czytaj nagłówki e-maili i adresy nadawców, żeby upewnić się, że pochodzą z zaufanego źródła;
- w miarę potrzeb i możliwości zastąp SMS-y bezpieczną aplikacją, np. Signal;
- zwróć uwagę na odpowiednią konfigurację systemu operacyjnego i oprogramowania; zmień domyślne ustawienia na takie, które będą lepiej chroniły Twoją prywatność, np. blokowanie śledzenia przez strony internetowe, czyszczenie ciasteczek w przeglądarce; w przeglądarce zainstaluj rozszerzenia (wtyczki, dodatki) blokujące ciasteczka, śledzenie i reklamy, które mogą być nośnikiem złośliwego oprogramowania (NoScript, HTTPS Everywhere, uBlock Orgin, Privacy Badger);
- regularnie rób kopie zapasowe, najlepiej w dwóch egzemplarzach – przechowuj je na nośnikach danych, z których jeden jest pod ręką, a drugi – ukryty poza zasięgiem (przechowywanie kopii zapasowej w chmurze może być ryzykowne);
- szyfruj dysk (najlepiej korzystać z narzędzia systemowego, np. w systemie Windows – BitLocker, Mac – FileVault, Linux – LUKS).

Bezpieczne gromadzenie i przechowywanie materiałów i dowodów

Informacje wrażliwe lub poufne powinny być przechowywane z zastosowaniem szczególnych środków bezpieczeństwa:

- zastosuj dodatkowe szyfrowanie (np. VeraCrypt);
- jeśli obawiasz się, że komputer może zostać zabrany, nie przechowuj wrażliwej informacji na jego dysku; użyj zaszyfrowanego nośnika danych (np. dysku zewnętrznego) i ukryj go (fizycznie) lub – w ostateczności – skorzystaj z niezależnie szyfrowanej chmury; zrób dodatkową kopię zapasową;

- zastanów się, czy potrzebujesz mieć dostęp do wszystkich informacji ze wszystkich urządzeń – ogranicz liczbę urządzeń, przez które masz dostęp do wrażliwych informacji;
- bardziej wrażliwe informacje przechowuj na dysku, a nie w chmurze, przy zachowaniu opisanych wyżej zasad bezpieczeństwa;
- ustal procedurę bezpiecznego kontaktu w nagłych przypadkach.

Bezpieczna poczta elektroniczna?

Poczta elektroniczna to jedno z najczęściej używanych narzędzi do komunikacji online. Czasem wręcz nadużywane – np. kiedy e-mailem (niezaszyfrowanym) przekazywane są informacje poufne czy wrażliwe. Żeby zwiększyć bezpieczeństwo komunikacji e-mailowej:

- unikaj wysyłania e-mailem bardzo wrażliwych informacji – wybierz inną, trudniejszą do skopiowania i upublicznienia formę; jeśli nie możesz przekazać informacji osobiście, wybierz szyfrowany czat, który nie zapisuje historii rozmowy (np. meet.jitsi.si);
- przestrzegaj zasad opisanych w punkcie dotyczącym zabezpieczenia urządzenia i innych punktach w tym przewodniku;
- wybierz serwer pocztowy, który najlepiej chroni Twoją komunikacje: zwróć uwagę, gdzie jest fizycznie zlokalizowany i gdzie zarejestrowany jest właściciel – jakiemu prawu podlega, jakie opcje zabezpieczenia oferuje (szyfrowanie połączenia, szyfrowanie od-końca-do-końca, dwustopniowa weryfikacja logowania, sprawdzanie aktywności na koncie itp.);
- sprawdź, czy można ufać administratorom i właścicielom serwera – jaka jest historia bezpieczeństwa i współpracy z rządami;
- używaj oddzielnych kont e-mail (ale też komunikatorów i telefonów) do komunikacji z różnymi grupami i w przypadku różnych tematów;
- świadomie zdecyduj, czy nazwa konta, opis, hasło i inne informacje związane z kontem powinny wskazywać na Ciebie;
- zabezpiecz konto silnym, unikalnym hasłem i dwustopniową weryfikacją logowania;
- rozważ używanie niezależnego szyfrowania od-końca-do-końca (PGP/GPG, np. przy pomocy Mailvelope lub Enigmail);
- rozważ używanie ustalonego systemu kodów dla wrażliwych informacji, takich jak nazwiska, adresy, daty itp. – uważnie analizuj to, co wysyłasz;
- kasuj niepotrzebne informacje – minimalizuj ilość przechowywanych informacji;
- używaj proxy (VPN lub Tor) do założenia konta i łączenia się z nim;
- jeśli musisz przesłać duży plik, który nie mieści się w poczcie elektronicznej, możesz użyć specjalnych narzędzi, np. share.riseup.net lub OnionShare.org.

Przechowywanie zaszyfrowanej informacji

Informacja zaszyfrowana jest trudniej dostępna dla osób postronnych bez wiedzy właściciela. Ale sam fakt zaszyfrowania informacji może spowodować wzrost zagrożenia, zwracając na nią i na Ciebie uwagę. W niektórych krajach i kontekstach szyfrowanie informacji automatycznie traktowane jest jako terroryzm (w Etiopii blogerzy z grupy Zone Nine Bloggers zostali aresztowani za szyfrowanie i używanie narzędzi chroniących informacje).

Jak bezpiecznie przechowywać zaszyfrowaną informację:

- szyfruj cały dysk urządzenia, również telefonu; stosuj narzędzia standardowe, dostępne w systemie operacyjnym Twojego urządzenia (np. w systemie Windows – BitLocker, Mac – FileVault, Linux – LUKS);

- informacje wrażliwe szyfruj dodatkowo (np. VeraCrypt) i przechowuj w bezpiecznym urządzeniu i miejscu;
- pamiętaj, że szyfrowanie jest tak silne jak hasło, którego używasz, i jak jakość wykorzystywanego narzędzia;
- pamiętaj, że w Polsce szyfrowanie jest legalne[1]. Szyfrując, nie narażasz się więc na problemy z prawem, a tylko utrudniasz osobom niepowołanym dostęp do posiadanej przez Ciebie informacji.

(Względnie) bezpieczna chmura

Żeby zmniejszyć zagrożenia opisane w części dotyczącej oceny ryzyka:

- zaszyfruj pliki, zanim wyślesz je na chmurę (np. cryptomator.org lub wspomniany VeraCrypt);
- wybierz rozwiązanie typu „zero knowledge", które nie daje właścicielowi chmury dostępu do przechowywanych na niej informacji (nie ma on możliwości odszyfrowania). Niektórych komercyjnych usług lepiej unikać, jeśli zależy Ci na bezpieczeństwie informacji, np. skompromitowanego licznymi włamaniami Dropboxa;
- używaj narzędzi zabezpieczających tożsamość (maskujących), np. VPN, Tor; nie rejestruj się na swoje imię/nazwisko/pseudonim, użyj oddzielnego, anonimowego e-maila;
- zabezpiecz sobie różne sposoby dostępu do chmury.

Zabezpieczenie telefonu

Telefon to narzędzie, które najmniej sprzyja bezpiecznemu zarządzaniu informacją. Rozważ zastąpienie komunikacji przez telefon bezpieczniejszą alternatywą: przynajmniej Skype'em, a lepiej – komunikatorem szyfrowanym, np. Signal, meet.jit.si. Korzystając z nich, łącz się z bezpieczną siecią (tego warunku nie spełnia otwarta, niezabezpieczona hasłem sieć Wi-Fi); użyj VPN lub Tor – a informacja będzie o wiele bezpieczniejsza. Jeśli jednak wybierzesz telefon, możesz ograniczyć ryzyko:

- nigdy nie zostawiaj telefonu bez opieki. Jeśli nie masz go z kim zostawić, a nie powinien Ci towarzyszyć, przed wyjściem wyłącz go, wyjmij baterię, włóż go do specjalnej torebki blokującej sygnał (tzw. klatka Faradaya, *Faraday signal blocking bag*) i umieść we wnętrzu torby, gdzie nie będą dochodziły do niego dźwięki;
- ustaw silne hasło, regularnie je zmieniaj;
- zaszyfruj dysk telefonu;
- aktualizuj system operacyjny i wszystkie aplikacje;
- wyłącz geolokalizację (GPS – tak w telefonie, jak i w aplikacjach), Bluetooth i Wi-Fi – włączaj je tylko, gdy są Ci niezbędne;
- unikaj przechowywania wrażliwych informacji na telefonie i przekazywania ich za jego pośrednictwem,
- używaj szyfrowanych kanałów informacji, np. Signal, do wiadomości tekstowych;
- nie zabieraj telefonu na spotkania z informatorami;
- jeśli posiadasz niezarejestrowany numer telefonu, nie noś go razem z zarejestrowanym;
- w telefonie instaluj tylko niezbędne aplikacje z zaufanych źródeł;
- czytaj regulaminy i ostrzeżenia, np. do jakich informacji dostęp będą miały instalowane przez Ciebie aplikacje; przejrzyj, do czego mają dostęp aplikacje fabryczne; jeśli możesz, powyłączaj je; kasuj niepotrzebne aplikacje.

[1] Stan na 24 stycznia 2017 r.

Bezpieczne dzielenie się informacją z innymi osobami

Dzieląc się z kimś daną informacją:

- zyskujesz dostęp do wiedzy i doświadczenia innych osób, np. do tego, jakie środki bezpieczeństwa podjąć, jak bezpiecznie się komunikować ze źródłem;
- w sytuacji niebezpieczeństwa (np. gdy podczas spotkania ze źródłem coś pójdzie nie tak) być może możesz liczyć na pomoc.

Wiąże się to jednak z dodatkowymi zagrożeniami:

- nawet jeśli Ty bezpiecznie zarządzasz informacją, nie możesz mieć pewności, że inne osoby robią to samo;
- im więcej osób jest w posiadaniu informacji, tym łatwiej o wyciek.

Jak zadbać o bezpieczeństwo:

- zanim podzielisz się informacją, przeanalizuj korzyści i potencjalne ryzyko;
- ustal procedurę zarządzania informacją, którą się dzielisz (także z informatorem);
- nie rozmawiaj o tym przy osobach postronnych.

Skuteczne pozbycie się informacji

Bezpieczne zarządzanie informacją to też pozbywanie się wszystkich informacji, które nie są Ci już potrzebne – szczególnie wrażliwych. Skasowanie informacji nie wystarcza. Żeby skutecznie się jej pozbyć:

- szyfruj cały dysk (komputera, telefonu, dysk zewnętrzny); jeśli chcesz zniszczyć dane przechowywane na przenośnym dysku – konieczne może być zniszczenie samego dysku;
- nie wyrzucaj w jednym miejscu kompletu dokumentów zniszczonych w niszczarce;
- wyczyść ślady w przeglądarce internetowej i aplikacjach: historię przeglądanych stron, pliki *cookie*, zbędne wtyczki.

III. OCHRONA DZIENNIKARSKICH ŹRÓDEŁ INFORMACJI[2]

Dlaczego trzeba chronić źródła?

Tajemnica dziennikarska jest nie tylko prawem dziennikarza, ale też jego obowiązkiem. Powstaje w chwili, gdy informator zastrzegł, że nie życzy sobie ujawniania swojej tożsamości. Poza ściśle określonymi przez prawo sytuacjami dziennikarze mają obowiązek zachować w tajemnicy wszelkie informacje, które mogłyby prowadzić do identyfikacji ich źródeł. Obowiązek ten dotyczy też innych osób zatrudnionych w redakcjach, wydawnictwach prasowych itp. (także pracowników technicznych) – niezależnie od tego, czy dostęp do informacji dotyczących źródła uzyskały w ramach pełnionych obowiązków służbowych, czy też trafiły one do nich przypadkiem.

Naruszenie tajemnicy zawodowej jest przestępstwem:

[2] Stan prawny na 24 stycznia 2017 r. Ochronie źródeł dziennikarskich poświęcony został przewodnik Helsińskiej Fundacji Praw Człowieka pt. „Wiem i powiem" (autorzy: Dorota Głowacka, Adam Ploszka, Marcin Sczaniecki, 2016, http://www.hfhr.pl/wp-content/uploads/2016/04/Wiem_i_powiem.pdf).

- zgodnie z art. 49 prawa prasowego naruszenie tajemnicy zawodowej przez dziennikarza lub innych depozytariuszy tajemnicy dziennikarskiej jest przestępstwem zagrożonym karą grzywny albo ograniczenia wolności;
- zgodnie z art. 266 Kodeksu karnego dotyczącym ujawnienia tajemnicy zawodowej dziennikarze oraz inni depozytariusze tajemnicy dziennikarskiej mogą podlegać odpowiedzialności karnej – mogą zostać ukarani grzywną, ograniczeniem wolności albo pozbawieniem wolności do lat 2.

Dziennikarz może być zwolniony z zachowania tajemnicy:

- za zgodą sądu, gdy informacja, materiał prasowy, list do redakcji lub inny materiał o tym charakterze dotyczy ciężkiego przestępstwa (określonego w art. 254 Kodeksu karnego, np. zabójstwa, pozbawienia człowieka wolności, ludobójstwa, przestępstwa o charakterze terrorystycznym) – zwolnienie z obowiązku zachowania tajemnicy nie może jednak dotyczyć danych umożliwiających identyfikację informatora;
- za zgodą informatora – na ujawnienie jego nazwiska lub samego materiału.

Sąd może nakazać ujawnienie tożsamości informatora bez jego zgody tylko w przypadku najcięższych przestępstw, jak ludobójstwo, zamach stanu, przestępstwo o charakterze terrorystycznym. W sprawach innych niż karne (cywilnych, administracyjnych, podatkowych, sądowo-administracyjnych) wyłącznie dysponent informacji, czyli samo źródło, może zwolnić dziennikarza z tajemnicy. Dla obowiązku zachowania tajemnicy dziennikarskiej nie ma znaczenia, jak informator wszedł w posiadanie informacji – legalnie czy nie.

Źródła trzeba chronić nie tylko z przyczyn prawnych, ale też ze względu na etykę dziennikarską. Jeśli informator Ci zaufa i przekaże poufne informacje, bierzesz odpowiedzialność za jego dalsze życie, dalszy los. To informator podejmuje decyzję o ujawnieniu informacji, ale często nie zdaje sobie sprawy z konsekwencji. Dlatego dziennikarz powinien mieć je na uwadze i chronić informatora. W ten sposób buduje też swoją wiarygodność na przyszłość.

Rodzaj sprawy / Zakres ochrony	**Informacja chroniona tajemnicą dziennikarską**	**Tożsamość źródła**
Sprawy inne niż karne (cywilne, administracyjne, podatkowe, sądowoadministracyjne)	Jest ujawniana tylko za zgodą źródła.	Jest ujawniana tylko za zgodą źródła.
Sprawy karne dot. ciężkich przestępstw (określonych w art. 254 kk)	Sąd może nakazać ujawnienie.	Jest ujawniana tylko za zgodą źródła.
Sprawny karne dot. najcięższych przestępstw (np. ludobójstwo, zamach stanu, przestępstwo o charakterze terrorystycznym)	Sąd może nakazać ujawnienie.	Sąd może nakazać ujawnienie.
Informacja przekazana dziennikarzowi dotyczy przestępstwa określonego w art. 240 kk	Zgodnie z art. 16 prawa prasowego dziennikarz ma obowiązek wyjawić informacje organom ścigania.	Zgodnie z art. 16 prawa prasowego dziennikarz ma obowiązek wyjawić tożsamość źródła organom ścigania.

Prawne wyłomy w tajemnicy dziennikarskiej

Polskie przepisy przyznają obecnie służbom dostęp do danych telekomunikacyjnych (np. o wykonywanych połączeniach i lokalizacji), internetowych (np. z portali społecznościowych, e-sklepów) i pocztowych bez większych ograniczeń, także jeśli chodzi o udostępnianie danych dotyczących dziennikarzy, mimo że powinny być one szczególnie chronione. Służby, w tym policja, ABW, CBA, Służba Celna i inne, mogą uzyskiwać dostęp do danych na różnych etapach postępowania, a czasem nawet bez konieczności wszczynania go. Mogą pobierać informacje dotyczące nie tylko samego dziennikarza, ale też szerokiego kręgu osób z jego otoczenia.

W wyniku częściowego wdrożenia wyroku Trybunału Konstytucyjnego (tzw. ustawą inwigilacyjną w lutym 2016 r.), który nakazał ograniczenie dostępu do danych telekomunikacyjnych i wprowadzenie gwarancji dla tajemnicy dziennikarskiej, dziennikarze zyskali dodatkową ochronę: jeśli materiały uzyskane w toku kontroli operacyjnej mogą zawierać m.in. informacje objęte tajemnicą dziennikarską, komendant przekazuje materiały do prokuratury, a ta – do sądu, który podejmuje decyzję o możliwości ich_wykorzystania (por. art. 19 ust. 15f ustawy o policji i analogiczne w innych ustawach kompetencyjnych).

Przepisy wprowadzone tzw. ustawą antyterrorystyczną w czerwcu 2016 r. umożliwiają jednak prowadzenie kontroli operacyjnej (np. zakładanie podsłuchów) wobec osób nieposiadających polskiego obywatelstwa bez konieczności uzyskania zgody sądu. Łatwo wyobrazić sobie nadużywanie tego uprawnienia w celu podsłuchania dziennikarza – chociażby „przy okazji" podsłuchiwania cudzoziemca.

Działania zmierzające do ustalenia tożsamości źródeł dziennikarskich w sposób niezależny od dziennikarza (np. przez analizę dokumentów, metadanych, podsłuch) są środkiem znacznie groźniejszym niż żądanie ujawnienia informatora bezpośrednio od dziennikarza. W takiej sytuacji dziennikarz nie ma kontroli nad ujawnieniem informacji, a zachowanie informacji i tożsamości źródła w tajemnicy przestaje być w jego gestii. Ta sytuacja może zniechęcać informatorów do przekazywania dziennikarzom ważnych informacji i ujawniania nieprawidłowości.

Dobre praktyki

- Ustal ze źródłem zasady: czy chce pozostać anonimowe, czy pozwala na cytowanie (chociażby pod pseudonimem). Mogą je zdradzić słowa, składnia, dlatego zachowanie anonimowości wymagałoby przeredagowania wypowiedzi.
- Ustal metody komunikacji, wyjaśnij zagrożenia związane z używaniem różnych narzędzi komunikacji (np. wykonane połączenie telefoniczne zostawia ślad w billingach; sama próba jego nawiązania zostawia ślad w pamięci telefonu). Narzędzia i metody komunikacji dobierz do sytuacji Twojej i źródła.
- Nie spotykaj się z informatorem/-ką w swoim lub jego/jej miejscu zamieszkania czy pracy ani w popularnych kawiarniach. Zwróć uwagę na obecne w otoczeniu kamery monitoringu. Nie przechowuj jego/jej wizytówki.
- Wyłącz geolokalizację w telefonie i innych urządzeniach i w aplikacjach (np. Facebook). To samo dotyczy Twojego źródła. Uwaga: jeśli robisz zdjęcia telefonem z włączoną geolokalizacją, informacja o Twoim położeniu zapisze się na zdjęciach.
- Pamiętaj o metadanych: jeśli umawiacie się na spotkanie przez telefon, dane o tym połączeniu mogą łatwo trafić w ręce organów państwa; nawet jeśli oboje wyłączycie geolokalizację w swoich urządzeniach, informacje o położeniu telefonu pozostają widoczne dla

operatora sieci telekomunikacyjnej, a tym samym mogą zostać udostępnione służbom lub wyciec. Na spotkanie nie zabierajcie smartfonów ani innych urządzeń podłączonych do Internetu.

- Nie włączaj swoich informatorów i bohaterów tematów, nad którymi pracujesz, do sieci znajomych i kontaktów w portalach społecznościowych. Analiza Twojej sieci powiązań może pozwolić na odkrycie tożsamości źródła.
- Poinformuj źródło, z kim będziesz się dzielić informacjami, i ostrzegaj je, kiedy to nastąpi.
- Stosuj zasady bezpiecznej komunikacji w sieci i zarządzania cyfrowym „ja" (więcej na ten temat poniżej).
- Działaj zgodnie z prawem: np. namawianie informatorów do ujawnienia informacji strzeżonych tajemnicą zawodową lub włamanie do systemu informatycznego w celu pozyskania takich informacji to przestępstwo, które może stać się przedmiotem śledztwa i sprowokować inwigilację lub przeszukanie całej redakcji.
- Analizuj ryzyko. Bądź przygotowany/-a na każdą ewentualność.

IV. ŚWIADOME ZARZĄDZANIE CYFROWYM „JA"

Zagrożenia

To, co publikujesz w Internecie, może mieć olbrzymie znaczenie nie tylko dla Twojej prywatności, ale i życia zawodowego, w tym dla możliwości zachowania tajemnicy zawodowej i fizycznego bezpieczeństwa: własnego oraz informatorów. W sieci nic nie ginie – aktualizacja statusu w mediach społecznościowych, nawet taka, do której dostęp mają (teoretycznie) tylko Twoi znajomi, szybko może stać się informacją publiczną. Zdjęcia często zdradzają więcej, niż tego chcesz, a to, co „lajkujesz" w Internecie, nie tylko buduje Twój profil jako użytkownika/-czki, ale może również naprowadzić na tematy, nad którymi pracujesz. Jeśli decydujesz się na aktywną obecność w mediach społecznościowych, świadomie zarządzaj swoim profilem.

Dobre praktyki

Korzystając z mediów społecznościowych i aplikacji, udostępniasz swoje dane prywatnym podmiotom. Żeby ograniczyć spektrum informacji, jakie wchodzą w ich posiadanie:

- Zapoznaj się z polityką prywatności. Sprawdź, do jakich danych uzyskują dostęp, co mogą z nimi zrobić, komu je przekazać. Łącz się tylko z zaufanymi serwisami.
- Zabezpieczaj swoje konta mocnymi hasłami. Jeśli to możliwe – włącz logowanie dwustopniowe; regularnie zmieniaj hasła i bezpiecznie je przechowuj.
- W ustawieniach swojego profilu sprawdź, kto będzie miał dostęp do zamieszczanych przez Ciebie informacji. Regularnie sprawdzaj ustawienia wszystkich aplikacji – dostawcy często je zmieniają i możesz przeoczyć powiadomienie.
- Jeśli na profilu w mediach społecznościowych umieszczasz informacje prywatne, ogranicz liczbę osób, które będą miały do nich dostęp; dziel znajomych na różne grupy z różnymi uprawnieniami (np. na Facebooku). Regularnie sprawdzaj listę znajomych. Usuwaj/ograniczaj te osoby, którym nie ufasz.

- Pamiętaj, że nawet jeśli publikujesz w trybie „dla znajomych”, istnieje ryzyko, że ktoś z Twojego kręgu przekaże informację dalej.
- Nie oznaczaj w mediach społecznościowych innych osób bez ich zgody. Ustal podobne zasady ze swoimi znajomymi w stosunku do Ciebie.
- Pamiętaj, by wyłączać usługi lokalizacji, zwłaszcza gdy pracujesz nad tematem w terenie. Usługi takie można wyłączać zarówno z poziomu urządzenia mobilnego, jak i aplikacji czy portali.
- Ostrożnie korzystaj z mediów społecznościowych w przestrzeni publicznej – wszechobecne kamery ułatwiają przeczytanie, co wstukujesz na klawiaturze Twojego urządzenia.
- Pamiętaj, że „lajkowanie” profili czy wpisów innych osób także składa się na Twój obraz – może pozwolić domyślić się, nad jakim tematem pracujesz, gdzie szukasz kontaktów. Jeśli akurat nie zależy Ci na budowaniu napięcia w mediach społecznościowych, powstrzymaj się od jakichkolwiek wpisów w związku z realizowanym tematem.
- W Twoich sieciach społecznościowych nie powinno być Twoich informatorów.
- W pracy dziennikarskiej unikaj korzystania z komunikatorów powiązanych z mediami społecznościami. Nie wysyłaj prywatnych wiadomości, zwłaszcza w tematach zawodowych – nie są one bezpieczne.

PODSUMOWANIE

Bądź na bieżąco

Technologie stale się rozwijają, co daje nowe możliwości, ale też rodzi nowe zagrożenia dla informacji. Raz wdrożone zasady bezpieczeństwa to dopiero początek. Żeby informacja w Twoich rękach była bezpieczna, rozwijaj się, czytaj, doszkalaj. W sieci znajdziesz dziesiątki poradników dotyczących konkretnych aplikacji i usług. Niewyczerpanym źródłem informacji jest Internet, a w nim blogi techniczne (np. Niebezpiecznik.pl). Chociaż nie warto podążać za każdą nowinką, dobrze jest poważnie traktować pojawiające się na nich ostrzeżenia: gdy trafisz na newsa o wycieku kilkudziesięciu tysięcy haseł do Twittera, nie zwlekaj ze zmianą hasła do swojego profilu na tym portalu.

POLECANE BLOGI I STRONY

Polskie

- Niebezpiecznik: https://niebezpiecznik.pl
- Sekurak: https://sekurak.pl
- Zaufana Trzecia Strona: https://zaufanatrzeciastrona.pl

Zagraniczne

- Digital First Aid Kit (Digital Defenders Partnership): https://www.digitaldefenders.org/digitalfirstaid

- Information Security for Journalists (The Centre for Investigative Journalism): http://www.tcij.org/resources/handbooks/infosec
- Journalist Security Guide (Committee to Protect Journalists): https://cpj.org/reports/2012/04/journalist-security-guide.php
- LevelUp (Digital protection training community): https://www.level-up.cc
- Safer Journo (Internews): https://saferjourno.internews.org
- Salama: Risk Assessment For Journalists and Bloggers: https://salama.io/#
- Security in-a-Box (Frontline Defender, Tactical Tech): https://securityinabox.org
- Surveillance Self-Defense (Electronic Frontier Foundation): https://ssd.eff.org

WOLNOŚĆ SIĘ LICZY!

Wspieraj działalność Fundacji Panoptykon, przekazując 1% swojego podatku (KRS: 0000327613).

Możesz też wspierać nas przez cały rok, przekazując darowizny na konto:
43 1440 1101 0000 0000 1044 6058

Więcej informacji: https://panoptykon.org/wspieraj-nasze-dzialania