PRAKTYCZNE WSKAZÓWKI RADY ADWOKATUR I STOWARZYSZEŃ PRAWNICZYCH EUROPY

w zakresie poprawy bezpieczeństwa teleinformatycznego prawników przed bezprawnym nadzorem

DANE KONTAKTOWE:

Council of Bars and Law Societies of Europe
Conseil des barreaux européens
Rada Adwokatur i Stowarzyszeń Prawniczych
Rue Joseph II, 40/8 1000 Brussels T +32 (0)2 234 65 10

Obserwuj nas na:
www.ccbe.eu
ccbe@ccbe.eu

SPIS TREŚCI

1 WPROWADZENIE

Wymóg zachowania poufności przez prawników w odniesieniu do komunikacji z klientami oraz informacji otrzymanych od klientów i przekazanych im porad (czy to zapisany jako obowiązek zachowania tajemnicy zawodowej czy tajemnicy adwokackiej/radcowskiej) stanowi zasadniczy element praworządności w wolnym i demokratycznym społeczeństwie. Jednakże jest to wartość, która okazuje się być coraz to bardziej zagrożona czy to w wyniku bezprawnej ingerencji osób trzech czy też – w niektórych sytuacjach – wskutek nieodpowiednio uregulowanego nadzoru rządowego.

Zwłaszcza gdy chodzi o nadzór ze strony organów rządowych, w maju 2016 r. Rada Adwokatur i Stowarzyszeń Prawniczych Europy (dalej: Rada) opublikowała Rekomendacje dotyczące zachowania poufności w relacjach z klientem w kontekście działań w dziedzinie nadzoru w celu poinformowania ustawodawców i decydentów o standardach, które powinny zostać wdrożone i które powinny być stosowane aby zapewnić, że zasady tajemnicy zawodowej i tajemnicy adwokackiej/radcowskiej nie są naruszane poprzez działania podejmowane przez państwo, które obejmują kontrolę komunikacji i dostęp do danych prawników do celów nadzoru i egzekwowania przepisów prawa.[1]

Rada zdaje sobie jednakże sprawę z faktu, że istnieje niebezpieczeństwo, że w niektórych jurysdykcjach kontrole regulacyjne dotyczące nadzoru rządowego mogą nie być w pełni adekwatne oraz, że zawsze występuje niebezpieczeństwo nieupoważnionej lub bezprawnej kontroli przez osoby trzecie. Stosownie, ten dokument zawiera praktyczne wskazówki dla europejskich samorządów i stowarzyszeń prawniczych w zakresie działań jakie poszczególni prawnicy i kancelarie prawne mogą podjąć w celu zapewnienia właściwej ochrony materiałów objętych tajemnicą adwokacką/radcowską, tajemnicą zawodową czy stosownym obowiązkiem ochrony danych.

Praktyczne wskazówki zostały opracowane dla samorządów prawniczych i stowarzyszeń prawniczych należących do Rady; organizacje te zachęca się do rozważenia potrzeby uwzględnienia przedstawionych tu porad (stosownie do uwarunkowań panujących w ich jurysdykcjach) we wskazówkach przekazywanych ich członkom.

Dokument został podzielony na dwie części. W pierwszej omówiono kwestie ogólne dotyczące podejścia prawników do kwestii bezpieczeństwa teleinformatycznego (bezpieczeństwa IT). Druga część zawiera bardziej szczegółowe wskazówki dotyczące środków technicznych, jakie prawnicy mogą zastosować do ochrony przez bezprawnym nadzorem i innymi naruszeniami systemów informatycznych.

[1] http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20160428_CCBE_recommendations_on_the_protection_of_client_confidentiality_within_the_context_of_surveillance_activities.pdf

2 KWESTIE OGÓLNE. W JAKI SPOSÓB MOŻNA POPRAWIĆ POZIOM BEZPIECZEŃSTWA TELEINFORMATYCZNEGO PRAWNIKÓW

1. Zapewnienie poufności stanowi fundamentalną zasadę zawodu prawniczego

"Karta Podstawowych Zasad Prawnika Europejskiego"[2] stanowi, że zachowanie poufności w odniesieniu do spraw klienta i poszanowanie tajemnicy zawodowej to obowiązek prawnika. Zachowanie poufności stanowi zarówno obowiązek prawnika jak i podstawowe prawo człowieka – klienta, które powinno być przez wszystkich respektowane.

Zakres w jakim poszczególne kraje przyjęły ramy regulacyjne gwarantujące poszanowanie tej zasady jest różny a w wielu jurysdykcjach nadzór rządowy może stanowić potencjalne zagrożenie dla zachowania tej zasady.

W swoim raporcie z 2014 r. „Krajobraz zagrożeń" (ang. *Threat Landscape*) Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ang. *European Union Agency for Network and Information Security („ENISA")*) podkreśliła, że „*przypadki naruszenia prywatności, ujawniane w publikacjach prasowych poświęconych praktykom inwigilacji, osłabiły zaufanie użytkowników do internetu*".[3] Ponadto Rezolucja Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych zawiera we wnioskach stwierdzenie, że „*podstawowe znaczenie ma zagwarantowanie ochrony tajemnicy zawodowej prawników [...] przed działaniami w dziedzinie nadzoru na masową skalę*" oraz że „*wszelka niepewność co do poufności komunikacji pomiędzy prawnikami a ich klientami może negatywnie odbić się na prawie obywateli UE do dostępu do porady prawnej, a także dostępu do wymiaru sprawiedliwości oraz prawie do rzetelnego procesu sądowego*."[4]

Z tych samych powodów, od roku 2013 Rada stale dzieliła się swoimi obawami, że takie praktyki naruszają nie tylko fundamentalną wartość zawodów prawniczych, ale także zaufanie do praworządności, przedstawiając w końcu wszystkie swoje uwagi w dokumencie opublikowanym w maju 2016 r. Rekomendacje dotyczące zachowania poufności w relacjach z klientem w kontekście działań w dziedzinie nadzoru. Niezależnie od istnienia ryzyka zarówno nadzoru rządowego, jak i bezprawnego dostępu osób trzecich od systemów informatycznych i danych, prawnicy nie są w stanie wykonywać swojego zawodu bez korzystania z systemów informatycznych, w tym bez korzystania z wiadomości elektronicznych (email) czy ogólnie internetu. W rzeczywistości, ponieważ stopień korzystania z internetu i rozwiązań przetwarzania w chmurze przez klientów stale rośnie, prawnicy mogą znaleźć się pod silną presją ze strony klientów, aby sami korzystali z takich systemów.

[2] http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_CoC/EN_DEON_CoC.pdf
[3] https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014
[4] http://www.eurooarl.eurooa.eu/sides/getDoc:.do?tvoe=TA&language=EN&reference=P7-TA-2014-0230

Kodeks postępowania prawników europejskich określa obowiązki prawników w zakresie zachowania poufności informacji. Jednocześnie Kodeks wymaga, aby prawnicy posiadali i rozwijali swoją wiedzę zawodową i umiejętności.[5]

Wymogi te wskazują na coraz większą konieczność nabywania przez prawników tych umiejętności, które mogą okazać się konieczne do zapewnienia ochrony poufności informacji dot. klienta w środowisku wirtualnym.

Stosownie, te Praktyczne wskazówki mają na celu wskazanie samorządom prawniczych i stowarzyszeniom prawniczym działania, które można podjąć w celu poprawy bezpieczeństwa teleinformatycznego prawników poprzez poinformowanie ich członków (w tym zwłaszcza prawników prowadzących jednoosobową działalność gospodarczą i małych kancelarii prawnych, które mogą nie mieć dostępu do tej samej wiedzy technicznej jaką dysponują większe kancelarie) o niektórych dostępnych dla nich opcji. Nie jest celem tego dokumentu omówienie technicznego zastosowania określonych narzędzi, ani przedstawienie szczegółowych rekomendacji z zakresu infrastruktury czy produktów informatycznych, w które samorządy prawnicze, stowarzyszenia prawnicze i prawnicy mogą zainwestować.

2. Znajomość podstaw bezpieczeństwa teleinformatycznego

Zainwestowanie w systemy bezpieczeństwa teleinformatycznego, narzędzia ochrony i narzędzia szyfrowania może okazać się konieczne dla prawników, ale nie jest to działanie wystarczające, gdy prawnik nie dysponuje dobrą wiedzą operacyjną na temat środowiska, w którym te narzędzia są posadowione. Przykładowo, nie ma sensu stosować narzędzi szyfrowania, jeżeli atakujący przejął kontrolę nad punktem końcowym, gdzie realizowane jest deszyfrowanie i gdzie informacje są przechowywane w niezaszyfrowanej formie.

Stąd, pewien poziom minimalnej wiedzy z dziedziny bezpieczeństwa teleinformatycznego stanowi ważną podstawową umiejętność każdego prawnika korzystającego z systemów informatycznych lub bazującego na nich. Nawet jeżeli prawnik zdecyduje się przekazać lub podzlecić ekspertom technicznym wprowadzenie określonych środków w celu zapewnienia bezpieczeństwa teleinformatycznego na poziomie ogólnym lub szczególnie w odniesieniu do poufności, zarządzanie świadczoną obsługą prawną w dalszym ciągu wymaga posiadania minimalnego poziomu wiedzy i kompetencji w tym zakresie. W przeciwnym razie, wykonując swoje czynności zawodowe, prawnicy mogą zostać osobiście pociągnięci do odpowiedzialności za nieposiadanie mechanizmów kontrolnych z obszaru bezpieczeństwa teleinformatycznego, w taki sam sposób w jaki zostaliby pociągnięci do odpowiedzialności za brak wewnętrznych mechanizmów kontrolnych w zakresie zarządzania środkami lub dokumentami klientów.

Stąd, przed rozważeniem środków technicznych, należy podkreślić potrzebę zapewnienia minimalnej wiedzy z dziedziny bezpieczeństwa teleinformatycznego, którą dysponowaliby wszyscy prawnicy.

[5] Zob. Kodeks postępowania dla prawników europejskich pkt. 2.3.2, 2.3.4 i 5.8.

3. Korzystanie ze wspólnych doświadczeń

Obowiązki nałożone na prawników w zakresie bezpieczeństwa teleinformatycznego przez przepisy unijne są ogólne i są zazwyczaj umiejscawiane w określonym kontekście ochrony danych, np. wymogi art. 17 Dyrektywy w sprawie ochrony danych 95/46/EU. Nie przewiduje się, aby Rozporządzenie w sprawie swobodnego przepływu danych czy projekt Dyrektywy w sprawie bezpieczeństwa sieci i informacji zmieniły to podejście ustawodawcy w bliskiej przyszłości. Stosownie, żadne formalne wymogi prawne nie przewidują technicznej realizacji przewidzianych prawem standardów z zakresu ochrony danych; realizacji tej należy szukać gdzieindziej, np. w uznanych praktykach sektorowych i standardach formalnych.

Zasypanie prawników szczegółami określonych rozwiązań informatycznych nie jest jednak celem tego dokumentu. Rada zdaje sobie sprawę z faktu, że ze względu na dużą różnorodność stosowanych systemów informatycznych i narzędzi, omawianie w tym materiale szczegółów technicznych nie ma sensu.

Raczej, w tym dokumencie wychodzi się od szerszej propozycji, że właściwym punktem wyjścia jest przyjęcie ogólnego podejścia do bezpieczeństwa teleinformatycznego stosowanego przez inne zawody i branże, w ramach którego przyjmuje się – na ile to możliwe – uznane standardy już stosowane w obszarze bezpieczeństwa informatycznego. Oprócz sensowności takiego działania per se, stanowi ono dla prawników także dodatkową korzyść – prawnik może wykazać, że stosuje standardy, które już są stosowane w innych sektorach, co zazwyczaj zwiększa zaufanie klientów gdy chodzi o ochronę poufności danych klienta i komunikacji.

Ponadto takie działanie a) pomaga klientom w porównaniu ich poziomu bezpieczeństwa teleinformatycznego i tego zapewnianego przez inne zawody i branże i b) ułatwia wykorzystanie doświadczeń, polityk i stosownych szczegółów technicznych (mechanizmów kontrolnych) już stosowanych w innych sektorach.

Stosownie samorządy prawnicze i stowarzyszenia prawnicze powinny wspierać prawników w uzyskaniu dobrego zrozumienia przydatności odpowiednich standardów bezpieczeństwa teleinformatycznego bez konieczności zobowiązywania wszystkich prawników do certyfikacji z zakresu tych standardów. W rzeczywistości, jako że standardy bezpieczeństwa teleinformatycznego są formułowane na tak wysokim poziomie, że tylko doświadczeni specjaliści z obszaru bezpieczeństwa teleinformatycznego są w stanie je bezpośrednio stosować (a niejednokrotnie pracownicy IT zatrudnieni przez kancelarie prawne mogą nie posiadać wymaganej wiedzy), w celu podniesienia świadomości z zakresu standardów wśród prawników nie jest wymaganie od nich uzyskanie certyfikacji z zakresu tych standardów, ale raczej zapewnienie im wglądu w pewne usystematyzowane i ustrukturyzowane podejście, które może zostać przyjęte.

Ponadto, bazując na minimalnych wymogach określonych w części drugiej tych Praktycznych wskazówek, samorządom prawniczym i stowarzyszeniom prawniczym zaleca się:

- przeanalizowanie na odpowiednim poziomie szczegółowości obecnego stanu przygotowania prawników w ich jurysdykcji w obszarze bezpieczeństwa teleinformatycznego;
- tam gdzie to właściwe, wydanie rekomendacji dla swoich członków, które stanowić będą tłumaczenie, przeniesienie, a tam gdzie to konieczne, lokalizację wymogów określonych w tym dokumencie i stosownych standardów bezpieczeństwa teleinformatycznego;

- opublikowanie stosownych standardów i wyjaśnienie ich członkom;
- zapewnienie, że wydawane przez nie rekomendacje i wytyczne są zgodne ze stosownymi standardami bezpieczeństwa teleinformatycznego;
- dążenie do zapewnienia zachowania przez ich członków zgodności z takimi rekomendacjami i wytycznymi.

Niektóre samorządy prawnicze już ustosunkowały się do jednej lub kilku kwestii wskazanych powyżej[6], przeprowadziły szkolenia z tej tematyki[7] lub wydały stosowne publikacje. Materiały takie stanowią praktyczny punkt wyjścia lub odniesienie dla innych samorządów prawniczych i stowarzyszeń prawniczych w Europie.

Podkreśla się, że kroki podejmowane w tej dziedzinie są nie tylko z korzyścią dla poszczególnych prawników, ale co ważniejsze dla ich klientów. Dlatego, w sytuacji gdy samorządy prawnicze i stowarzyszenia prawnicze publikują takie wytyczne dla swoich członków, powinny one także rozważyć czy nie dobrze byłoby poinformować także opinię publiczną i klientów o wytycznych i rekomendacjach; informując o istnieniu takich wytycznych samorządy prawnicze i stowarzyszenia prawnicze mogą uświadomić klientom, że prawnicy w dalszym ciągu poważnie podchodzą do kwestii ochrony poufnych informacji klienta niezależnie od kanału wykorzystywanego w komunikacji.

[6] Np. Conseil National des Barreaux, http://cnb.avocat.fr/Securite-de-l-information-au-sein-des-cabinets-deux-guides-mis-a-disposition-de-_la-Profession_a1191.html, practice notes from the Law Society of England and Wales e.g. at [praktyczne uwagi Stowarzyszenia Prawników Anglii I Walii np. na stronie] http://www.lawsociety.org.uk/support-services/_advice/practice-notes/information-security/, or the Hungarian Bar Association at [lub Stowarzyszenia Węgierskiego na stronie] http://www.magyarugyvedikamara.hu/common/file-servlet/_document/898/default/doc_url/160113_Utmutato_IT_biztonsaghoz_kamarai1096398_1.pdf

[7] Np. Poradnik dot. cyberbezpieczeństwa (ang. *Cyber Security Toolkit) Petera Wrighta, wydany przez Law Society Publishing*), lub Przewodnik po cyberbezpieczeństwie ABA; Pomoc dla prawników, kancelarii prawnych i innych zawodów prawniczych (ang. *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms and Business Professionals*).

3 ŚRODKI TECHNICZNE ZABEZPIECZAJĄCE PRZED NIEUPRAWNIONYM NADZOREM

1. Przegląd obowiązujących norm i standardów bezpieczeństwa teleinformatycznego

Istnieje wiele różnych globalnych standardów bezpieczeństwa teleinformatycznego. Niektóre z nich są dobrze znane, ale nie zapewniają odpowiednich ram, za pomocą których osoby wykonujące wolne zawody np. prawnicy mogliby skutecznie zapewnić wysoki poziom bezpieczeństwa teleinformatycznego. Na przykład, dobrze znana norma *Common Criteria (CC)* dotyczy zdefiniowania profili ochrony dla poszczególnych kategorii stosowania np. dla szyfrowania pamięci USB, bankomatów, aplikacji generujących podpisy elektroniczne itd. A poza profilami ochrony także oceny czy określone poszczególne produkty i systemy („obiekty bezpieczeństwa") (ang. *security targets*) spełniają takie profile. Toteż, chodzi tu raczej o zapewnienie, że dany produkt lub system spełnia uprzednio zdefiniowane konkretne wymagania, takie jak ogólne bezpieczeństwo teleinformatyczne produktów przeznaczonych do celów komercyjnych. Z tego powodu norma ta choć może wydawać interesująca dla prawników gdy chodzi o sprzęt i produkty związane z ogólnym bezpieczeństwem (pamięci USB, karty inteligentne, firewalle itd.), z których prawnik może korzystać, należy zdawać sobie sprawę z faktu, że nie zapewnia ona odpowiedniego wzorca odniesienia dla kwestii poruszanych w tym dokumencie.

Innym szeroko stosowanym standardem globalnym jest standard *COBIT* (*Control Objectives for Information and Related Technology* (Cele kontroli dla informacji i powiązanych technologii)). Standard ten ma obecnie bardzo szeroki zakres i stanowi ramy nadzoru i zarządzania dla infrastruktury informatycznej przedsiębiorstwa, w tym zarządzania bezpieczeństwem teleinformatycznym. Mając na uwadze zakres standardu, wydaje się on być odpowiedni tylko dla organizacji, które posiadają skomplikowaną infrastrukturę informatyczną i które są w stanie przyjąć ten standard jako holistyczne podejście do obszaru IT i przełożyć wymagania biznesowe na wymagania IT lub zapewnić utrzymywanie kontroli zarządczej nad funkcjami IT. Standard ten koncentruje się jednak na innych kwestiach, niż te z którymi boryka się większość prawników i małych kancelarii.

Toteż, zobaczymy, że z małej liczby globalnych rodzin standardów bezpieczeństwa teleinformatycznego tylko dwie mają zastosowanie do zarządzania ryzykiem naruszenia bezpieczeństwa teleinformatycznego, mianowicie:

(a) *FIPS 800-53* i *FIPS Cybersecurity Framework (and related standards)* (Ramy bezpieczeństwa cybernetycznego) (i powiązane standardy) NIST (Narodowego Instytutu Standardów i Technologii)[8];

(b) Standardy oparte na normie ISO 27000.

Druga część tego dokumentu służy sformułowaniu bardziej szczegółowych rekomendacji na podstawie tych norm i standardów. W szczególności, w sekcji 7 przedstawiono bardziej szczegółowy przykład podejścia do jednego szczególnego aspektu ryzyka, mianowicie do poufności komunikacji pomiędzy klientem i prawnikiem.

[8] FIPS Cybersecurity Framework. FIPS 800*53: Specjalna publikacja NIST 800-53 wersja 4, kwiecień 2013 r., Mechanizmy kontroli bezpieczeństwa i prywatności dla federalnych systemów informatycznych i organizacji (ang. *NIST Special Publication 800*53 Revision 4, April 2013, Security and Privacy Controls for Federal Information Systems and Organization*s).

a) *Standardy NIST*

Standardy opublikowane przez Narodowy Instytut Standardów i Technologii USA (NIST) są lepiej dostępne i mogą stanowić punkt wyjścia do przyszłych dyskusji na temat ram bezpieczeństwa teleinformatycznego dla prawników. Standard Specjalna publikacja NIST 80053 (Mechanizmy kontroli bezpieczeństwa i prywatności dla federalnych systemów informatycznych i organizacji (ang. *NIST Special Publication 80053 (Security and Privacy Controls for Federal Information Systems and Organizations*) obejmuje ogólne mechanizmy z obszaru bezpieczeństwa dla federalnych systemów informatycznych. Jest to bardzo szczegółowy, dobrze znany i szeroko stosowany standard, który może jednak okazać się zbyt szczegółowy, gdy spojrzy się na niego z perspektywy rozmiaru przeciętnej europejskiej kancelarii prawnej. Także ocena zgodności ze standardem może okazać się trudnym zadaniem dla takich kancelarii w kontekście europejskim. Inne, bardziej ogólne i zwięzłe ramy amerykańskie zapewnia dokument *FIPS*[9] *Cybersecurity Framework (and related standards)*[10] (Ramy bezpieczeństwa cybernetycznego) (i powiązane standardy) (także opublikowany przez NIST), który jest bardziej odpowiedni do stosowania przez mniejsze organizacje takie jak typowa kancelaria prawna. Fakt, że opublikowano także projekt wskazówek dla małych firm[11] stanowi tu dodatkową korzyść.

b) *Normy ISO*

Ostatnia, ale nie mniej ważna kwestia: istnieje ekwiwalent ISO dla wdrożenia standardów zarządzania bezpieczeństwem teleinformatycznym – standardy oparte na normie ISO 27000, które obejmują standardy, w oparciu o które organizacje otrzymują certyfikacje takie jak ISO 9001. Tu także opublikowane zostały szczegółowe wytyczne techniczne takie jak ISO 27002 oraz liczne wytyczne dla mniejszych firm[12].

Rodziny standardów wskazane powyżej mają takie same założenia, ale różnią się od siebie poziomem szczegółowości, są kierowane do różnych odbiorców a zgodność z nimi jest wykazywana w różny sposób.

Oczywiście istnieje o wiele więcej standardów bezpieczeństwa teleinformatycznego, niż te wymienione powyżej, obejmujących swoim zakresem szerszy obszar. Jednakże większość z tych standardów bezpieczeństwa teleinformatycznego wpisuje się w jedne ze wskazanych powyżej ram, obejmując swoim zakresem konkretny aspekt bardziej ogólnej struktury IT.

2. Działania niezbędne do zapewnienia skutecznego systemu bezpieczeństwa

W celu zbudowania podstawowego systemu bezpieczeństwa informacji, kancelaria prawna lub prawnik prowadzący jednoosobową działalność gospodarczą powinni rozpocząć – mając na uwadze dziedzinę prawa, w której kancelaria się specjalizuje, jej typowych klientów i umiejętności jej pracowników – od podjęcia następujących działań:

- zidentyfikować kluczowe zasoby informacji, w szczególności informacje i dokumenty klienta, kluczowe usługi i rejestry/zbiory, które mają krytyczne znaczenie dla prowadzenia działalności;

---

[9] FIPS to skrót od „*Federal Information Processing Standards*" („Federalne standardy przetwarzania informacji").
[10] http://www.nist.gov/cvberframework/upload/cvbersecuritv-framework-021214.pdf
[11] Publikacja NIST: Bezpieczeństwo informacji w małych firmach: Podstawy (ang. *NIST Small Business Information Security: The Fundamentals*, http://csrc.nist.gov/publications/drafts/nistir7621-r1/nistir_7621_r1_draft.pdf.)
[12] Zob. np. „ISO/IEC 27001 dla małych firm: Praktyczne wskazówki" opublikowane przez Edward Humphreys, ISO, w 2010 r. (ang. "*ISO/IEC 27001 for Small Businesses: Practical Advice" by Edward Humphreys, published by ISO in 2010*.)

- po identyfikacji tych kluczowych zasobów, kancelaria prawna powinna zidentyfikować także braki w zakresie bezpieczeństwa, które miałyby największe konsekwencje dla działalności kancelarii (uwzględniając także prawdopodobieństwo wystąpienia takich braków w zakresie bezpieczeństwa i konsekwencje w sytuacji ich wystąpienia) oraz zidentyfikować możliwości kancelarii w zakresie zminimalizowania tego ryzyka.

Zaleta opierania oceny na standardach bezpieczeństwa teleinformatycznego uwidacznia się w trakcie analizowania możliwych podejść do ryzyka, sposobu uwzględnienia danego podejścia i kategorii, od których należy rozpocząć cały proces. Opcje te powinny uwzględniać przynajmniej następujące aspekty:

- kontrolowanie dostępu do kluczowych zasobów informacji (w tym identyfikacja użytkowników systemów informatycznych i przyznawanie im tylko koniecznych praw dostępu);
- definiowanie obszarów bezpieczeństwa fizycznego i mechanizmów kontrolnych;
- bezpieczne usuwanie i wycofywanie sprzętu (w tym urządzeń mobilnych i niemobilnych nośników danych) oraz bezpieczeństwo sprzętu poza siedzibą;
- bezpieczeństwo sieci (zwłaszcza stosowanie dzielonych infrastruktur takich jak sieci bezprzewodowe i kablowe);
- procedury operacyjne w celu zapewnienia ochrony przed złośliwymi kodami;
- zarządzanie hasłami, kopie zapasowe, zgłaszanie incydentów w obszarze bezpieczeństwa itd.[13]

Działania opisane w sekcji 7 zapewniają bardziej szczegółowy przykład podejścia do jednego szczególnego aspektu ryzyka, mianowicie do poufności komunikacji pomiędzy klientem i prawnikiem.

3. Mechanizmy kontrolne z obszaru bezpieczeństwa teleinformatycznego dla urządzeń mobilnych (zob. mechanizm kontrolny 6.2.1 – norma ISO 27001).

Szczególny aspekt analizy ryzyka wskazanej powyżej stanowi konkretne ryzyko towarzyszące korzystaniu z urządzeń mobilnych.

Urządzenia mobilne np. laptopy, tablety czy telefony komórkowe są narażone na różne rodzaje ryzyka i powiązaną z nimi utratę kontroli nad samym zasobem. Narzędzia te są stosowane poza dobrze kontrolowanym środowiskiem biura. Stąd są one narażone na podwyższone ryzyko utraty, uszkodzenia czy naruszenia ich samych lub też zapisanych na nich informacji. Jeżeli osoba mająca złe zamiary uzyska dostęp do któregoś z tych urządzeń będzie w stanie przeprowadzić wiele ataków w obszarze bezpieczeństwa.

Urządzenia mobilne wymagają większej liczby mechanizmów kontrolnych z obszaru bezpieczeństwa niż urządzenia przechowywane w biurze. Absolutnie konieczne jest szyfrowanie pamięci masowej w środowisku komputerów, jednakże dla laptopów jest to działanie zdecydowanie wymagane. W przypadku braku odpowiednich i skutecznych zabezpieczeń, w prosty sposób, za pomocą podstawowych narzędzi, można uzyskać dostęp do nośnika danych urządzenia mobilnego niezależnie od siły hasła użytkownika. Toteż, chociaż bezpieczne hasło może chronić zasoby dostępne poprzez sieć, dane na przenośnym nośniku są skutecznie chronione tylko wtedy gdy są zaszyfrowane. Dotyczy to

[13] Podejście do tego ryzyka obejmuje listę „Guidedesecuritederinformationpourlesavocats" lub document NIST: Bezpieczeństwo informacji w małych firmach: Podstawy. (ang. *NIST Small Business Information Security: The Fundamentals*) na stronie http://csrc.nist.gov/publications/drafts/nistir7621-r1/nistir 7621 r1 draft.pdf. and of course, the longer lists in ISO 27002 and NIST FIPS 800-53.

wszystkich urządzeń mobilnych, w tym telefonów komórkowych, pamięci USB i oczywiście laptopów. Szyfrowanie z kontrolą dostępu jest szeroko dostępne dla wszystkich urządzeń i zazwyczaj jest oferowane w przystępnej cenie.

Ponadto, mając na uwadze ryzyko kradzieży urządzenia konieczne może okazać się wprowadzenie dodatkowych zabezpieczeń, np. zastosowanie miniaturowego zamka zabezpieczającego, z którego można skorzystać do ochrony laptopów przed kradzieżą (kradzież typu „złap i uciekaj") oraz podstawowych środków bezpieczeństwa takich jak pakowanie urządzeń mobilnych raczej do bagażu podręcznego niż do rejestrowanego.

Poza fizyczną ochroną takich urządzeń, prawnicy powinni także zwracać uwagę na zasoby sieciowe, które wykorzystują do podłączania swoich urządzeń zdalnych lub lokalizacji przechowywania danych. Smartphony i tablety mogą stanowić szczególne ryzyko, ponieważ użytkownicy stosują tutaj raczej mniej zabezpieczeń niż gdy chodzi o laptopy, mimo że ryzyko jest podobne. Należy zauważyć, że na urządzeniach mobilnych można zainstalować oprogramowanie antywirusowe, firewalle oraz zabezpieczenia przed szkodliwymi stronami (oraz, jak wspomniano powyżej, można też szyfrować zapisywane na nich dane). Jednakże, w chwili zakupu urządzenia mobilne nie posiadają zazwyczaj takiego oprogramowania, stąd użytkownik musi zaplanować w budżecie zakup takiego oprogramowania wraz licencją oraz sam je zainstalować i skonfigurować.

4. Mechanizmy kontrolne z obszaru bezpieczeństwa teleinformatycznego chroniące przed złośliwym oprogramowaniem (zob. mechanizm kontrolny 12.2.1 – norma ISO 27001).

Złośliwe oprogramowanie ma różne formy: wirusy, robaki, konie trojańskie, oprogramowanie typu *backdoor*, narzędzia hackerskie typu *rootkit*. Dokładna kategoryzacja rodzaju złośliwego oprogramowania nie jest ważna z punktu widzenia tego dokumentu[14].

Złośliwe oprogramowanie może poważnie uszkodzić lub zniszczyć zasoby komputerowe, zapewnić nieuprawniony dostęp do przechowywanych danych (w celu wykorzystania do jakichkolwiek złych zamiarów) i np. wysłać do klientów wprawiające w zakłopotanie wiadomości, które wydają się pochodzić od kancelarii prawnej.

Kody te mogą zainfekować komputery na różne sposoby, zwane wektorami ataku. Infekcja może także nastąpić wskutek skorzystania z zainfekowanego nośnika przenośnego (np. pamięci USB), ale obecnie szkodliwe kody najczęściej pochodzą z dalszych odległości, stale poszukując świeżych „ofiar". Mogą one infekować zasoby za pomocą uprzednio zgromadzonych adresów email[15] lub innych połączeń komputerowych (usługi sieciowe). Dosyć często atakujący wabią nieświadomych użytkowników poprzez wydające się być atrakcyjnymi lub przydatnymi strony internetowe. Oczywiście takie szkodliwe kody mogą być także kierowane w ramach aktywnego rekonesansu lub np. próby przeskanowania adresów sieciowych.

Po uzyskaniu takich adresów, atakujący, bazując na próbach i błędach, może dosyć skutecznie odnaleźć lukę systemu informatycznego w urządzeniu, które chce zaatakować a taka słabość pozwoli mu aktywować nieuprawniony kod na urządzeniu[16]. Niestety nie istnieje nic takiego jak wolna od wirusów platforma dla konsumentów ani podobna platforma dla użytkowników biznesowych.[17]

---

[14] Więcej informacji można znaleźć z pkt. 2 tego przewodnika: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

[15] Poprzez przesyłanie szkodliwych kodów w załącznikach lub kierowanie ludzi na niebezpieczne strony ze złośliwym oprogramowaniem.

[16] Lukę oprogramowania, która może zostać wykorzystana do nieuprawnionego zgromadzenia informacji lub aktywowania nieuprawnionych kodów określa się terminem ang. *exploit* (tzw. kod umożliwiający bezpośrednie włamanie do komputera ofiary – przyp. tłum.).

[17] Różnica we wskaźniku skutecznych ataków często wynika z faktu, że złośliwe kody muszą zostać zaprogramowane dla danego rodzaju

Najważniejszą linią obrony dla kancelarii jest stosowanie odpowiedniego oprogramowania chroniącego przed złośliwym oprogramowaniem. Aby podjąć dobrą decyzję, które oprogramowanie chroniące przed złośliwym oprogramowaniem kupić należy kierować się nie tylko ceną, ale także wynikami testów skuteczności ochrony danego oprogramowania publikowanymi przez niezależne europejskie laboratoria testowe.[18] To wydaje się trywialne, ale w przypadku oprogramowania chroniącego przed złośliwym oprogramowaniem ciągle jeszcze zaskakuje nas fakt, że nie jest ono promowane jako proste w stosowaniu oprogramowanie, które zapewnia najlepszą ochronę.

Oprogramowanie chroniące przed złośliwym oprogramowaniem powinno być instalowane nie tylko na komputerze biurkowym i innym stałym sprzęcie, ale także na urządzeniach mobilnych, np. tabletach czy smartfonach, w sytuacji gdy na tych urządzeniach przechowuje się dane klienta i inne ważne informacje prawne[19].

Oprogramowanie antywirusowe nie zapewnia ochrony przed wszystkimi atakami. Według wskazanych wyżej laboratoriów wskaźniki wykrycia ponad 99% można uzyskać poprzez ochronę przed złośliwym oprogramowaniem już zidentyfikowanym i przeanalizowanym przez firmy zajmujące się oprogramowaniem antywirusowym. Jednakże, od pojawienia się danego złośliwego oprogramowania do czasu jego uwzględnienia w oprogramowaniu antywirusowym może upłynąć długi okres czasu a ogólna strategia ukierunkowanych ataków (hackerskich) polega na wykorzystaniu luki, która nie została jeszcze ujęta w żadnej aktualizacji oprogramowania antywirusowego ani nie została jeszcze usunięta na komputerze będącym celem ataku. Takie luki określa się lukami typu *zero-day*.

Jeżeli sprzęt już został zainfekowany a oprogramowanie chroniące przed złośliwym oprogramowaniem nie jest w stanie usunąć takiego oprogramowania, prawnikom zaleca się skorzystanie z profesjonalnej pomocy przed przywracaniem danych z kopii zapasowych; w przeciwnym razie złośliwe oprogramowanie może dalej być aktywne i może zniekształcić także odzyskane dane. Kancelarie prawne powinny koniecznie wymagać od użytkowników zgłaszania takich incydentów.

Ochrona przed złośliwym oprogramowaniem prowadzi do delikatnej kwestii terminu aktualizacji oprogramowania. Producenci oprogramowania często oferują aktualizacje w celu usunięcia najnowszych odkrytych luk oprogramowania. Stąd szybka instalacja aktualizacji i pakietów naprawczych w znacznym stopniu zmniejsza stopień narażenia nie tylko na złośliwe kody, ale także na ukierunkowane ataki IT. Jednakże instalowanie aktualizacji niesie także ryzyko, że zamiast naprawy danego oprogramowania instalacja naruszy oprogramowanie, które wcześniej działało bez problemu. Z tego powodu duże kancelarie, które dysponują dostatecznymi zasobami powinny najpierw przetestować wszelkie aktualizacje na odpowiednim środowisku testowym, zamiast od razu wgrywać je na komputer wykorzystywany do obsługi klientów.

urządzenia i stąd rzadziej wykorzystywane systemy są w mniejszym stopniu narażone na ataki złośliwego oprogramowania.

[18] https://www.av-test.org/en/antivirus/. http://www.av-comparatives.org/dvnamic-tests/. https://www.virusbtn.com/vb100/latest comparative/ index

[19] Zob. Jeden z raportów dot. urządzeń z systemem Android: http://www.av-comparatives.org/wp-content/uploads/2015/09/avc_mob_2015_en.pdf

5. Mechanizmy kontrolne dotyczące bezpiecznego usuwania nośników wykorzystywanych przez prawników (mechanizm kontrolny 8.3.2./10.7.2. – norma ISO 27001)

Jako że dane klientów stanowią jedne z najbardziej cennych zasobów prawników, dane takie muszą być chronione nawet w sytuacji gdy nie są już dłużej wykorzystywane. Dane te muszą być także bezpiecznie kasowane czy inaczej niszczone.

Dane klientów przechowuje się zarówno na narzędziach przechowywania danych (pamięciach USB, zewnętrznych dyskach twardych), jak i na nośnikach wbudowanych (np. SSD/ pamięciach *flash*). Należy pamiętać o tym fakcie, gdy urządzenia te są przekazywane do serwisu lub gdy sprzedaje się czy w inny sposób pozbywa się takich już nieużywanych urządzeń. Prawnicy muszą pamiętać, że takie dane są przechowywane nie tylko na komputerach, tabletach czy smartfonach, ale także na sprzęcie kopiującym, skanerach czy w faksach.

Jako że proste skasowanie przechowywanych danych lub sformatowanie urządzenia nie powstrzyma zdeterminowanej osoby przez odzyskaniem danych, w procesie przekazywania nośników poza organizację należy albo zastosować specjalne mechanizmy kasowania danych albo nie należy sprzedawać ani i w inny sposób pozbywać się takich nośników danych.

6. Przegląd kategorii działań w dziedzinie nadzoru i powiązanych rodzajów ryzyka (zob. np. sieciowe mechanizmy kontrolne i kryptograficzne mechanizmy kontrolne wskazane w 13.1.1. i 10.1.1. normy ISO 27001)

W celu uzyskania informacji na temat narzędzi, które mogą pomóc prawnikom w poprawie stanu bezpieczeństwa teleinformatycznego w zakresie bezprawnego nadzoru, poniżej przedstawiono kilka scenariuszy wskazujących różne kategorie (1) działań w dziedzinie nadzoru, (2) ryzyka nadzoru oraz (3) sytuacji, w których prawnicy są narażeni na to ryzyko. W scenariuszach szczególną uwagę poświęcono działaniom służącym identyfikacji i ochronie przed ryzykiem bezprawnego nadzoru. Ze względu na istnienie jurysdykcji eksterytorialnej (która nie jest niczym nadzwyczajnym np. w prawie karnym czy prawie konkurencji), mogą zaistnieć sytuacje, w których czynność nadzoru wykonywana przez organy władzy jednego kraju będzie zgodna z prawem w tym kraju, ale nie będzie zgodna z prawem we wszystkich krajach objętych nadzorem (np. w kraju osoby trzeciej danej komunikacji).

Zazwyczaj różnice te można pogodzić przy wykorzystaniu tradycyjnych metod współpracy międzynarodowej pomiędzy organami ochrony porządku publicznego i bezpieczeństwa narodowego, ale oczywiście nie zawsze się to udaje. Nawet w samej Unii Europejskiej państwa mogą prowadzić działania wsparcia bezpieczeństwa narodowego, które mogą być niezgodne z interesami i/lub przepisami prawa innego dotkniętego nimi państwa. W takim przypadku, opracowanie środków ochrony przed nadzorem rządowym może okazać się zasadne jako działanie zgodne z prawem, pożądane i istotne, oczywiście pod warunkiem, że

środki takie mogą zostać zastosowane z technicznego punktu widzenia. Nawet jeżeli krajowe przepisy prawa wymagają od dostawcy usług łączności elektronicznej zapewnienia dostępu do komunikacji realizowanych w sieci lub za pomocą usługi nie oznacza to koniecznie, że środek nadzoru w każdym przypadku będzie zgodny z prawem. Dlatego w poniższej analizie uwzględniono także takie sytuacje.

1) Kategorie działań w dziedzinie nadzoru

a) Działania w dziedzinie nadzoru oparte na zapewnieniu przez usługodawców organom uprawnionym do wykonywania działań w dziedzinie nadzoru z wyprzedzeniem dostępu do określonej infrastruktury na mocy krajowych przepisów prawa.

b) Działania w dziedzinie nadzoru oparte na określonym prawnym procesie nadzoru, np. uzyskanie nakazów lub zewnętrznych upoważnień. Można poczynić rozróżnienie pomiędzy dostępem do danych stanowiących treść i metadanych, ale należy zauważyć, że dane są coraz częściej interpretowane jako metadane i że coraz więcej danych można zgromadzić z metadanych powiązanych z komunikacją, w tym z komunikacją prawników z klientami. Dlatego, z perspektywy zachowania poufności, różnica pomiędzy metadanymi a danymi stanowiącymi treść jest praktycznie minimalna i dla obu tych zbiorów widzimy takie samo zagrożenie dla komunikacji klienta z prawnikiem.

c) Działania w dziedzinie nadzoru stosowane w sposób nieukierunkowany i masowy do całej populacji lub jej znaczącej części („Nadzór masowy/ na dużą skalę"). Jest to forma nadzoru, która stała się ostatnio technologicznie możliwa.

d) Ukierunkowane działania w dziedzinie nadzoru obejmujące gromadzenie informacji o określonych osobach lub grupach osób. W tym dokumencie działania te określono terminem „ukierunkowany nadzór". Jednak granica pomiędzy nadzorem masowym i ukierunkowanym nadzorem została źle zdefiniowana i podlega zmianom, zwłaszcza w ramach analizy sądowej. Przykładowo, gdy sąd stwierdza, że „*nieukierunkowane przeglądanie informacji w drodze kontroli czy to na masową skalę czy w inny sposób stanowiłoby działanie niezgodne z prawem*"[20] wtedy najważniejszym pytaniem staje się to jaki rodzaj „selekcjonerów" uczyniłby nadzór działaniem zgodnym z prawem. Sugeruje się, że rzeczony nadzór stanowiłby ukierunkowany nadzór tylko wtedy gdy przynajmniej jeden podmiot nadzoru zostałby zidentyfikowany z wyprzedzeniem przed rozpoczęciem działań nadzoru.

2) Rodzaje ryzyka nadzoru

Z perspektywy prawnika, należy zidentyfikować następujące różne kategorie ryzyka.

a) **Rejestrowanie rozmowy** bez wiedzy żadnego z uczestników rozmowy (np. z pomocą usługodawców zaangażowanych w techniczną realizację łączności elektronicznej w trybie online lub offline lub bez ich pomocy, z pomocą dostawcy usług internetowych lub innego dostawcy usług poczty elektronicznej czy innych systemów poczty elektronicznej);

b) **Rejestrowanie metadanych** dotyczących rozmowy (identyfikator lub tożsamość osób, czas, okres trwania, długość/rozmiar wiadomości, lokalizacja stron, zapewniające dostęp adresy IP lub fizyczne itd.);

c) **Uzyskanie dostępu do urządzeń** użytkownika końcowego komunikacji (smartfon, komputer) i stosowne rejestrowanie komunikacji i powiązanych metadanych po stronie użytkownika końcowego lub rejestrowanie/uzyskanie dostępu do logów (dzienników) i innych metadanych (historia konwersacji itd.) przechowywanych na urządzeniu użytkownika końcowego;

d) Uzyskanie dostępu do danych w drodze **odzyskania** ze sprzętu, którego się **pozbyto** lub z **nośników danych**;

e) **Uzyskanie dostępu do danych niekonwersacyjnych**, np. przechowywanych dokumentów czy historii wyszukiwania i korzystania.

[20] Trybunał ds. skarg dot. komunikacji elektronicznej Libery i in. przeciw GCHQ 160 (ii) (ang. *Investigatory Powers Tribunal Libery et al. vs. GCHQ 160 (ii)*) http://www.ipt-uk.com/docs/IPT 13 168-173 H.pdf.

3) Scenariusze użytkowania

Poniżej przedstawiono listę głównych scenariuszy użytkowania, które są obarczone ryzykiem nadzoru:

a) Prawnik komunikuje się z klientem lub innym prawnikiem (w tym za pomocą „zwykłego" telefonu biurowego, usługi VoIP czy serwisu OTT np. komunikatora WhatsApp itd.);

b) Prawnik wysyła wiadomość email do klienta lub innego prawnika;

c) Prawnik wysyła dokumenty do klienta lub innego prawnika za pomocą technologii innej niż poczta elektroniczna;

d) Prawnik wykorzystuje rozwiązania elektroniczne zapewniane przez rząd czy sąd do celów wysyłania, odbierania czy przechowania komunikacji (np. wnioski skierowane do sądu);

e) Prawnik przechowuje/pozyskuje pliki, dokumenty czy zapisy drogą elektroniczną (bez wysyłania do osób trzecich);

f) Prawnik przeprowadza analizę prawną;

g) Prawnik pozbywa się sprzętu informatycznego obarczonego ryzykiem naruszenia bezpieczeństwa (telefony, komputery, a także faksy, skanery, drukarki i fotokopiarki posiadające pamięć i twarde dyski);

W pierwszej części poniższej analizy przyjrzymy się cechom charakterystycznym wspólnym dla większości scenariuszy wskazanych powyżej. W drugiej części omówimy konkretne cechy stosownych scenariuszy.

7. Zapewnienie poufności komunikacji – szczególne rodzaje ryzyka nadzoru i możliwe środki zaradcze

Ryzyko nr 1: Rejestrowanie rozmowy i powiązanych metadanych

W zależności od rodzaju technologii i usług zazwyczaj zostaje zapewniony pewien poziom ochrony rozmowy. Jednakże komunikacje często przechodzą przez różne segmenty sieci, których możliwości są różne i które są narażone na różne zagrożenia. Lokalne sieci tradycyjnych rozmów telefonicznych są chronione tylko na poziomie fizycznym (np. w zamykanych na klucz szafach), którą to ochronę można łatwo obejść wewnątrz budynków.

a) Rejestrowanie za pomocą usługodawców

Usługi objęte wyraźnie określonymi standardami np. w ramach infrastruktury zapewnianej przez technologie bezprzewodowe (np. UMTS czy LTE) zapewniają określony wymagany poziom ochrony rozmów. Jednocześnie, dostawcy tych usług mogą często pozostawać zobowiązani do zapewnienia dostępu agencjom rządowym do objętych ochroną rozmów. W Unii Europejskiej sieci i usługi dopuszczone w ramach reżimu „łączności elektronicznej" z 2002 r. muszą umożliwiać legalną kontrolę (zob. Dyrektywa 2002/20/WE, Załącznik A.11) a niezapewnienie możliwości przeprowadzenia takiej kontroli pozwala większości organów krajowych wstrzymać proces dostarczania usług lub sieci. Dotyczy to usług telefonii stacjonarnej i komórkowej oraz dostępu do internetu.

Jednakże usługi bazujące na już istniejącym dostępie do internetu nie są traktowane jako usługi „łączności elektronicznej". Toteż, chociaż wiadomość email i chat (wiadomość przesłana komunikatorem) są traktowane jako usługi łączności elektronicznej, usługi takie jak Skype, Viber i inne podobne usługi korzystające z rozmów w trybie „inapp" nie we wszystkich krajach unijnych są uznawane za usługi łączności elektronicznej (w tym dokumencie także zwane „usługami OTT").

Niektórym organom ochrony porządku publicznego i bezpieczeństwa narodowego udało się przekonać niektórych dostawców usług OTT do współpracy i zapewnienia im praktycznie takiego samego dostępu jak to ma miejsce w sytuacji tradycyjnych usług łączności elektronicznej. Jednakże jeżeli w ujęciu technicznym dostawca usług OTT nie znajduje się wcale w danym kraju (np. ma tam tylko sprzedawców), wtedy dla większości organów wywarcie presji na takich usługodawców, którzy nie chcą współpracować może okazać się bardzo trudne. Stosownie organy te muszą skorzystać z międzynarodowych kanałów koordynacji i współpracy. Ponadto, z mocy prawa, dostawca usług OTT nie ma obowiązku dysponowania określonymi możliwościami zapewnienia kontroli na własny koszt. Stąd, gdy dostawca usług OTT decyduje się na współpracę, przeniesienie kosztów legalnej kontroli na organ rządowy domagający się takiej kontroli może okazać się bardziej skutecznym działaniem.

Korzystanie z usług OTT, których dostawca fizycznie znajduje się tylko w innych jurysdykcjach może służyć jako pewne działanie ochronne przed ukierunkowanym nadzorem ze strony organów rządu, o ile dane jurysdykcje ściśle ze sobą nie współpracują. Jednocześnie należy pamiętać, że większość popularnych dostawców usług OTT jest fizycznie zlokalizowanych w krajach gdzie – przynajmniej według niepotwierdzonych źródeł – ryzyko nadzoru na masową skalę jest najbardziej widoczne. Ponadto należy zauważyć, że wszystkie usługi OTT mogą być rejestrowane na poziomie dostawcy usług internetowych a operator lokalnej sieci komórkowej czy operator lokalnego internetu stacjonarnego może oczywiście w prosty sposób rejestrować emaile do celów legalnej kontroli.

Potencjalne środki zaradcze

Wdrożenie środków ochrony przed nadzorem może mieć wpływ na łatwość korzystania z usługi lub jej efektywność. Jest to kwestia, o której należy pamiętać, chociaż pierwszeństwo należy się tu obowiązkowi deontologicznemu dążenia do zapewnienia poufności.

a) Szyfrowanie komunikacji jako środek ochrony

Jedno rozwiązanie to szyfrowanie rozmów. Ponieważ istnieje wiele różnych metod szyfrowania, zrozumienie co jest szyfrowane a co nie wymaga głębszej analizy. Np. chociaż nawet rozmowy komórkowe drugiej generacji są szyfrowane pomiędzy urządzeniem użytkownika końcowego a stacją bazową, ten rodzaj szyfrowania jest słaby gdy mamy do czynienia z wyspecjalizowanym prywatnym atakującym posiadającym pewne zasoby. Nawet wtedy gdy usługodawca reklamuje swoją usługę jako szyfrowaną, usługodawca może mieć dostęp do kluczy szyfrowania, wskutek czego dana rozmowa będzie bezpieczna tylko do czasu kiedy usługodawca zostanie zmuszony do współpracy z organami porządku publicznego.

Tym niemniej istnieją urządzenia użytkownika końcowego (np. telefony, PBX) zapewniające całościowe szyfrowanie pomiędzy kompatybilnymi urządzeniami, szyfrujące zarówno tradycyjne rozmowy telefoniczne, jak rozmowy OTT[21]. Należy jednak zauważyć, że:

- niektóre z tych rozwiązań mają tzw. „legalne oprogramowanie typu *backdoor*" zapewniające dostęp organom rządowym;
- aby całościowe szyfrowanie działało, obaj użytkownicy muszą korzystać z kompatybilnych urządzeń;
- w niektórych krajach, nawet w ramach UE, import lub sprzedaż takich produktów może podlegać ograniczeniom ze względu na kwestie bezpieczeństwa narodowego[22].

[21] http://www.cryptophone.de/en/products/mobile/. Blackphone https://www.silentcircle.com/products-and-solutions/devices/. http://www.bull.com/hoox etc.

[22] Np. import lub sprzedaż telefonów *Cryptophone* na Węgrzech jest zakazana ze względów bezpieczeństwa.

Całościowe szyfrowanie może zostać zapewnione przez włączenie specjalnego oprogramowania na smartfonie lub tablecie. [23]WhatsApp i Viber umożliwiły wbudowanie całościowego szyfrowania rozmów w oprogramowanie wykorzystywane do uzyskania dostępu do ich usług (lub nawet zapewniły takie ustawienie domyślne).

Większość rozwiązań programowych nie korzysta z tradycyjnych numerów komórkowych w celu przekierowania rozmowy lub wysłania wiadomości.

Ponadto, gdy korzysta się z szyfrowania całościowego opartego tylko na oprogramowaniu, rozmowa może w dalszym ciągu być narażona na ataki na poziomie systemu operacyjnego lub środowiska oprogramowania działającego na urządzeniu (np. Android) (zob. poniżej szczegółowe informacje w punkcie „Uzyskanie dostępu do urządzenia").

Jeżeli chodzi o ryzyko legalnego oprogramowania typu *backdoor* czy ryzyko nierzetelnych obietnic składanych przez dostawców usług łączności elektronicznej, pojedynczym prawnikom bardzo trudno jest temu zaradzić, tak samo jak nie ma możliwości ochrony przed oprogramowaniem typu *backdoor* na poziomie sprzętu sieciowego czy przed nierzetelnymi organami certyfikacyjnymi wydającymi np. certyfikaty SLL dla atakujących.

b) Korzystanie z nierejestrowanych telefonów do komunikacji lub telefonów, dla których dane abonenta lub użytkownika są nieaktualne

Głośno było o tym, że podczas ataków terrorystycznych w Bataclan, we Francji, sprawcy zamiast szyfrowania co celów komunikowania się wykorzystywali jedynie wyrzucone telefony. Jako że w niektórych krajach można kupić kartę SIM bez okazania danych identyfikacyjnych użytkownika oraz ponieważ istnieją telefony typu prepaid gdzie poprzedni użytkownicy nie muszą zgłaszać faktu przeniesienia numeru na nowego użytkownika (w rzeczywistości w niektórych krajach członkowskich nie ma mechanizmów regulacyjnych ani innych, które by to umożliwiały), ta opcja także może służyć ograniczeniu ryzyka nadzoru.

b) Rejestrowanie metadanych rozmów

Najważniejsza różnica pomiędzy rejestrowaniem metadanych i rejestrowaniem samej rozmowy polega na tym, że organ rządowy nie musi uzyskać zewnętrznej zgody na dostęp do takich lub wszystkich metadanych komunikacji (i stąd także „papierowa ścieżka" nadzoru zostaje ograniczona do minimum).

Potencjalne środki zaradcze

Większość metadanych dotyczących rozmów utworzonych w trakcie dostarczania usługi może być rejestrowanych przez usługodawcę, o ile usługodawca wyraźnie nie zdecyduje się wyłączyć rejestrowanie tych danych. Prawnicy nie dysponują technicznymi możliwościami zapobiegania rejestracji takich metadanych. Nawet przy zastosowaniu całościowego szyfrowania, gdy prawnik zadzwoni na tradycyjny numer telefonu, wszystkie ważne metadane zostaną zarejestrowane przez usługodawcę, w tym wybrany numer telefonu, długość rozmowy itd.

Tak więc, jeżeli stanowi to problem prawnik powinien domagać się unikania tego sposobu komunikacji i zamiast niego korzystać z usług OTT.

Ryzyko nr 2: Uzyskanie dostępu do urządzenia

Jak wskazano powyżej, nawet całościowe szyfrowanie może okazać się bezużyteczne, jeżeli atakujący ma dostęp do samego urządzenia użytkownika końcowego.

Ze względu na duże zróżnicowanie różnych programów, które mogą być instalowane na dużej liczbie potencjalnych urządzeń, największe ryzyko stanowią luki w oprogramowaniu tzn. błędy nieprawione w niektórych elementach środowiska oprogramowania wykorzystywanego przez dane urządzenie. Atakujący może wykorzystać te luki, aby uzyskać

[23] Np. zob. inne produkty Cellcrypt, Chatsecure, Signal Private Messenger, Silent Circle, wickr itd.

nieuprawniony dostęp do funkcjonalności urządzenia i w konsekwencji przejąć kontrolę nad urządzeniem, w tym rejestrować rozmowy lub uzyskać dostęp do logów zawierających ważne metadane.

Obecne na urządzeniu złośliwe oprogramowanie (wirusy, robaki itd.) może także przyznawać nieuprawniony dostęp atakującym. Takie złośliwe oprogramowanie mogło zostać zainstalowane przez przypadek, także wskutek wchodzenia na urządzeniu na strony ze złośliwym oprogramowaniem.

Ostatnia, ale nie mniej ważna kwestia: posiadanie fizycznego dostępu do urządzenia może dać taką możliwość atakującym.

Potencjalne środki zaradcze

Ryzyko to można obniżyć poprzez stosowanie podstawowych środków bezpieczeństwa określonych w powyższych rekomendacjach i ograniczanie fizycznego dostępu do urządzenia lub odpowiednio regularną wymianę urządzeń. Aktywacja opartych na hasłach blokad na urządzeniach i szyfrowanie narażonych na utratę danych przechowywanych na urządzeniu stanowi minimalne zabezpieczenie, które ma pewne znaczenie i które wszyscy prawnicy powinni stosować nienależnie od tego czy dążą do ochrony przed nadzorem czy też nie. Oczywiście należy stosować silne hasła i należy je regularnie zmieniać.

Ryzyko nr 3: Uprzednio skasowane dane

Prawnicy i kancelarie prawne często muszą pozbywać się określonego sprzętu informatycznego, który zawiera pamięci trwałe lub nośniki danych (media dla danych), np. telefonów, laptopów czy komputerów. Nowoczesne skanery i fotokopiarki dosyć często posiadają wbudowane pamięci lub dyski twarde.

O ile prawnik nie pozbywa się takiego sprzętu w odpowiedni sposób, każdy kto posiada dostęp do takich nośników danych może odzyskać znaczące części danych przechowywanych na tych urządzeniach, nawet wtedy gdy dane zostały uprzednio skasowane.

Potencjalne środki zaradcze

Ważne jest, aby prawnicy zapewniali, że albo wszystkie dane na nośnikach danych zostają nadpisane przed pozbyciem się tych nośników albo takie nośniki danych zostają fizycznie zniszczone lub że wszystkie nośniki danych są przechowywane (i nie są odsprzedawane) do celów bezpieczeństwa. Większość biurowych niszczarek papieru jest w stanie zniszczyć płyty CD i DVD, natomiast zniszczenie dysków twardych czy SSD może okazać się stosunkowo drogie.

Gdy nośniki danych są niszczone poza siedzibą prawnika, przez osobę trzecią, zaleca się zażądania od osoby trzeciej potwierdzenia, że nośniki faktycznie zostały zniszczone.

Ryzyko nr 4: Uzyskanie dostępu do danych niekonwersacyjnych

Dane niepowiązane z rozmowami, np. dane przechowywane w siedzibie kancelarii prawnej czy u osoby trzeciej, są narażone na podobne ryzyko nadzoru jak dane dotyczące rozmów. Zazwyczaj dostęp do takich danych w siedzibie kancelarii prawnej przez organ rządowy podlega dodatkowej ochronie regulacyjnej (np. nakazom). Jednakże dostęp do danych przechowywanych dla prawnika przez osobę trzecią stosunkowo często nie podlega takiej samej ochronie prawnej jaka ma zastosowanie do siedziby kancelarii prawnej a usługodawca może nie traktować informacji jako objętej klauzulą poufności.

Potencjalne środki zaradcze

Nawet gdy przekazanie przez kancelarię prawną podlega ochronie za pomocą np. szyfrowania SSL, radzi się korzystanie z usług przechowywania umożliwiających tzw. „szyfrowanie po stronie klienta”[24].

W takiej sytuacji sprawą najwyższej wagi jest jednak zapewnienie przez prawnika zabezpieczenia hasła lub innych mechanizmów ochrony (np. tokenów) stosowanych do uzyskania dostępu do zaszyfrowanych danych. Ludzie przyzwyczaili się do posiadania dostępu do zasobu nawet w sytuacji utraty hasła poprzez zapewnienie alternatywnego wiarygodnego sposobu uwierzytelnienia. Zasada ta nie działa w przypadku szyfrowania: gdy prawnik utraci hasło, usługodawca nie będzie miał technicznej możliwości zapewnienia dostępu do zaszyfrowanych danych, tak więc zaszyfrowane dane zostaną na pewno utracone.

[24] Np.. SpiderOak, TresorIT.

8. Rekomendacje dotyczące określonych technologii łączności

a) Bezpieczeństwo sieci dostępu

Chociaż sieci wi-fi są szeroko stosowane, prawnicy powinni być ostrożni w korzystaniu z takich sieci w celu uzyskania dostępu. Na ogół sieć wi-fi nie stanowi sieci odpowiedniej do stosowania do celów zawodowych, w tym do pracy na informacjach poufnych, o ile nie stosuje się dodatkowej warstwy ochrony w ramach całościowego szyfrowania podobnej do tej stosowanej przez usługi VPN.

Bez takiej dodatkowej warstwy ochrony, prawnik nie powinien korzystać z sieci wi-fi niezapewniającej najbardziej podstawowej kontroli dostępu, aby wysłać informacje dotyczące klienta. W sytuacji braku takich środków ochrony, dowolna osoba (anonimowe osoby, maszyny) znajdująca się w pobliżu może zobaczyć i zarejestrować pełny przepływ danych.

Ponadto, sam fakt, że sieć jest chroniona hasłem nie czyni jej bardziej bezpieczną od „otwartych" sieci wi-fi. Jeżeli niemożliwy do zidentyfikowania atakujący może włączyć się do tej samej sieci ze względu na wspólne hasło (np. hasło współdzielone z wszystkimi w zasięgu widoczności lub z tymi, którzy mogli korzystać z sieci w przeszłości) taki atakujący będzie miał taką samą możliwość oglądania przepływu danych prawnika jaką miałby w sieci niechronionej hasłem. Toteż, prawnicy powinni powstrzymywać się od korzystania z sieci wi-fi bez VPN, gdy nie ma możliwości zapewnienia, że hasło do sieci wi-fi zostało zmienione w ciągu ostatniego dnia lub dwóch ostatnich dni.[25] Wiarygodne i bezpieczne uwierzytelnienie „użytkowników gości" jest dosyć skomplikowane, i stąd bez wątpienia, bardzo rzadkie.

Korzystanie z mobilnego internetu jest bezpieczniejsze niż korzystanie z sieci wi-fi, ale zagranicą nie zawsze jest to możliwe.

Najbezpieczniejszym rozwiązaniem jest nawiązanie połączenia w sieci VPN pomiędzy urządzeniem zdalnym a biurem lub innym wrażliwym mobilnym zasobem IT.

O tym także należy pamiętać, gdy prawnicy zapewniają swoim klientom (darmowy) dostęp do sieci wi-fi w siedzibie prawnika – kancelaria prawna może nieświadomie narazić dane klienta na niepotrzebne ryzyko. Oferowane klientowi połączenie wi-fi nie może być takie samo jak to wykorzystywane w biurze. Różnica pomiędzy dwiema sieciami powinna zostać wyjaśniona wszystkim członkom i pracownikom kancelarii i należy ich poprosić o niekorzystanie z sieci wi-fi udostępnianej klientom do celów zawodowych. Ponadto, prawnicy powinni oferować klientom dostęp do sieci wi-fi tylko wtedy gdy są w stanie zapewnić odpowiednia ochronę i wiarygodność sieci.[26]

Prawnicy prowadzący jednoosobową działalność gospodarczą i małe kancelarie prawne powinny pamiętać, że korzystając z sieci (np. Ethernet) dostarczonej przez właściciela (np. w obsługiwanych środowiskach biurowych), muszą weryfikować z właścicielem (lub najlepiej z ekspertem IT) czy sieci LAN wszystkich najemców są bezpiecznie od siebie oddzielone. Jeżeli inni najemcy są w stanie uzyskać dostęp do komputerów kancelarii prawnej, te komputery i znajdujące się w nich pliki klientów są narażone na znaczące ryzyko, nawet wtedy gdy zwykły użytkownik nie jest świadomy możliwości uzyskania takiego dostępu.

b) Wiadomości email

[25] Atakujący może przechwycić komunikacje pomiędzy punktem dostępu do sieci wi-fi i wykorzystywanym urządzeniem po wpisaniu wspólnego lub współdzielonego hasła. Jednak nie jest to takie proste jak w przypadku otwartej sieci wi-fi. (WPA PSK).

[26] Zamiast korzystać z połączenia wi-fi bez hasła lub opartego na wspólnym haśle, możemy skorzystać z systemu generującego prywatny punkt dostępu tzw. hotspot, np.http://www.zyxel.com/us/en/products_services/uag50.shtml.

Stosowane przez kancelarie prawne wiadomości email mogą być rejestrowane na wiele sposobów, przez dostawcę lokalnej sieci (sieci LAN) w lokalizacji nadawcy lub odbiorcy, przez dostawcę usług internetowych nadawcy lub odbiorcy (gdy jest to inna osoba niż dostawca sieci LAN), przez dostawcę zapewniającego usługi poczty elektronicznej lub przez podmiot przekazujący emaile do wysyłki do odbiorcy.

Z punktu widzenia nadzoru rządowego i obowiązku usługodawcy, dostawcom usług poczty elektronicznej jest bliżej do dostawców usług OTT i nie podlegają oni a priori skomplikowanym wymogom rejestrowania i przechowywania wiadomości email zgodnie z potrzebami organów nadzoru – przynajmniej do czasu wystąpienia do nich z takich żądaniem przez te organy rządowe. Niezależnie od powyższego, udzielanie dostępu organom nadzoru do wiadomości email powinno zawsze podlegać zewnętrznemu zatwierdzeniu (np. w formie nakazu sądowego)

Coraz częściej połączenie pomiędzy dostawcą usług poczty elektronicznej i lokalnym oprogramowaniem klienta jest zabezpieczane za pomocą szyfrowania SSL. Ale nie musi to oznaczać, że wiadomość ta pozostanie zaszyfrowana w trakcie jej przekazywania przez usługodawcę do usługodawcy odbiorcy lub usługodawców pośredniczących. W przyszłości takie szyfrowanie stanie się bardziej powszechne, jednak mając na uwadze dużą liczbę dostawców usług poczty elektronicznej i stosowane przez nich różne ustawienia bardzo trudno jest zapewnić całościowe szyfrowanie wiadomości email bez poświęcenia możliwości dostarczenia wiadomości w dowolne miejsce na ziemi.

Z punktu widzenia zapewnień prawnych w zakresie komunikacji klienta z prawnikiem, lepszą ochronę zapewnia korzystanie z wewnętrznej usługi poczty elektronicznej zarządzanej przez kancelarię prawną. W praktyce jednak w większości kancelarii prawnych zastosowanie takiego „opracowanego własnym sumptem" podejścia skutkować będzie obniżeniem bezpieczeństwa operacyjnego i technicznego oraz niezawodności niż jakimiś korzyściami z tytułu dodatkowych zapewnień prawnych. Najwięksi dostawcy usług poczty elektronicznej dysponują możliwościami technicznymi prowadzenia nieukierunkowanego nadzoru na dużą skalę.

Z tego powodu ważne jest, aby opcja stosowania całościowego szyfrowania wiadomości email stanowiła stały element większości klientów poczty elektronicznej („agentów użytkownika email"). Ponadto, mając na uwadze fakt, że wielu prawników europejskich ma dostęp do certyfikatów podpisu elektronicznego X.509 (i podobnych certyfikatów dot. szyfrowania), bezpieczeństwo wiadomości email mogłoby zostać znacząco poprawione w całej Unii gdyby istniał prosty do wykorzystania i wiarygodny katalog certyfikatów szyfrowania dla prawników.

W sytuacji gdy takie szyfrowanie nie jest możliwe, ponieważ np. trzeba było wysłać do klienta email bez żadnego certyfikatu szyfrowania, byłoby lepiej zaszyfrować najważniejsze informacje dotyczące klienta w załączniku i wysłać klientowi jednorazowe hasło innym kanałem (np. za pomocą SMS czy przekazać telefonicznie, ale nie emailem).

c) Procedury e-sądu i e-rządu

Aby złożyć lub otrzymać dokumenty, prawnicy coraz częściej muszą korzystać z transmisji elektronicznej zapewnianej przez sądy. Korzystanie z takich rozwiązań zawsze niesie z sobą ryzyko uzyskania nieuprawnionego dostępu przez osoby trzecie lub zagraniczne rządy. Zaszyfrowana transmisja dokumentów i zaszyfrowane przechowywanie stanowią ważne zabezpieczenie, ale coraz częściej narzędzia te mogą zostać zapewnione tylko po stronie usługodawcy rządowego zapewniającego dostęp do swojego systemu. W niektórych krajach członkowskich samorządy prawnicze i stowarzyszenia prawnicze mogą zapewnić rozwiązania transmisji elektronicznej, w ramach których rola rządu będzie ograniczała się do zapewnienia bramki (dostępu) do takich rozwiązań. Chociaż rozwiązanie to ma pewne zalety takie jak możliwość utrzymania kontroli na systemem w ramach profesji prawniczej i zapewnienia prawnikom praktycznych rozwiązań dopasowanych do ich potrzeb oraz

zapewnienie, że uzyskują oni pełne informacje na temat stosowania i wszelkich szkodliwych incydentów, jakie mogą mieć miejsce, przenosi ono także na samorządy prawnicze i stowarzyszenia prawnicze koszt i ryzyko zapewnienia takich rozwiązań. Z tego powodu rozwiązanie to nie przypadłoby raczej do gustu samorządom prawniczym i stowarzyszeniem prawniczym.

4 WNIOSEK

Nie da się osiągnąć absolutnej ochrony systemów informatycznych przed legalnym czy innego rodzaju nadzorem ani przed innymi atakami hackerskimi. Systemy IT zawsze będą narażone na atak, a te Wskazówki pokazują, że nie istnieje nic takiego jak całościowy system, który zapewniałby całkowitą ochronę danych. Istnieje wiele rodzajów ryzyka naruszenia bezpieczeństwa, na które każdego dnia wystawiane są dane przechowywane przez prawników i komunikacje pomiędzy prawnikami i klientami.

W tym kontekście ważne jest, aby prawnicy byli w stanie wykazać podejmowane działania wobec swoich klientów i szerszej opinii publicznej. Zasadniczy komponent stanowi tu ustrukturyzowane i spójne podejście do analizy ryzyka.

Stosownie, w tym dokumencie przedstawiono sugerowane ramy ogólne, które Samorządy i Stowarzyszenia Prawnicze mogą wykorzystać do opracowania rekomendacji dla swoich członków w zakresie usystematyzowanego i ustrukturyzowanego podejścia jakie może zostać przyjęte do ograniczenia wskazanych rodzajów ryzyka. Może okazać się, że sugestie tu podane posłużą poszczególnym Samorządom i Stowarzyszeniom Prawniczym za punkt wyjścia do opracowania bardziej szczegółowych rekomendacji a nawet obowiązkowych wymogów dla swoich członków podobnie do systemów stosowanych do ochrony dokumentów papierowych i komunikacji osobistej.

Stosowanie zawartych tu wskazówek nie polega jednak na „odhaczaniu” kolejnych pozycji. Zagrożenia dla bezpieczeństwa systemów informatycznych stale się zmieniają, tak jak i same systemy. Nawet duże organizacje, które dysponują lepszymi zasobami niż największe kancelarie prawne są narażone na sytuacje naruszenia bezpieczeństwa, pomimo podejmowanych przez nie wysiłków w zakresie ochrony przez takim zdarzeniami.

Toteż nie chodzi tu o to czy naruszeniu bezpieczeństwa teleinformatycznego można zapobiec, ale raczej o to w jaki sposób prawnicy mogą wykazać, że zastanowili się nad kwestiami problematycznymi, odnieśli się do nich oraz że podjęli odpowiednie działania zaradcze w tym zakresie.