ISSA POLSKA

Bezpieczeństwo IT w kancelarii

Poradnik

PATRONAT MERYTORYCZNY

Cyberlaw.pl

PATRONAT HONOROWY

Adwokatura Polska — Prawo Ojczyzna Honor — aplp

Celem "ISSA Polska – Stowarzyszenie do spraw Bezpieczeństwa Systemów Informacyjnych" jest krzewienie wiedzy na temat bezpieczeństwa systemów informacyjnych oraz promowanie zasad i praktyk, które zapewniają poufność, integralność, niezaprzeczalność i dostępność zasobów informacyjnych, a także promowanie i rozwój swoich członków poprzez podnoszenie ich umiejętności zawodowych związanych z ochroną systemów informacyjnych, w szczególności poprzez:

- dostarczanie wiedzy związanej z tematyką szeroko pojętego bezpieczeństwa systemów informacyjnych,
- edukację i promowanie standardów dotyczących bezpieczeństwa systemów informacyjnych,
- opiniowanie wydarzeń i rozwiązań z zakresu bezpieczeństwa systemów informacyjnych,
- propagowanie potrzeby bezpieczeństwa systemów informacyjnych.

ISSA to elitarne, ogólnoświatowe Stowarzyszenie osób zajmujących się zawodowo oraz związanych z branżą bezpieczeństwa informacji oraz bezpieczeństwa systemów informatycznych. Polski oddział jest 100 oddziałem (chapterem) w skali światowej, i należy do najszybciej rozwijających się oddziałów w Europie. Tworzą go zarówno eksperci ds. bezpieczeństwa, jak i pasjonaci.

Zapraszamy na stronę https://issa.org.pl

Szanowny Czytelniku,

w imieniu zespołu projektowego i Stowarzyszenia ISSA oddajemy w Twoje ręce zestaw dobrych praktyk, których wdrożenie zapewni, że bezpieczeństwo informacji przetwarzanych w kancelarii za pomocą systemów teleinformatycznych będzie dużo większe. Ze względu na szczególny charakter pracy prawników, związany z koniecznością przetwarzania informacji stanowiących tajemnicę zawodową oraz dane osobowe z wykorzystaniem systemów informatycznych, chcemy pomóc podnieść poziom wiedzy i świadomości prawników z zakresu bezpieczeństwa teleinformatycznego. W odróżnieniu od świata papierowych dokumentów, dbanie o bezpieczeństwo informacji w świecie elektronicznym jest mniej intuicyjne i ma więcej aspektów niż tylko zabezpieczenie nośnika informacji przed utratą czy kradzieżą. Wykonanie kopii informacji w postaci elektronicznej też jest prostsze i z reguły wymaga mniej czasu niż skopiowanie papierowych akt, ponadto nie zostawia wielu śladów takiej operacji. Ponadto komputer podłączony do sieci Internet nie wymaga fizycznego dostępu do urządzenia aby podjąć próby włamania do niego i pozyskać informacje zawarte w nim, nie ma ograniczeń fizycznych ani czasowych. Mam nadzieję że niniejsze opracowanie pomoże lepiej zabezpieczyć systemy komputerowe w kancelariach włączając w to laptopy samych zainteresowanych. Pamiętajmy że komputer i sieć Internet to z jednej strony szereg ułatwień w dostępie i przetwarzaniu informacji, a z drugiej znacznie większa możliwość wycieku informacji.

Gorąco polecam lekturę zainteresowanym i wdrożenie w praktyce proponowanych rozwiązań!

Z poważaniem –

Adam Danieluk

Prezes ISSA Polska

Bezpieczeństwo w kancelarii to temat niezwykle ważny. Wyciek jakichkolwiek informacji dotyczących klienta jest niedopuszczalny. Często inwestujemy w zabezpieczenia takie jak kraty, sejfy (tzw. bezpieczeństwo fizyczne), ale nie zwracamy tak dużej uwagi na to jak łączymy się z siecią Internet czy też korzystamy z popularnych, darmowych kont pocztowych do obsługi klienta. Jednocześnie w Internecie jest coraz więcej przestępców, którzy „polują na informacje" i ich celem stają się kancelarie. A w kancelariach przetwarzanych jest wiele danych, w tym o różnym charakterze, nierzadko danych wrażliwych (dotyczących skazań, stanu zdrowia etc.). Niniejsza publikacja ma za zadanie przybliżyć prawnikom ten skomplikowany, ale istotny w pracy zawodowej temat. Celem jest poznanie dobrych praktyk, które są potrzebne w życiu codziennym, jak i przybliżenie różnych możliwości przetwarzania danych, w tym wymiany informacji z klientem oraz przykładowych scenariuszy ataków.

Beata Marek

Dyrektor ds. Prawnych ISSA Polska

Spis treści

I. Ogólne zasady bezpieczeństwa: dobre praktyki (B. Marek, M. Juszczyk)

Stosowanie się do dobrych praktyk związanych z bezpieczeństwem pozwala zmniejszyć ryzyko wystąpienia naruszeń lub incydentów bezpieczeństwa IT w kancelarii. Poniższe zestawienie jest przydatne dla wszystkich pracowników kancelarii, przyda się także w zwiększeniu bezpieczeństwa prawnika w codziennym korzystaniu przez niego z sieci Internet.

1

Pobieraj pliki tylko z zaufanych stron

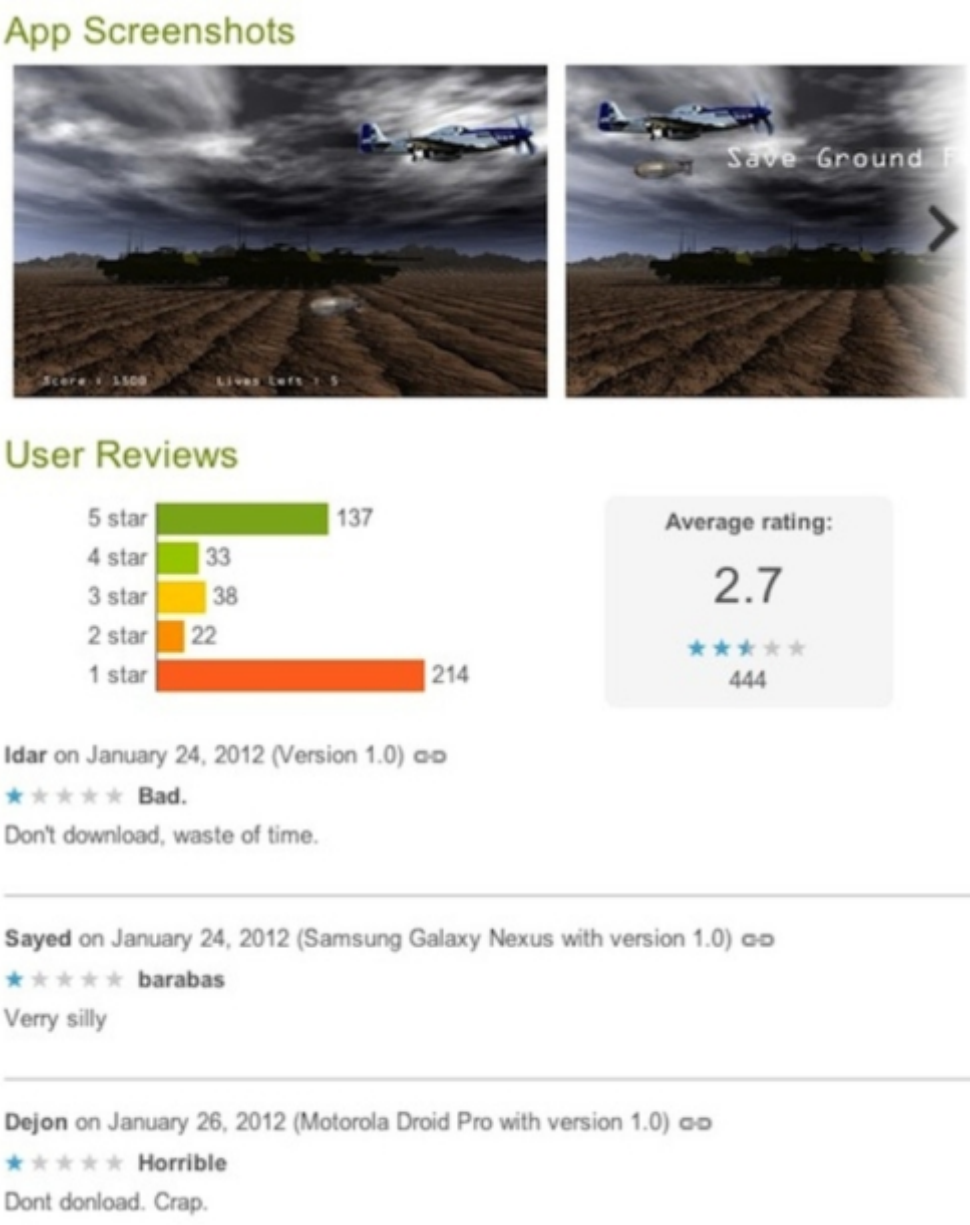
tj. z oficjalnych stron producentów oprogramowania, a w przypadku aplikacji – tylko od dostawców, którzy są wiarygodni (np. programisty prowadzącego zarejestrowaną działalność albo zaufanego, którego aplikacja jest dostępna co najmniej kilka miesięcy i ma relatywnie dużą liczbę ściągnięć i pozytywną ilość komentarzy). Nie pobieraj oprogramowania lub aplikacji za SMS.

Za niezaufane strony należy uznać inne niż strony producenta. Niekiedy strony te wymagają ściągnięcia dedykowanego programu do instalacji programów komputerowych. Zdarza się, że gdy przeglądasz Internet, reklama może poinformować Cię o potrzebie instalacji oprogramowania (np. w celu sprawdzenia czy nie masz wirusa albo oczyszczenia komputera by działał szybciej). Nie instaluj takich programów.

Programy komputerowe, w tym aplikacje pobierane na firmowe lub prywatne urządzenia, powinny być pobierane z zaufanych źródeł. Jest to bardzo ważne, gdyż program może wykonywać w tle informacje, które mogą prowadzić do szpiegowania Ciebie lub wysyłania ukrytych SMS-ów premium. Dzięki dobrej praktyce pobierania możesz uchronić się od zainstalowania złośliwego oprogramowania, które podszywa się pod znane oprogramowanie albo jest prostym programem wykonującym w tle nieautoryzowane czynności. Szczególnie uważaj przy pobieraniu darmowych programów. Czy wiesz, że cyberprzestępcy celowo umieszczają w marketach (czyli miejscach, z których pobierasz aplikacje na smartphone/tablet) lub katalogach stron z różnymi programami komputerowymi oprogramowanie, które jest najczęściej

bezpłatne, a jednocześnie zainfekowane? Robią to w taki sposób, że tworzą fikcyjne konta w popularnych marketach z aplikacjami albo umieszczają linki do stron z pobieraniem na forach lub stronach www z różnymi programami komputerowymi. Szczególnie uważaj przy instalacji gier lub prostych programów. Nie pobieraj oprogramowania z reklam, które informuje o "wykryciu zagrożenia", potrzebie przyspieszenia komputera albo aktualizacji.

Poniżej znajduje się przykład aplikacji zainfekowanej, która została umieszczona jako darmowa gra na urządzenia z systemem Android.



Użytkownicy wystawiali negatywne opinie oraz komentarze. Pomimo to gra miała wiele pobrań. Dlatego ważne jest, by z tabletu albo smartphone, z którego prawnik korzysta do pracy, mieć kontrolę nad tym, jakie aplikacje chce instalować np. dziecko. Aplikacja przedstawiona na rysunku została usunięta dopiero po zbadaniu przez firmę zajmującą się ochroną oprogramowania, która sprawę zgłosiła. Aplikacja zawierała złośliwe oprogramowanie[1].

2.

Utwórz dwa konta w systemie operacyjnym Twojego komputera.
Jedno konto "administratora" a drugie "użytkownika".
Loguj się do konta "użytkownika" i to na tym koncie pracuj i korzystaj z Internetu.

Dzięki tej praktyce, gdy przestępca będzie chciał zainfekować Twój komputer w czasie przeglądania Internetu bądź poczty, utrudnisz mu to. Zastosuj tę praktykę na wszystkich komputerach w kancelarii.

3.

Hasło do konta "administratora" powinno być znane Tobie, może być znane także informatykowi, który opiekuje się zasobami IT w kancelarii. Inne osoby nie powinny go znać.
Hasło administratora nie powinno być słabe (zbyt krótkie i zbyt oczywiste), łatwe do odgadnięcia. Unikaj zapisywania haseł na karteczkach lub w ogólnodostępnych plikach, które z łatwością mogą odczytać osoby trzecie lub nieuprawnieni do tego użytkownicy. Hasło nie powinno być także powszechnie znane i dostępne dla wszystkich, którzy korzystają z infrastruktury komputerowej kancelarii. Daje to bowiem możliwość bezpośredniej ingerencji w zasoby IT organizacji i instalowania dowolnego oprogramowania przez pracowników.

Dzięki tej praktyce osoby nieupoważnione przed instalacją jakiegokolwiek oprogramowania albo dokonywania poważniejszych zmian w systemie nie będą mogły ich dokonać bez znajomości hasła administratora. W ten sposób zwiększysz także kontrolę nad zasobami, które instalowane są na komputerach w kancelarii.

[1] Źródło zdjęcia oraz informacji: http://www.computerworld.com/article/2500566/malware-vulnerabilities/massive-android-malware-op-may-have-infected-5-million-users.html , data dostępu: 6.12.2016.

4.

Jeżeli zatrudniasz informatyka albo korzystasz z zewnętrznego wsparcia technicznego, podpisz odpowiednią umowę, gwarantującą Ci odpowiedni poziom jakości oraz regulującą powierzenie przetwarzania danych osobowych.

Dzięki tej praktyce zostaną zakreślone lepiej wymagania i obowiązki, a także uregulowane podstawy pociągania do odpowiedzialności.

5.

Szyfruj dane klientów w obrębie pełnego szyfrowania dysków lub co najmniej w obrębie folderów na dyskach (w tym przypadku dokonuj edycji wszystkich dokumentów, nie przenosząc ich z szyfrowanego folderu).

Dzięki tej praktyce osoba nieupoważniona, która zaloguje się do Twojego urządzenia, nie będzie miała dostępu do danych Twoich klientów jeżeli nie będzie znała dodatkowego hasła dostępu. W dalszej części poradnika znajdziesz konkretne informacje o tym, jak w prosty sposób szyfrować.

6.

Wykonuj regularnie kopie bezpieczeństwa i kopie zapasowe danych z Twoich urządzeń.
W przypadku danych klientów – pamiętaj, aby kopia była szyfrowana.
Wykonywane regularnie kopie zapasowe danych z wszystkich urządzeń (komputerów stacjonarnych, przenośnych, urządzeń mobilnych) zgodnie z procedurą bezpieczeństwa kancelarii pozwalają utrzymać ciągłość działania. Stworzone kopie sprawdzane powinny być pod kątem poprawności wykonania oraz możliwości odtworzeń. W przypadku danych klientów, kopia bezpieczeństwa może być szyfrowana kluczem (hasłem) użytkownika. Zapewnia to znacznie wyższy poziom bezpieczeństwa. Proces wykonywania kopii bezpieczeństwa powinien być zautomatyzowany, regularny i przeprowadzany w ściśle zdefiniowanym terminie. Kopie zapasowe powinny być wysyłane do kilku różnych źródeł (nośniki zewnętrzne, chmura). Po sporządzeniu kopii bezpieczeństwa nośnik powinien zostać odłączony.
Pamiętaj, żeby wymieniać nośniki co jakiś czas, gdyż sprzęt się starzeje i może się nie uruchomić po kilku latach.

Jeżeli kopie zapasowe nie są wykonywane, bądź też są wykonywane nieregularnie, zwiększasz ryzyko utraty dostępu do cennych danych. Backup nie powinien być także zapisywany wyłącznie na nośnikach optycznych typu (CD/DVD/Blu-ray), bo nie daje gwarancji ich odtworzenia w przypadku awarii. Pamiętaj, że kopia bezpieczeństwa powinna być szyfrowana. Jeśli nie jest, to ułatwisz dostęp do wrażliwych danych na temat kancelarii osobom nieupoważnionym.

dzięki tej praktyce będziesz mógł szybko wrócić do historycznych wersji w razie utraty urządzeń albo utraty dostępu do nich. Pamiętaj, że awaria dysku lub złośliwe oprogramowanie może spowodować brak dostępu do danych. Pomyśl, gdyby teraz zniknęły dane o klientach, które posiadasz na dysku, czy mógłbyś w jakiś sposób je odtworzyć?

7

Ustanawiaj różne poziomy dostępu do danych klientów dla pracowników.

Dzięki tej praktyce będziesz mieć kontrolę nad tym, z jakiego rodzaju informacjami zapoznają się określeni pracownicy, a do jakich nie powinni mieć dostępu.

8

Korzystaj z firmowej poczty e-mail albo przypisanej Tobie przez organizację zawodową przy obsłudze korespondencji od klientów i stosuj tę zasadę także w stosunku do swoich pracowników.

Korzystanie z firmowej poczty e-mail, którą dostarcza zaufany hostingodawca, stosujący protokoły SSL/TLS daje Ci pewność, że przesyłane informacje są odpowiednio zabezpieczone, a filtry antyspamowe przechwytują niechcianą korespondencję. Komunikuj się wyłącznie przy użyciu firmowej, bezpiecznej poczty e-mail. Nie będziesz narażać na niebezpieczeństwo klientów kancelarii oraz zawsze, w przypadku jakichkolwiek problemów z pocztą, możesz skorzystać z supportu technicznego firmy hostingowej.

Korzystanie z prywatnej, darmowej poczty e-mail jest niebezpieczne dla prawnika (nie masz żadnej kontroli nad dostawcą) i uniemożliwia Ci także podpisanie umowy powierzenia przetwarzania danych osobowych.

Dzięki tej praktyce możesz ograniczyć otrzymywanie niechcianych reklam i spamu oraz korzystasz z infrastruktury zaufanego dostawcy, z którym kancelaria powinna mieć podpisaną umowę powierzenia przetwarzania danych osobowych.

9.

Korzystaj z wiarygodnego oprogramowania chroniącego Twoje urządzenie i urządzenia w kancelarii.

Pamiętaj by oprogramowanie to było zawsze aktywne (działało w czasie rzeczywistym). Sprawdź, czy systemy operacyjne i urządzenia, z których korzystasz posiadają firewalla, czyli zaporę sieciową, chroniącą przed atakami.

Dzięki tej praktyce możesz zminimalizować ryzyko zainfekowania Twojego urządzenia lub zwiększyć jego wykrycie. Dobierz rodzaj oprogramowania zabezpieczającego do potrzeb kancelarii, szczególnie do rodzaju i ilości przetwarzanych danych klientów.

10.

Podpisz umowę powierzenia przetwarzania danych osobowych z dostawcą infrastruktury lub hostingu, na którym znajduje się Twoja strona www / kancelaryjna poczta lub dedykowana aplikacja dla klientów.

Dzięki tej praktyce wypełniasz obowiązek prawny, a jednocześnie masz podstawę do pociągnięcia do odpowiedzialności w przypadku przekroczenia uprawnień określonych w umowie bądź niedochowania określonych w umowie obowiązków. Co więcej, masz zapewnienie dostawcy, że wszelkie dane osobowe znajdujące się na serwerze kancelarii spełniają niezbędne kryteria dla bezpiecznego i zgodnego z przepisami przechowywania danych osobowych.

11.

Używaj nieoczywistych haseł, składających się z co najmniej 10 znaków, w tym małych i dużych liter, jednej cyfry i znaku specjalnego (np. Lubie!Zelki23) co najmniej do obszarów logowania gdzie jest dostęp do danych klientów.

Dobrą praktyką jest, gdy hasło składa się z niepowiązanych ze sobą wyrazów.

Używaj kombinacji haseł do różnych swoich kont. Dodatkowo, wszędzie tam, gdzie to możliwe, miej włączoną dwuetapową weryfikację logowania. Przykładowo – do otwarcia systemu i później do otwarcia teczki klienta. Procedury zarządzania hasłami, w tym ich zmian, wpisane powinny być w politykę bezpieczeństwa kancelarii. W przypadku stosowania wielu silnych haseł pomocne są specjalne menadżery haseł.

Dzięki tej praktyce będziesz mieć kilka silnych haseł, które łatwo zapamiętasz. Mogą się one różnić od siebie niuansami, o których tylko Ty będziesz wiedzieć (unikaj jednak różnic występujących tylko w pojedynczych znakach specjalnych lub liczbach). Wymagaj, by Twoi pracownicy także stosowali tę zasadę w pracy. Możesz ich do tego zobowiązać poprzez odpowiednie zapisy w Polityce Bezpieczeństwa.

12.

Nie korzystaj z publicznych sieci Wi-Fi.

Dzięki tej praktyce ograniczysz ryzyko wycieku Twoich haseł. Jeśli jednak wcześniej korzystałeś z sieci publicznych, to koniecznie usuń je z zapisanych sieci w swoim urządzeniu. Nawet jeśli nie będziesz znajdować się w obrębie danej sieci publicznej, przestępcy mogą utworzyć sieć o identycznej nazwie, do której Twoje urządzenie – bez Twojej wiedzy – podłączy się automatycznie i zacznie przez nią wysyłać informacje. Jeśli już musisz skorzystać z publicznej sieci Wi-Fi, to zainstaluj klienta VPN, który zaszyfruje połączenie i będzie chronił przed utratą ważnych danych.

13.

Jeżeli korzystasz z Internetu za pomocą zaufanej sieci bezprzewodowej (Wi-Fi z modemu/routera kancelarii), zmień hasło administratora oraz wybierz w urządzeniu Wi-Fi sposób szyfrowania WPA2 AES. Jeśli z przyczyn technicznych nie możesz wybrać tego sposobu szyfrowania, to skorzystaj z WPA TKIP.

Dzięki tej praktyce zminimalizujesz ryzyko powodzenia ataku poprzez router kancelarii.

14.

Pracuj na danych klienta i sprawdzaj pocztę kancelaryjną wyłącznie na zaufanym urządzeniu, spełniającym wymagania bezpieczeństwa akceptowane przez Twoją kancelarię.

Dzięki tej praktyce ograniczysz ryzyko, że pewne dane klientów znajdą się na niezaufanych urządzeniach.

15.

Po odejściu pracownika z kancelarii upewnij się, czy wszystkie dostępy do danych klientów zostały mu zablokowane.

Dzięki tej praktyce ograniczysz ryzyko, że były pracownik będzie logował się do systemu kancelarii (np. CRM w chmurze) i uzyska nieautoryzowany dostęp do danych.

16.

Sprawdzaj czy pracownicy oraz systemy teleinformatyczne kancelarii są podatne na atak cyberprzestępców. Przeprowadzaj szkolenia.

Dzięki tej praktyce będziecie mogli lepiej chronić dane klientów w obrębie kancelarii. Warto przeprowadzić testy penetracyjne czy prowadzić szkolenia z bezpieczeństwa dla pracowników. Nie muszą być to szkolenia długie i stacjonarne. Mogą być to szkolenia online. Istotne by były wartościowe i skuteczne. Możesz także zamówić symulację cyberataku na kancelarię albo pracowników. Symulacja powinna być przeprowadzona w sposób niegroźny, to znaczy przy niewłaściwej reakcji powinien wyświetlać się komunikat informujący, że osoba zainfekowałaby właśnie urządzenie lub spowodowałaby zagrożenie albo incydent, a jednocześnie wyjaśniający skutki, jakie mogłyby nastąpić gdyby faktycznie do ataku doszło i krótkie wytyczne, jak można było ataku uniknąć (szczególnie warto przeprowadzić pod kątem potencjalnych ataków socjotechnicznych). Pamiętaj, że w większości przypadków najsłabszym ogniwem w bezpieczeństwie jest właśnie człowiek i jego działanie.

17. **Wymagaj by Twoi pracownicy stosowali się do zasad bezpieczeństwa, które wdrożysz w kancelarii.**

Dzięki tej praktyce wprowadzisz jednolity standard bezpieczeństwa i ochrony danych klientów kancelarii, a jednocześnie wypełnisz obowiązek prawny, według którego każdy pracownik powinien mieć upoważnienie do przetwarzania danych osobowych oraz potwierdzić zapoznanie się z zasadami określonymi w Polityce Bezpieczeństwa i stosowanie się do nich.

18. **Nie używaj tego samego hasła do kilku kont (np. konta pocztowego, konta dostępu do komputera, konta bankowego).**

Pamiętaj, że atakujący po poznaniu jednego hasła zyskuje dostęp do wielu zasobów, więc nie ułatwiaj mu tego.

19. **Ustaw ekran monitora w sposób uniemożliwiający dostęp do zasobów osobom postronnym.**

Nieupoważniona osoba korzystając z okazji może podejrzeć wpisywane dane. Możesz stosować folie ochronne, które uniemożliwiają podejrzenie z boku tego, co jest widoczne na ekranie komputera.

20. **Nie używaj domyślnych haseł i ustawień do administracji urządzeń.**

Domyślne hasła do urządzeń są dostępne w Internecie i jeżeli ich nie zmienimy, to osoby postronne mogą zmienić nam ustawienia naszych urządzeń nawet wbrew naszej woli. Domyślne ustawienia urządzeń są zwykle ustawieniami gwarantującymi wygodę, ale by zwiększyć bezpieczeństwo należy je zmienić.

21. **Odbieraj wydruki z drukarek od razu po ich wydrukowaniu. Pamiętaj o zabraniu z ksero lub faksu oryginałów dokumentów.**

Osoby postronne nie zapoznają się z dokumentami, które nie są dla nich przeznaczone.

II. Bezpieczeństwo urządzeń

Informacje wprowadzające (K. Pszczółkowski, B. Marek)

Prawnik, w swej codziennej pracy, korzysta z wielu urządzeń IT.

Najczęściej są to komputer stacjonarny, laptop, tablet, telefon komórkowy, pamięć zewnętrzna, drukarka, skaner, a także urządzenie pozwalające połączyć się z siecią Internet (np. router, modem). Coraz częściej do pracy grupowej lub pracy z klientem wykorzystywane są także aplikacje chmurowe, które umożliwiają pracownikom dostęp do danych z ich prywatnych urządzeń.

Urządzenia IT, które są wykorzystywane przez pracowników kancelarii, powinny być odpowiednio zarządzane i autoryzowane. Zalecane jest, by osoba odpowiedzialna za bezpieczeństwo w kancelarii lub prawnik zarządzający zdefiniował wymagania w zakresie bezpiecznego korzystania z urządzeń, zarówno tych należących do kancelarii jak i prywatnych, wykorzystywanych do pracy. Nie musi być jednak stosowana forma nadzoru nad pracownikiem obejmująca monitoring jego pracy. Chodzi raczej o posiadanie wiedzy na temat tego, jakie urządzenia są wykorzystywane do pracy, gdzie wykorzystuje się te urządzenia, kto ma prawo ich używać oraz na jakich zasadach można z nich bezpiecznie korzystać (np. czy kilku pracowników może pracować na jednym komputerze, jakie prywatne urządzenia pracownika mogą łączyć się z siecią wewnętrzną kancelarii, czy urządzenia służbowe można wynosić poza miejsce pracy, na jakich zasadach można korzystać z aplikacji chmurowych do pracy grupowej). Źródłami definiowania wymagań bezpieczeństwa są:

a) wymagania prawne (przepisy prawa);
b) wewnętrzne wytyczne i wymagania organizacyjne;
c) oczekiwania i potrzeby klientów;
d) szacowanie ryzyka bezpieczeństwa informacji – zdefiniowanie w jaki

sposób korzystanie z urządzeń IT może wpłynąć na bezpieczeństwo danych przetwarzanych w kancelarii oraz wybranie adekwatnych mechanizmów bezpieczeństwa, mających na celu minimalizację prawdopodobieństwa i skutków urzeczywistnienia się ryzyka.

Posiadanie urządzeń IT w kancelarii wiąże się często także z posiadaniem wsparcia technicznego, które ma zapewnić efektywne rozwiązywanie problemów związanych z danym systemem lub aplikacją, w określonym w umowie czasie. Niezbędne jest, by kancelaria miała zawartą umowę o świadczenie usług wsparcia technicznego, m.in. definiującą czas realizacji i naprawy (SLA), a także umowę powierzenia przetwarzanych danych osobowych i klauzulę poufności. Należy pamiętać o tym, że technik może mieć zdalny dostęp do urządzeń IT tylko za zgodą kancelarii, a jego działania powinny być możliwe do skontrolowania, tzn. wiemy co, gdzie i kiedy robił. Technik, w trakcie wykonywania swojej pracy, może zapoznać się z dokumentami, które zawierają dane osobowe lub inne dane o klientach, stąd też należy zachować szczególną ostrożność przy definiowaniu dla niego uprawnień dostępu.

2. Dlaczego warto szyfrować pliki, foldery, dyski? Jak to robić? (G. Cenkier, A. Ziaja)

Wszelkie pliki zawierające dane, które nie powinny zostać publicznie udostępnione, jak np. dane klienta, szczegóły sprawy i inne wrażliwe informacje, powinny być przesyłane do klienta w sposób szyfrowany. W przypadku jeśli w sposób pośredni osoba trzecia uzyska dostęp do szyfrowanego pliku, to nie będzie w stanie odczytać jego zawartości. Szyfrowanie jest w praktyce możliwe do złamania, jednak jest to bardzo ciężkie w realizacji, czasowo i kosztowo, ponieważ wymaga potężnych zasobów sprzętowych; należy jednak pamiętać, że bardzo ważnym aspektem jest tutaj dobre hasło, ponieważ w przypadku słabego hasła (np. słowa występującego w słowniku lub innego prostego do zgadnięcia np. „Lipiec2016") pomimo stosowania szyfrowania będzie istniało realne ryzyko odzyskania danych przez osobę niepowołaną.

Jest wiele metod szyfrowania. Warte uwagi prawnika są takie, które zapewniają:

a) szyfrowanie z poziomu systemu operacyjnego (dostępne dla wszystkich popularnych systemów operacyjnych takich jak Windows, OS X oraz Linux);

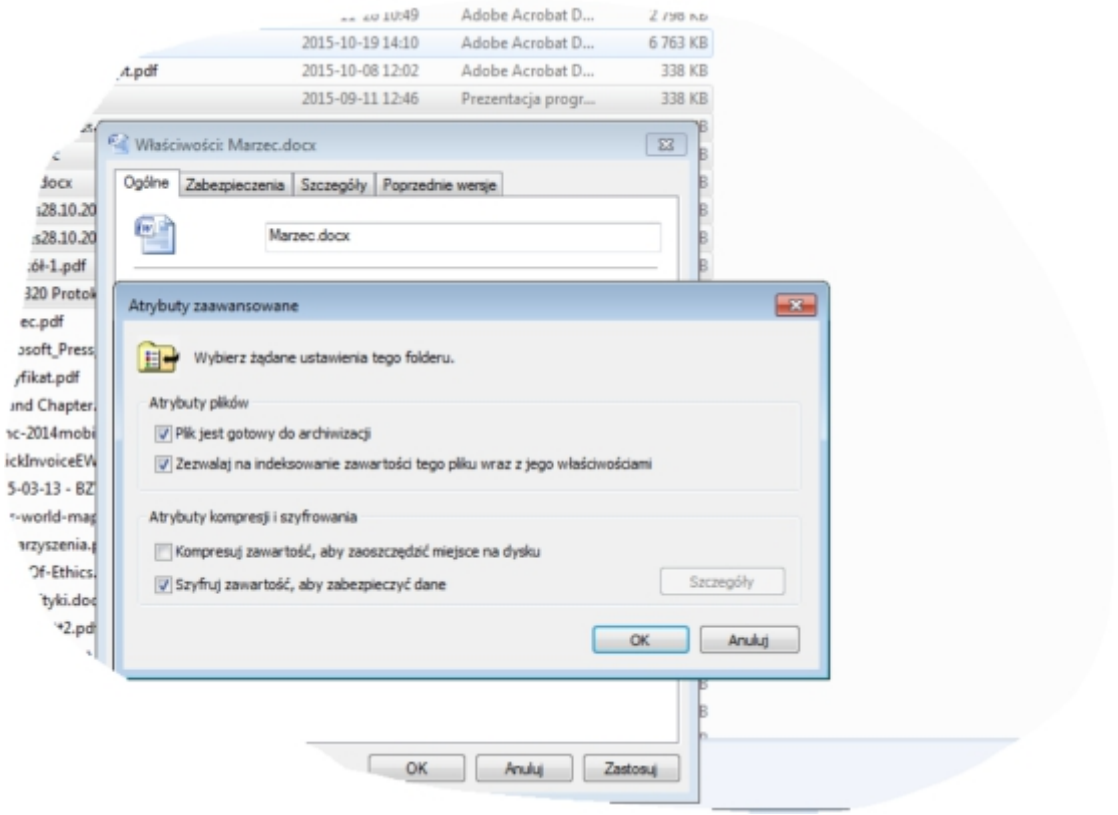
b) przesyłanie plików szyfrowanych PGP (GPG) – jednak jest to rozwiązanie bardzo mało spopularyzowane wśród osób nietechnicznych i może prowadzić do wielu problemów natury technicznej;

c) w pełni szyfrowane archiwum ZIP (łącznie z nazwami plików w archiwum) albo szyfrowanie na poziomie aplikacji (np. Word, Excel); hasło w takim wypadku nigdy nie powinno być wysyłane razem z plikami; najlepszą praktyką jest przesłanie do klienta hasła innym kanałem komunikacji, np. w postaci wiadomości SMS.

Szyfrowanie plików w systemie operacyjnym Windows

Najprostszy system szyfrowania plików to wykorzystanie w tym zakresie możliwości systemu operacyjnego, np. najczęściej stosowanego Windows i nie ma tu znaczenia wersja tego systemu. W jaki sposób to zrobić:

- otworzyć Eksploratora Windows;
- podświetlić plik, który chcemy zaszyfrować;
- wybrać Właściwości i opcję Ogólne, następnie Atrybuty zaawansowane;
- na liście atrybutów ostatnia opcja to właśnie szyfrowanie;
- po zaznaczeniu tej opcji i naciśnięciu klawisza Enter otworzy się okno dialogowe, gdzie wpisujemy dowolny ciąg znaków (liter i/lub cyfr), który będzie hasłem dostępu do dokumentu, które można wysłać do adresata wiadomości – klienta – oddzielną wiadomością lub SMS-em (rysunek na następnej stronie).



Szyfrowanie folderów w systemie operacyjnym Windows

Szyfrowanie folderów jest ważne m.in. w sytuacjach, gdy z jednego komputera korzysta np. kilku pracowników, a dokumenty zawierają dane chronione, np. teleadresowe klientów. Ważnym jest, aby w takiej sytuacji każdy z pracowników miał własny folder z dokumentami. Folder należy zaszyfrować w taki sam sposób jak w przypadku dokumentów, z tą różnicą, że podświetlamy folder i po naciśnięciu prawego klawisza myszki wybieramy opcję Właściwości.

Szyfrowanie dysku systemu operacyjnego Windows

Szyfrowanie dysku jest ważne w przypadku, gdy mamy do czynienia z komputerem przenośnym (laptopem), bo w ten sposób chronimy dane w przypadku kradzieży albo zgubienia. Jednocześnie pracując na komputerze stacjonarnym warto szyfrować dane ze względu np. na zawarte informacje. Dysk można zaszyfrować najlepiej przy wykorzystaniu specjalnego oprogramowania np. BitLocker, który szyfruje cały dysk i dostępny jest standardowo w każdej nowszej wersji systemu Windows. Oprogramowanie to

umożliwia normalną pracę z plikami, ale funkcja BitLocker będzie w tym czasie utrudniać przestępcom uzyskanie dostępu do plików systemowych, dzięki którym mogliby odkryć hasło użytkownika, lub do dysku, gdyby go wymontowali i zainstalowali w innym komputerze. Gdy do dysku szyfrowanego BitLocker'em zostają dodane nowe pliki, to są automatycznie szyfrowane. Pliki pozostają zaszyfrowane dotąd, dopóki są przechowywane na zaszyfrowanym dysku. Pliki kopiowane na inny dysk lub komputer są odszyfrowywane. Jeśli pliki są udostępniane innym użytkownikom, np. przez sieć, są one szyfrowane podczas przechowywania na szyfrowanym dysku, ale autoryzowani użytkownicy mają do nich dostęp. Instalację takiego oprogramowania najlepiej powierzyć informatykowi sprawującemu opiekę nad systemem informatycznym w kancelarii.

Szyfrowanie dysku systemu operacyjnego OS X (dotyczy komputerów Mac)

Analogicznie jak dla systemu Windows, gdzie nowe wersje posiadają wbudowane szyfrowanie BitLocker, komputery Mac z systemem OS X również posiadają wbudowaną możliwość szyfrowania dysku twardego komputera.

W przypadku komputerów marki Apple dysk można zaszyfrować wybierając kolejno:

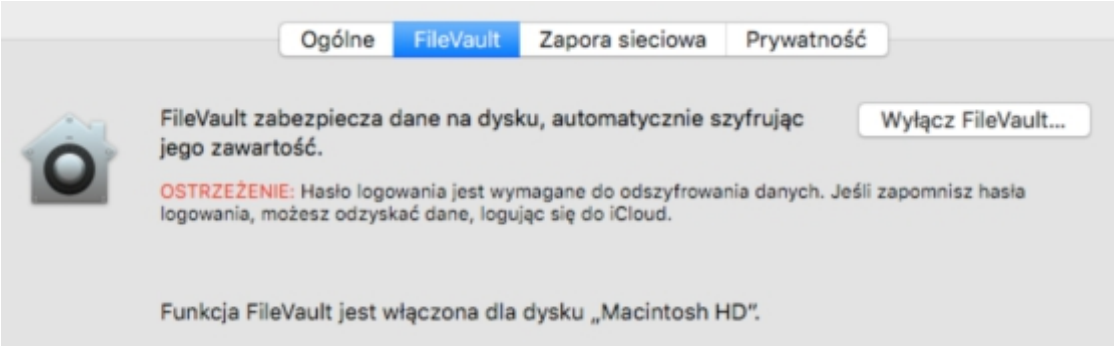
Logo Apple (lewy górny róg) >

Preferencje systemowe >

Ochrona i prywatność >

FileVault >

Włącz FileVault.



Szyfrowanie dysku systemu operacyjnego Linux Ubuntu

Dzisiejsze systemy operacyjne z rodziny Debian (w tym Ubuntu) również posiadają wbudowaną możliwość szyfrowania. W tym celu należy pamiętać, aby w trakcie instalacji systemu wybrać opcję szyfrowania, najlepiej całego dysku (a nie tylko katalogu roboczego użytkownika). Jeśli w trakcie instalacji systemu nie została wybrana powyższa opcja, włączenie szyfrowania na tym etapie nie jest proste dla osoby nietechnicznej i powinno być zlecone informatykowi.

Szyfrowanie urządzeń przenośnych (telefonów komórkowych, tabletów)

W dzisiejszych czasach nawet na telefonach komórkowych posiadamy bardzo wiele istotnych danych np. skrzynkę pocztową, która posiada załączniki czy zdjęcia (np. akt sprawy). Dlatego bardzo ważne jest również szyfrowanie urządzeń przenośnych. Obecnie wszystkie popularne urządzenia tego typu posiadają wbudowaną możliwość szyfrowania zawartości. Z uwagi na różnorodność urządzeń i systemów operacyjnych w publikacji tej odstąpiono od szczegółowej instrukcji jak włączyć szyfrowanie w takich urządzeniach, jednak w większości przypadków taka funkcja będzie możliwa do wyszukania w ustawieniach bezpieczeństwa danego urządzenia.

3. Jak i po co zmienić hasło routera / komunikacji Wi-Fi? (G. Cenkier)

Spowolnienie pracy sieci bezprzewodowej (Wi-Fi), co widać choćby poprzez fakt, że zarówno pocztę elektroniczną jak i strony internetowe pobiera się dłużej, może być sygnałem, że ktoś kradnie Twoje łącze! Poza oczywistą stratą, jaką jest wolniejszy Internet, można mieć problemy z powodu działań swojego sąsiada, np. zakupów w sieci na rachunek Twojej kancelarii. Inną przyczyną może być system zabezpieczeń. Sposób ochrony dostępu do sieci bezprzewodowej wpływa nie tylko na jej bezpieczeństwo, ale również na szybkość jej pracy.

Pełną prędkość w najczęściej stosowanym standardzie 802.11n osiągniemy tylko wtedy, gdy zastosujemy zabezpieczenie WPA2 oraz szyfrowanie AES. Ważne jest również samo hasło. Jego długość i złożoność nie wpływa na szybkość transmisji, ale musi być możliwie skomplikowane (najlepiej co najmniej 10 znaków zawierających małe i duże litery, cyfry i symbole), aby maksymalnie utrudnić włamanie do naszej sieci.

Jak sprawdzić, czy do naszej sieci nikt się nie loguje, to stosunkowo proste. Należy uruchomić przeglądarkę internetową i zalogować się do panelu administracyjnego routera – zazwyczaj jest on dostępny pod adresem http://192.168.2.1 lub http://192.168.1.1.

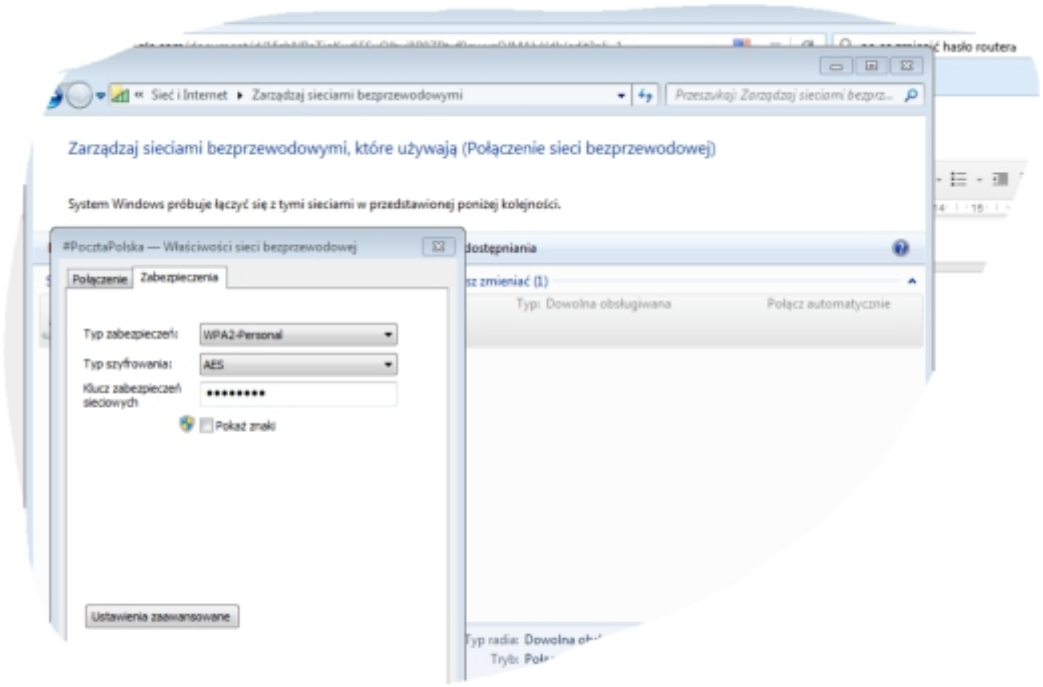
Nazwa i hasło to *admin* i *admin*, jeśli jest inaczej to należy obejrzeć router i znaleźć przyklejoną kartkę z nazwą i hasłem. Po zalogowaniu w zależności od routera wybieramy:

- **D-Link**: z poziomego menu wybieramy **Tools** i w polach **Admin Password** dwukrotnie podajemy nowe hasło. Klikamy na **Save Settings**.
- **Linksys**: z poziomego menu wybieramy **Administration**, a następnie w polu **Router Password** i polu poniżej dwa razy wpisujemy nowe hasło. Klikamy na **Save Settings**.
- **TP-Link**: w bocznym menu wybieramy **System Tools**, a następnie nieco niżej klikamy na **Password**. Podajemy teraz stary login i hasło oraz poniżej wprowadzamy nową nazwę użytkownika i dwa razy hasło. Zmianę zatwierdzamy, klikając na **Save**.

W kolejnym kroku należy sprawdzić i/lub skonfigurować zabezpieczenia sieci Wi-Fi, ustawiając WPA2 z szyfrowaniem AES.

- **D-Link**: w menu bocznym wybieramy pozycję **Wireless Settings** i klikamy na **Manual Wireless Network Setup**. Wybieramy typ zabezpieczenia **Security Mode: WPA-Personal**, a nieco niżej precyzujemy typ ochrony **WPA Mode: WPA2 Only** i ustawiamy szyfrowanie **Cipher Type: AES**.
  W pole **Pre-Shared Key** wpisujemy hasło i klikamy na **Save Settings**.

- **Linksys**: w menu poziomym klikamy na **Wireless**, a następnie na **Wireless Security**. Z listy wybieramy typ zabezpieczenia **Security Mode: WPA2 Personal** i wpisujemy hasło chroniące naszą sieć **Passphrase: haslo_do_sieci_123**. Klikamy na przycisk **Save Settings**.
- **TP-Link**: w bocznym menu klikamy na **Wireless**, a następnie na **Wireless Settings** (w nowszych modelach na **Wireless Security**). Z listy wybieramy (w nowszych modelach zaznaczamy) typ **Security Type: WPA-PSK/WPA2-PSK**, następnie dokładnie definiujemy rodzaj zabezpieczenia **Security Option: WPA2-PSK**, ustawiamy szyfrowanie **Encryption: AES** i wpisujemy hasło **PSK Passphrase: haslo_do_sieci123**. Klikamy na **Save**.



Inna metoda to uruchomienie wiersza poleceń z poziomu systemu operacyjnego i wpisanie komendy ipconfig/all. Wśród pojawiających się informacji znajdujemy słowa Brama domyślna – będzie tam podany adres Twojego routera.

Większość routerów udostępnia informacje o sprzęcie działającym w sieci lokalnej. Należy poszukać sekcji lub zakładki nazwanej Podłączone urządzenia, Device List lub czegoś podobnego i tam można sprawdzić, jakie urządzenia są aktywne. Warto pamiętać, że smartfony i tablety są też widoczne. Co jakiś czas należy uruchomić instrukcję ipconfig/all, aby sprawdzić, czy sąsiad nie jest aktywnym klientem naszej sieci lokalnej.

4. Zasady dotyczące haseł (K. Pszczółkowski, B.Marek)

Wszyscy pracownicy kancelarii posiadający dostęp do urządzeń IT, wykorzystywanych do pracy zawodowej tj. komputerów stacjonarnych, laptopów, tabletów, telefonów komórkowych, pamięci zewnętrznych i urządzeń pozwalających połączyć się z siecią Internet (np. router, modem), powinni uwierzytelniać się (logować) do nich przy użyciu hasła. Polityka dotycząca zarządzania hasłami powinna zawierać następujące wymagania:

1. Hasło powinno składać się z minimum 3 rodzajów znaków tj. liter małych i dużych, cyfr i/lub znaków specjalnych (@#$%).

2. Minimalna długość hasła akceptowanego powinna wynosić 10 znaków.

3. Zmiana hasła do każdego urządzenia IT powinna być przeprowadzana co najmniej raz na 90 dni, a w przypadku systemów przetwarzających dane osobowe – co najmniej raz na 30 dni (jednak po 25 maja 2018 r. częstotliwość zmiany haseł będzie mogła być inna i będzie zależeć od oceny ryzyka dokonanej przez administratora danych).

4. Hasło początkowe (startowe) do urządzenia IT administrator systemu przekazuje użytkownikowi osobiście. Użytkownik urządzenia IT przy pierwszym logowaniu zobowiązany jest do natychmiastowej zmiany hasła początkowego zgodnie z obowiązującymi regułami tworzenia haseł dla użytkowników.

5. Nowe hasło nie może być takie samo jak co najmniej 5 poprzednio użytych haseł.

6. Hasło musi być przechowywane w postaci niejawnej, dozwolone metody to silne szyfrowanie lub użycie funkcji skrótu. Administrator systemu nie powinien znać hasła użytkownika.

7. W przypadku utraty hasła (gdy np. użytkownik zapomniał hasła), administrator systemu powinien zrestartować hasło, przekazując użytkownikowi nowe hasło początkowe (startowe) do urządzenia IT, które natychmiast po otrzymaniu powinno zostać zmienione przez użytkownika.

8. Administrator systemu powinien się upewnić czy osoba, która wnioskuje o zrestartowanie hasła jest osobą, za którą się podaje.

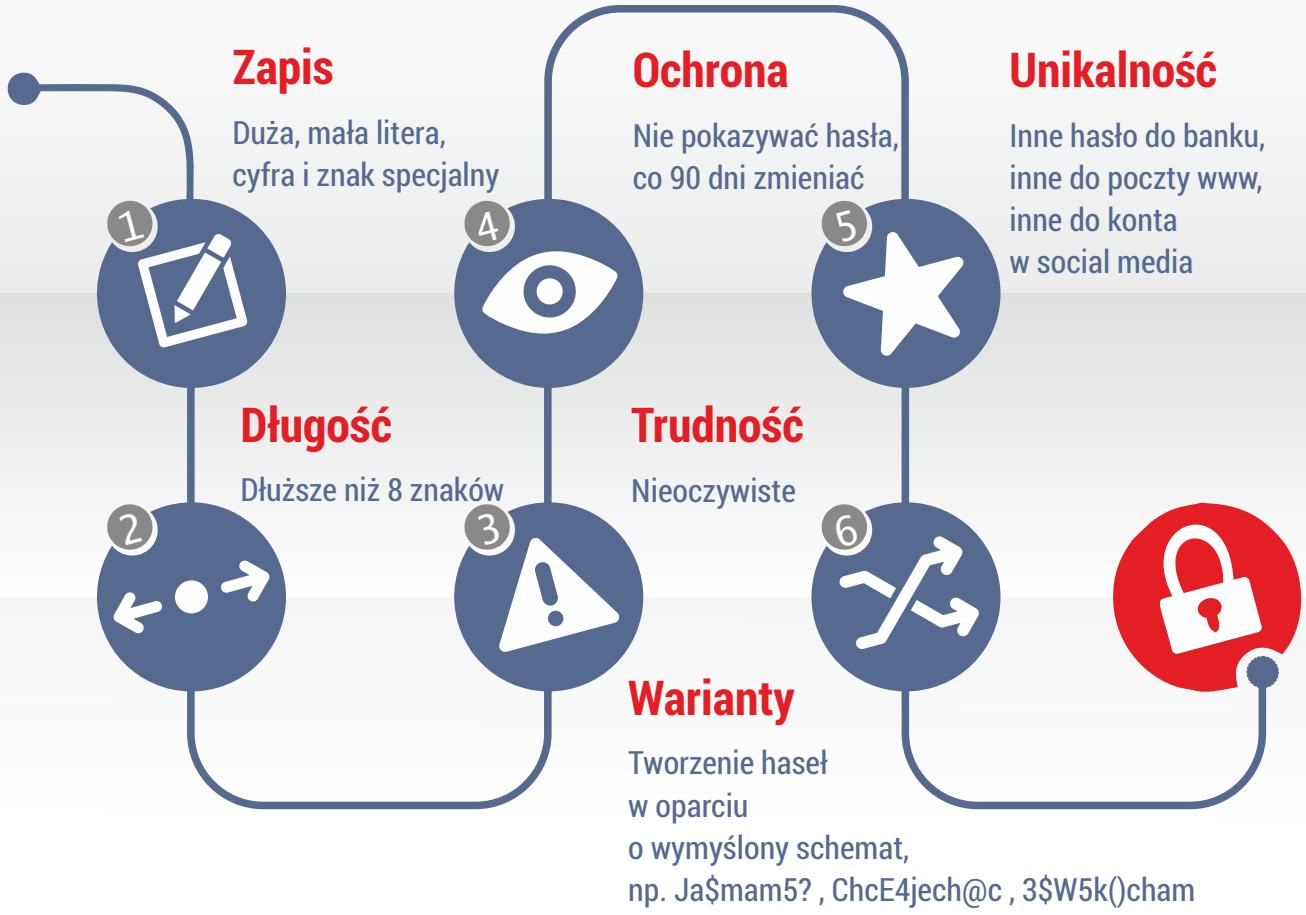
9. Konto użytkownika powinno być blokowane po kilku nieudanych próbach zalogowania się do systemu (nie mniej niż 3).

10. W przypadku braku aktywności użytkownika powinna być ustawiona blokada sesji / komputer powinien przechodzić w stan uśpienia.

11. Użytkownicy są zobowiązani do utrzymywania swoich haseł w tajemnicy. Nie wolno zapisywać haseł na papierze, w pliku lub urządzeniu przenośnym, nie wolno ich również przekazywać administratorowi systemu, przełożonemu lub osobie zastępującej w czasie nieobecności.

12. W przypadku podejrzenia możliwości ujawnienia hasła użytkownik zobowiązany jest je zmienić.

Jak stworzyć dobre hasło?



5. Jak wyłączyć skradziony telefon komórkowy? (G. Cenkier)

Aby sprawdzić numer seryjny swojego telefonu komórkowego, wciśnij następujące klawisze w telefonie:

***#06#**

15-cyfrowy kod (IMEI) pojawi się na ekranie. Możesz też sprawdzić kod na kartonie Twojego telefonu (zwykle w formie naklejki).

Ten numer jest unikalny dla Twojego telefonu. Zapisz go i schowaj gdzieś bezpiecznie.

Gdy telefon zostanie skradziony, możesz zadzwonić do swojego providera (dostawcy usług telefonicznych) i podać mu ten kod. Najpierw jednak powinieneś zgłosić fakt kradzieży na policji.

Operator będzie miał możliwość zablokować Twój telefon nawet jeśli złodziej zmieni kartę SIM. Telefon będzie całkowicie bezużyteczny.

Prawdopodobnie nie otrzymasz swojego telefonu z powrotem, ale przynajmniej wiadomo, że ktoś, kto go ukradł, nie będzie mógł z niego korzystać ani sprzedać go dalej.

Jeśli wszyscy ludzie by to robili, złodzieje nie mieliby powodu, by kraść telefony komórkowe, gdyż byłyby one bezużyteczne.

Powyższe rozwiązanie działa na każdym systemie operacyjnym telefonu.

6. Lista kontrolna – jak dbam o bezpieczeństwo urządzeń, na których przetwarzam dane klientów? (B. Marek)

Zaznacz odpowiedź TAK albo NIE przy każdej czynności:

	WYKONYWANA CZYNNOŚĆ	TAK / NIE
1.	Urządzenie jest zabezpieczone przed dostępem osób nieupoważnionych.	
2.	Urządzenie ma połączenie z Internetem tylko z zaufanych punktów (np. korporacyjna sieć WiFi, Internet mobilny podpinany tylko do urządzeń korporacyjnych).	
3.	Urządzenie ma zaszyfrowaną zawartość co najmniej na poziomie folderów.	
4.	Wykonuję regularnie kopię bezpieczeństwa zawartości urządzenia.	
5.	Nie pobieram na urządzenie jakichkolwiek plików z niezaufanych stron, tj. innych niż oficjalne strony producenta lub sprawdzone aplikacje w markecie.	
6.	Przed oddaniem urządzenia do serwisu czyszczę zawartość dysku lub oddaję informatykowi, z którym mam podpisaną umowę powierzenia przetwarzania danych osobowych albo ma on upoważnienie do przetwarzania danych.	
7.	Utylizuję urządzenie po uprzednim trwałym usunięciu danych zapisanych na dysku albo fizycznie jest niszczony dysk. Robię to samodzielnie albo pomaga mi informatyk, z którym mam podpisaną umowę powierzenia przetwarzania danych osobowych albo ma on upoważnienie do przetwarzania danych.	

Jeżeli zaznaczyłeś co najmniej jedną odpowiedź NIE – oznacza to, że powinna zostać przeprowadzona rewizja Systemu Zarządzania Bezpieczeństwem Informacji w kancelarii.

III. Usługi chmurowe dla prawników (B. Janiuk i M. Michalski)

1. Informacje wprowadzające

Aktualnie na świecie rośnie popularność "cloud computing" co oznacza "pracę z danymi w zdecentralizowanym środowisku" nazywanym potocznie chmurą, która pozwala na korzystanie z najnowszych rozwiązań informatycznych bez ponoszenia wydatków inwestycyjnych na zakup infrastruktury, licencji oraz jej utrzymanie.

Z "chmur" korzystają wszyscy, czyli duże i małe firmy, instytucje publiczne oraz osoby fizyczne (Public cloud, Private cloud, Hybrid). Z uwagi na koszty, najczęściej wybierane są rozwiązania oparte o chmurę publiczną, rzadziej spotykane są rozwiązania hybrydowe. Na chmury prywatne decydują się najczęściej bogatsze firmy i instytucje o dużych potrzebach.

Korzystanie z rozwiązań chmury powoduje, iż odpowiedzialność za poszczególne elementy infrastruktury systemu, aplikacje i obsługę informatyczną spoczywa na dostawcy zależnie od wybranego modelu usług (IaaS, PaaS, SaaS, CaaS, IPaaS).

Dzięki elastyczności modelu chmury użytkownicy mają dostęp do zasobów firmowych lub prywatnych z dowolnego miejsca na świecie za pośrednictwem urządzenia posiadającego dostęp do Internetu, jak również istnieje możliwość dopasowania pakietu usług do bieżących potrzeb danego użytkownika.

Przykładami powszechnie znanych usług w chmurze są: przechowywanie muzyki i zdjęć na Cloud Apple, Picassa, dokumentów na Google, udostępnianie plików przez Dropbox.

Nie można jednoznacznie stwierdzić, iż korzystanie z takich usług jest dobrym albo złym rozwiązaniem, gdyż nie mamy pełnej kontroli nad naszymi danymi i istnieje ryzyko ataku hakerskiego na te dane, znajdujące się na serwerach

danego podmiotu, jak również możliwość awarii skutkującej czasową niedostępnością albo całkowitą utratą danych. Jednakże w tym miejscu należy zwrócić uwagę, iż każdego roku firmy, dostarczające usługi w chmurze, zwiększają środki finansowe na poszukiwanie najlepszych zabezpieczeń, które wraz z całodobowym nadzorem pracowników usługodawcy minimalizują ryzyko uszkodzenia plików bądź możliwość niepowołanego dostępu do plików.

2. Zagrożenia

Zanim kancelaria zdecyduje się na korzystanie z usług chmurowych, powinna zastanowić się nad kosztami i zyskami, jakie przynosi korzystanie z takiego rozwiązania.

W szybkim rozrachunku takie rozwiązanie wydaje się jak najbardziej uzasadnione ekonomicznie, wręcz w niektórych przypadkach darmowe (!). Ale czy jest takie na pewno?

Poniżej znajduje się kilka najczęściej wskazywanych zagrożeń związanych z przetwarzaniem danych w chmurze:

- utrata kontroli nad danymi (trudność ochrony danych)
- ograniczone możliwości migracji (utrudniony eksport danych, niezgodność formatów)
- brak izolacji od danych innych klientów
- publicznie dostępny interfejs zarządzający (poprzez Internet)
- niepewność dotycząca usunięcia danych (brak kontroli nad nośnikami)
- niejasne sposoby licencjonowania
- nieautoryzowany dostęp do danych firmowych i klienckich
- przerzucanie/zrzucanie odpowiedzialności za bezpieczeństwo i integralność danych pomiędzy klientem i usługodawcą
- różne poziomy i rodzaje oferowanego wsparcia technicznego.
- stabilność parametrów świadczonej usługi (SLA)

- stabilność i długotrwałość prowadzenia działalności przez usługodawcę
- brak dostępu do danych w chmurze, w tym brak możliwości szybkiego odzyskania danych lub niemożność ich odzyskania
- brak pełnego zrozumienia sposobu funkcjonowania chmury
- brak spójnej, jasnej i otwartej polityki komunikacji z klientami
- niekompatybilność Planów Ciągłości Działania (BCP) i Procedur Awaryjnych (DR) lub ich niski poziom
- brak zgodności prawnej poszczególnych krajów, na terenie których odbywa się przetwarzanie danych.

Katalog zagrożeń godzących w bezpieczeństwo danych przechowywanych w chmurze wciąż jest zbiorem otwartym.

3. Dobre praktyki – czym warto kierować się, jeśli kancelaria ma przetwarzać dane w chmurze.

Pamiętaj – jako kancelaria prawna przetwarzasz szereg informacji podlegających prawnej ochronie i masz obowiązek je chronić.

Sprawdź czy dane, które chcesz przetwarzać w chmurze, mogą być tak przetwarzane. Polskie przepisy prawne przewidują ponad 70 rodzajów danych i informacji podlegających ochronie. Informacje te muszą być chronione zgodnie z zasadami określonymi w przepisach prawnych. Przetwarzając dane w chmurze musisz się liczyć z tym, że dany rodzaj informacji może być nielegalny w innym kraju lub też informacje, dane oraz sposoby ich ochrony mogą być inne. W przypadku gdy strony zawierając umowę nie dokonały wyboru prawa (w umowie jest brak klauzuli wyboru prawa), prawem właściwym będzie prawo państwa, w którym siedzibę ma dostawca usług w chmurze. Warto zasygnalizować, że na gruncie przepisów prawa przekazanie danych do chmury stanowi ich powierzenie i powinno być odpowiednio uregulowane w umowie.

Wybieraj zaufanych i wiarygodnych dostawców usług.

Wybieraj tylko zaufanych, znanych i sprawdzonych dostawców usług chmurowych. Pamiętaj, że darmowa usługa nie istnieje. Owszem, korzystający z tej usługi nie ponosi kosztów bezpośrednich, jednakże firmy świadczące w regulaminach usług wprowadzają częstokroć zapisy, które pozwalają np. na śledzenie preferencji użytkownika oraz analizują rodzaje i typy zamieszczanych plików. W skrajnych przypadkach osoba zamieszczająca dane zezwala, akceptując regulamin, na wykorzystanie treści dokumentów lub też ich upublicznienie.

Zabezpieczaj dane przed dostępem osób nieuprawnionych.

Przed wysłaniem do chmury danych, które mają zostać zachowane w poufności, zaszyfruj te dane. Szyfrowanie danych niezależnie od miejsca ich przechowywania zawsze zwiększa bezpieczeństwo ich przechowywania oraz zapewnia ich poufność.

Zabezpieczaj informacje dotyczące dostępu do danych.

Nie ujawniaj kluczy szyfrujących, nazw użytkowników i haseł do usług chmurowych i zabezpieczaj je. Tak samo jak w przypadku danych gromadzonych lokalnie – ich ujawnienie lub pozyskanie przez osoby nieuprawnione może Ciebie i Twoich klientów narazić na utratę danych i poważane straty finansowe oraz wizerunkowe.

Przeczytaj uważnie umowę określającą podmioty świadczenia usług.

Umowa to nie wszystko – zapoznaj się z załącznikami oraz poszczególnymi regulaminami poszczególnych usług. Przede wszystkim zwróć uwagę gdzie i na jakim sprzęcie przetwarzane są dane, kto nimi zarządza (firma, siedziba, kraj, miejsce rozstrzygania sporów sądowych), gdzie jest fizycznie zainstalowane oprogramowanie, z którego korzystamy (firma, siedziba, kraj, opłaty za korzystanie, zasady prywatności dokumentów, prawo licencyjne danego kraju), gdzie gromadzone i przetwarzane są jego dane (firma, siedziba, kraj – strefa czasowa, zasady prywatności danych, kto ma dostęp do danych).

Zapoznaj się szczegółowo z zasadami dostawy usług określonymi w umowie oraz regulaminie.

Szczegółowo zapoznaj się ze wszystkimi dokumentami opisującymi usługę; to one będą podstawą do dochodzenia późniejszych roszczeń. Regulaminy usług są bardzo często integralną częścią zawieranych umów. W nich to najczęściej zawierane są wszystkie najważniejsze zapisy związane z bezpieczeństwem danych, zasadami dostępu i prawami własności oraz, w zależności od wybranej opcji, mogą w znaczący sposób wpływać na wybraną usługę.
Zwróć uwagę jakie inne usługi są wykorzystywane, aby dostarczyć zamawianą usługę. Należy zwrócić szczególną uwagę na poziom szyfrowania danych transmisji (uwaga: w niektórych krajach zabronione jest przesyłanie i składowanie zaszyfrowanych danych lub też istnieje gwarancja dostępu do danych przez służby specjalne), na to, czy i na jakich zasadach jest wykonywana kopia zapasowa (częstotliwość tworzenia kopii, czas odtwarzania, zakres podlegający zabezpieczeniu) oraz dostępność całodobowej obsługi (usługa może być świadczona przez podmiot znajdujący się w innej strefie czasowej).

Zabezpiecz się przed utratą dostępu do danych.

Dostęp do danych gromadzonych w płatnych usługach chmurowych jest możliwy tylko po uregulowaniu zobowiązań finansowych wobec dostawcy. Przy opóźnieniach dostęp ten może zostać ograniczony, dane mogą zostać przejęte przez usługodawcę lub dostęp do nich całkowicie wyłączony, a dane trwale usunięte. Zastanów się nad przechowywaniem kopii danych w innym miejscu (usłudze, nośniku).

Kontroluj informacje które przesyłane są do chmury.

Wyłącz domyślne przekazywanie danych i dokumentów do usług chmurowych. Większość oferowanych obecnie urządzeń posiada domyślnie zainstalowane oprogramowanie do gromadzenia danych w chmurze i oferuje aktywację tych usług podczas konfiguracji wstępnej urządzenia. Nie uruchamiaj pochopnie tych usług, przejrzyj urządzenie i oprogramowanie oraz zdecyduj co i gdzie będziesz przechowywał.

Zachowaj w poufności informacje i dane przesłane do chmury

Przesyłając dane do chmury licz się z tym, iż inne osoby będą mogły uzyskać do nich w jakiś sposób dostęp – zabezpiecz je. Jeżeli chcesz mieć pewność, że nikt nieuprawniony nie zapozna się z treściami, które zamieściłeś w chmurze, zaszyfruj dane, które chcesz przesłać i korzystaj z bezpiecznej (szyfrowanej) transmisji danych.

Korzystaj tylko z zaufanych urządzeń dostępowych.

Przesyłając dane, korzystaj tylko z urządzeń, które są pod Twoją kontrolą. Nie korzystaj z dostępu do chmury na urządzeniach dostępnych publicznie lub udostępnionych przez inne osoby oraz unikaj publicznych punktów dostępowych (hotspot). Urządzenia te mogą posłużyć przechwyceniu Twoich danych.

Świadomie korzystaj z usług.

Jeżeli nie posiadasz wiedzy lub nie rozumiesz działania usług chmurowych – nie korzystaj z nich lub poproś kogoś o wyjaśnienie z czym masz do czynienia. Nieostrożne lub nieświadome korzystanie z usług może doprowadzić do utraty danych własnych oraz klientów, ujawnienia ich treści oraz poważnych strat finansowych i długotrwałych procesów sądowych, także poza granicami Polski.

W chmurze nie ma anonimowości i prywatności.

Umieszczaj w chmurze jawnie tylko te informacje, które takimi mogą być; umieszczając je także identyfikujesz siebie mogą one posłużyć innym w złych celach. Każda informacja wprowadzona do przestrzeni publicznej jest szybko powielana oraz udostępniana przez inne serwisy (Facebook, LinkedIn). Podobnie Twoje informacje mogą być wykorzystane (patrz: regulaminy darmowych usług) jako baza danych dla innych użytkowników chmury. Łącząc się z usługami w Internecie identyfikujesz siebie i swoje urządzenia (IP, numery seryjne, informacje o systemie i inne). Nie informuj wszystkich dookoła co, gdzie i z kim robisz oraz czego używasz – czytają to także przestępcy i Twoja konkurencja.

Stosuj dobre praktyki.

Korzystając z chmury stosuj także pozostałe dobre praktyki, z którymi zapoznasz się w tym dokumencie. Zdrowy rozsądek i spokojne podejście do każdego tematu sprawdza się zarówno w świecie rzeczywistym, jak i wirtualnym.

IV. Wymiana informacji z Klientem

1. Dlaczego przesyłanie wiadomości przez formularz na stronie kancelarii po HTTPS jest bezpieczniejsze niż po HTTP? (M. Hornowski)

Wszystkie przeglądarki jako podstawę obsługują protokół HTTP. Protokół ten nie jest jednak bezpieczny, bo pozwala np. podsłuchać osobom trzecim, jakie informacje są wysyłane przez stronę i je podmienić. Na stronach kancelarii powinien być stosowany HTTPS, czyli szyfrowana wersja protokołu HTTP. W ten sposób przesyłane dane będą szyfrowane, a co za tym idzie bezpieczniejsze. Co więcej – strona będzie lepiej indeksowana w wynikach wyszukiwania.

Początkowo HTTPS był używany do ochrony transakcji bankowych, ale z czasem rozpowszechnił się też na inne dziedziny życia społecznego i gospodarczego. W tej chwili wiele sklepów internetowych korzysta z certyfikatów SSL i ich strony są szyfrowane, i zaczynają się od przedrostka HTTPS. Czy strona Twojej kancelarii także zapewnia wiarygodność na takim poziomie?

Oto najważniejsze cechy, które powinny skłonić do wybrania protokołu HTTPS:

- zwiększenie wiarygodności i uwierzytelnienie odwiedzanej strony (np. certyfikat może potwierdzać, że znajdujemy się na stronie kancelarii i wyświetlać w certyfikacie informacje o podmiocie; w ten sposób klienci czują się bezpiecznie przy przesyłaniu informacji i komunikowaniu się z kancelarią);
- poufność (tylko my i druga strona wiemy, jakie dane przesyłamy, oczywiście o ile strona nie zawiera podatności lub złośliwego kodu);
- integralność przesyłanych danych (nikt nie podmieni przesyłanych danych w momencie ich przesyłania).

Warto wiedzieć, że HTTPS pozwala, mówiąc najogólniej, na szyfrowanie transmisji, co jest niezbędne w przypadku prawników.

Z technicznego punktu widzenia szyfrowanie tego typu polega na istnieniu dwóch kluczy do szyfrowania komunikacji – klucza "publicznego" i klucza "prywatnego". Cokolwiek jest zaszyfrowane kluczem publicznym, może być odczytane tylko przy użyciu klucza prywatnego i na odwrót.

Jak sama nazwa wskazuje, klucz prywatny powinien być dobrze strzeżony przez właściciela i tylko przez niego używany. Natomiast klucz publiczny może być wysłany do każdego, kto potrzebuje odszyfrować wiadomość zaszyfrowaną kluczem prywatnym lub chce wysłać sekretną wiadomość tylko do właściciela klucza prywatnego.

Certyfikaty w Internecie to jakby "poświadczone wizytówki". Kiedy żądamy połączenia HTTPS z wybraną stroną w sieci, rozpoczyna się wymiana pakietów danych zwana SSL handshake. W efekcie strona sieci wysyła do naszej przeglądarki swój certyfikat. Zawiera on klucz publiczny niezbędny do nawiązania szyfrowanego połączenia oraz informacje pomocnicze do skutecznego i sprawnego szyfrowania transmisji. Certyfikaty są poświadczone przez zaufaną stronę trzecią.

Jeżeli przeglądarka uzna, że połączenie HTTPS jest bezpiecznie zestawione, to na pasku adresu pojawia się symbol kłódki. W nowych przeglądarkach zmienia się też na zielony kolor paska adresu.

Jeżeli chcesz skorzystać z HTTPS, skontaktuj się z informatykiem czy dostawcą usługi hostingowej – czyli tam gdzie masz swoją stronę www.

2. Jakie pliki warto szyfrować przy przesyłaniu ich do klienta? (B. Marek)

Do klientów przesyłane są różne rodzaje dokumentów, które w postaci elektronicznej mają formę plików o rozszerzeniach “.doc” / “.docx” / “.pdf” etc. Można podzielić je na dwie grupy: pliki małej wagi i pliki o większym znaczeniu dla klienta. Kryterium powinno być ustalenie czy w razie wycieku informacji

zawartych w danym pliku przy ich przesyłaniu i zapoznaniu się z nimi przez osoby niepowołane klient poniesie szkodę. Mając to na uwadze pliki o większym znaczeniu warto, a nawet trzeba szyfrować. Pliki przesyłane pomiędzy serwerem poczty kancelarii a poczty klienta przekazywane są, co do zasady, "tunelem", który nie jest zabezpieczony. Tylko w wyjątkowych przypadkach, gdy serwery pocztowe są odpowiednio skonfigurowane, jest inaczej. Warto pamiętać także, że fakt, iż serwer poczty kancelarii wymaga bezpiecznego połączenia SSL nie oznacza, że wysyłane wiadomości e-mail wraz z załącznikami są zabezpieczone.

Oferty dotyczące usług kancelarii nie muszą być szyfrowane, podobnie jak proste dokumenty mające na celu pokazać pewien wzornik dla klienta (np. opinie na temat interpretacji przepisów) albo dokumenty zanonimizowane tj. pozbawione treści zawierających informacje na temat sprawy klienta. Jednak wszelkie inne dokumenty warto przekazywać drogą elektroniczną – np. e-mailem lub umieszczając na serwerze albo w aplikacji chmurowej – w postaci zaszyfrowanej.

W przypadku korzystania z rozwiązań chmurowych i np. dedykowanej aplikacji chmurowej, wielu prawników może zastanawiać się, po co szyfrować dokumenty. Jest to niezbędne, gdyż dostawca usługi nie jest zobligowany do zachowania tajemnicy zawodowej i jest zobowiązany udostępnić dane na żądanie organów ścigania. Najistotniejsze jednak jest to, że wśród jego pracowników mogą znaleźć się osoby, które mogą mieć niepowołany dostęp do informacji i uczynić szkodę kancelarii lub jej klientom. Z tych powodów wszelkie pliki, umieszczane na serwerach lub w dedykowanych aplikacjach do komunikacji z klientem, powinny być szyfrowane, o ile są to pliki o większym znaczeniu. Wyjątkiem są rozwiązania IT gdzie kancelaria korzysta wyłącznie z zewnętrznej architektury informatycznej, a aplikacja została napisana dla kancelarii i wyłącznie kancelaria jest w posiadaniu kluczy umożliwiających odszyfrowanie zawartości danych gromadzonych w aplikacji.

O tym, w jaki sposób szyfrować pliki, by później przesłać je za pomocą np. e-maila, możesz przeczytać w rozdziale 4 pkt. b.

3. W JAKI SPOSÓB PRZESYŁAĆ WIĘKSZE ILOŚCI PLIKÓW? (B. MAREK)

Przy przesyłaniu dokumentów znajdujących się w wielu plikach, warto skorzystać z dedykowanego rozwiązania wdrożonego w kancelarii. Może być to rozwiązanie komercyjne albo typu open source do przesyłania plików. W ten sposób na serwer kancelarii będą przesyłane informacje od Klienta oraz odwrotnie, bez pomocy chmury publicznej i, tym samym, rozwiązań szczególnie niezalecanych do stosowania w kancelarii. Jeżeli decydujemy się na przesyłanie plików za pomocą serwera kancelarii pamiętajmy, że dane w transporcie jak i w spoczynku powinny być szyfrowane. Oznacza to tym samym, że należy zaszyfrować komunikację oraz chronić dostęp do danych fizycznie znajdujących się na serwerze.

Niezbędne jest także, by po zapoznaniu się z danymi skopiować je na nośnik, za pomocą którego wykonywana jest regularna kopia bezpieczeństwa, i trwale usunąć je z serwera. W ten sposób minimalizujemy ryzyko, że po włamaniu na serwer albo ustaniu jego pracy dane te nie zostaną w jakikolwiek sposób skopiowane, gdyż nie będą one w tym miejscu fizycznie dostępne.

4. LISTA KONTROLNA – JAK DBAM O WYMIANĘ INFORMACJI Z KLIENTAMI? (B. MAREK)

Zaznacz odpowiedź TAK albo NIE przy każdej czynności:

	WYKONYWANA CZYNNOŚĆ	TAK / NIE
1.	Strona kancelarii, na której znajduje się formularz kontaktowy jest szyfrowana (zaczyna się od https).	
2.	Korzystam z poczty firmowej, z adresem zawierającym po znaku @ nazwę domeny kancelarii, do kontaktu z klientami i mam podpisaną umowę powierzenia z dostawcą hostingu.	
3.	Nie korzystam z prywatnej poczty do obsługi spraw firmowych.	
4.	Każdorazowo oceniam wagę dokumentów i w zależności od potrzeby szyfruję zawartość wysyłanego pliku.	

5.	Większą ilość plików przesyłam za pomocą rozwiązania wdrożonego na serwerze w kancelarii albo hostingu i mam podpisaną umowę powierzenia z dostawcą.	
6.	Trwale usuwam dane z dysku urządzenia po zakończeniu pracy na nich i w razie potrzeby sięgam do szyfrowanej kopii bezpieczeństwa, zawierającej sprawy archiwalne.	
7.	Jeżeli wymieniam informacje o sprawie z Klientem za pomocą usługi chmurowej, to udostępniam Klientowi bezpieczny panel logowania oraz wyłącznie upoważnieni pracownicy mają dostęp do danych Klienta.	

Jeżeli zaznaczyłeś co najmniej jedną odpowiedź na NIE – oznacza to, że powinna zostać przeprowadzona rewizja Systemu Zarządzania Bezpieczeństwem Informacji w kancelarii.

V. Przetwarzanie danych osobowych w kancelarii

1. Obowiązki prawne (B. Marek)

Przynależność prawnika do korporacji zawodowej, np. adwokackiej lub radcowskiej, nakłada obowiązek bezpiecznego przetwarzania danych zgodnie z etyką zawodową, jednak nie wyklucza to stosowania przepisów na poziomie ustawy o ochronie danych osobowych (dalej "ustawa") oraz aktów wykonawczych do tejże ustawy przez prawników. Zatem każda kancelaria i prawnicy w niej pracujący są zobowiązani przestrzegać przepisów o ochronie danych osobowych.

Właściciel kancelarii albo odpowiednio prezes zarządu jest reprezentantem administratora danych w rozumieniu przepisów o ochronie danych osobowych. Jest to bowiem w świetle prawa osoba decydująca o celach i środkach przetwarzania danych osobowych w kancelarii. Osoba ta może wspierać się wiedzą i doświadczeniem osób specjalizujących się w tematyce bezpieczeństwa i w tym celu powołać Administratora Bezpieczeństwa Informacji. Jednakże w dalszym ciągu administratorem danych jest kancelaria i osoba bezpośrednio ją reprezentująca.

Za dane osobowe uznaje się dane pozwalające na zidentyfikowanie pośrednie albo bezpośrednie osoby fizycznej bez nadmiernych nakładów czasu i kosztów. Bez wątpienia dane osobowe są przetwarzane w każdej kancelarii prawnej i obejmują co najmniej:

- dane pracowników, w tym aplikantów czy praktykantów,
- dane kandydatów do pracy albo na staż albo praktykę,
- dane klientów będących osobami fizycznymi albo osób upoważnionych do kontaktu po stronie klientów firmowych na potrzeby rozliczeń,
- dane o klientach, w tym dane o osobach trzecich, które są przetwarzane w związku z prowadzoną na rzecz klienta sprawą, tj. świadczoną na jego rzecz umową.

Powyżej wymienione grupy można uznać jednocześnie za przykłady zbiorów danych. Każdy nowy zbiór danych wyróżniamy na podstawie celu przetwarzania. Jeżeli przykładowo przetwarzamy określony zakres danych na potrzeby prowadzenia dokumentacji pracowniczej, to jest to zbiór danych o pracownikach. Jeżeli na potrzeby rekrutacji, to jest to zbiór dotyczący rekrutacji, etc.

Przetwarzanie danych jest dopuszczalne wyłącznie wtedy, gdy zachodzi co najmniej jedna przesłanka legitymizująca do przetwarzania danych:

1. gdy osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych;

2. jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;

3. jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;

4. jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;

5. jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Obowiązki podstawowe

Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany wdrożyć System Zarządzania Bezpieczeństwa Informacji, rozumiany w niniejszym dokumencie jako Politykę Bezpieczeństwa i Instrukcję Zarządzania Systemem Informatycznym, a także zapewnić, aby dane te były:

1. przetwarzane zgodnie z prawem;

2. zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane

dalszemu przetwarzaniu niezgodnemu z tymi celami;

3. merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;

4. przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania;

5. spełniające obowiązki informacyjne oraz inne, opisane szczegółowo poniżej.

Obowiązki informacyjne

Dane pozyskane bezpośrednio od osoby fizycznej

W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o:

1. adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku;

2. celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych;

3. prawie dostępu do treści swoich danych oraz ich poprawiania;

4. dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Powyższych punktów nie stosuje się, jeżeli:

1. przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania;

2. osoba, której dane dotyczą, posiada już te informacje.

Dane pozyskane pośrednio (tj. nie wprost) od osoby fizycznej

W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:

1. adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku;

2. celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych;

3. źródle danych;

4. prawie dostępu do treści swoich danych oraz ich poprawiania;

5. uprawnieniach do wniesienia, w przypadku przetwarzania danych na podstawie prawnie usprawiedliwionego celu albo wykonania określonych prawem zadań realizowanych dla dobra publicznego, pisemnego, umotywowanego żądania zaprzestania przetwarzania danych ze względu na szczególną sytuację tej osoby;

6. uprawnieniach do wniesienia sprzeciwu wobec przetwarzaniu jej danych na podstawie prawnie usprawiedliwionego celu albo wykonania określonych prawem zadań realizowanych dla dobra publicznego, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

Powyższych punktów nie stosuje się, jeżeli:

1. przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą;

2. dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie wymagań określonych powyżej wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania;

3. dane są przetwarzane przez administratora: podmiot niepubliczny realizujący zadania publiczne, organy państwowe, organy samorządu terytorialnego oraz przez państwowe i komunalne jednostki organizacyjne;

4. osoba, której dane dotyczą, posiada informacje, o których mowa powyżej.

Zgłaszanie, aktualizacja, wyrejestrowanie zbiorów

Administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 i 1a ustawy. Rozpoczęcie przetwarzania jest możliwe po dokonaniu zgłoszenia. Jednak w przypadku danych wrażliwych (ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym) można rozpocząć ich przetwarzanie dopiero po zarejestrowaniu zbioru. Z obowiązku rejestracji zwolniony jest administrator danych, który powołał i zgłosił do Generalnego Inspektora Administratora Bezpieczeństwa Informacji. Nie dotyczy to jednak zbiorów zawierających dane wrażliwe.

Każdy zbiór należy aktualizować w terminie 30 dni od momentu dokonania w nim zmian. Przykładowo zmiany zakresu danych albo przetwarzającego.

Zbiór należy wyrejestrować, jeżeli ustała przesłanka legitymizująca do jego przetwarzania.

Wydawanie upoważnień i zawieranie umów powierzenia

Każdy pracownik kancelarii powinien być dopuszczony do przetwarzania tylko takich danych, które są niezbędne do wykonywania jego pracy. Oznacza to, że nie powinien mieć dostępu, i zazwyczaj nie ma, do wszystkich danych o klientach gromadzonych w kancelarii. Zgodnie z przepisami należy każdemu pracownikowi wydać upoważnienie do przetwarzania danych i cofnąć je, tj. uniemożliwić dostęp do danych, gdy ustanie przesłanka upoważniająca do przetwarzania.

W przypadku osób, które wykonują prace w kancelarii w wyniku zawarcia umowy o świadczenie usług z określoną firmą albo w przypadku firm lub ich pracowników świadczących usługi IT, należy zawrzeć umowę powierzenia przetwarzania danych osobowych.

Umowa dla swej ważności musi zostać zawarta na piśmie oraz zawierać co najmniej:

- wskazanie zakresu i celu przetwarzania danych;
- zobowiązanie przetwarzającego, że przed rozpoczęciem przetwarzania danych podejmie środki zabezpieczające zbiór danych, o których mowa w art. 36–39 ustawy, oraz spełnił wymagania określone w przepisach, o których mowa w art. 39a ustawy; w zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych;
- informację czy wyrażana jest, a jeśli tak to na jakich zasadach, zgoda na dalsze powierzenie (w celu wykazania kontroli i realnego określenia pozycji administratora w umowie);
- informację, jaka kontrola przetwarzającego jest zapewniona;
- co dzieje się z danymi po rozwiązaniu umowy oraz jak jest uregulowana płatność – np. czy powierzenie jest wliczone w cenę świadczonej usługi głównej.

Zabezpieczanie danych osobowych

Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne, zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator danych w tym celu prowadzi dokumentację, opisującą sposób przetwarzania danych oraz środki, o których mowa w zdaniach poprzednich – System Zarządzania Bezpieczeństwem Informacji.

Administrator danych może powołać Administratora Bezpieczeństwa Informacji, do którego podstawowych obowiązków należy:

a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych;

b) nadzorowanie opracowania i aktualizowania Systemu Zarządzania Bezpieczeństwem Informacji oraz przestrzegania zasad w nim określonych;

c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Administrator Bezpieczeństwa Informacji (ABI) może w całości zajmować się wykonywaniem obowiązków nałożonych na administratora danych w zakresie zapewnienia prawidłowego przestrzegania przepisów, o ile ma zapewnione odpowiednie warunki i ostateczne decyzje podejmuje administrator danych po zaopiniowaniu ich przez ABI.

Przekazywanie danych osobowych do państwa trzeciego

Przekazanie danych osobowych do państwa trzeciego może nastąpić, jeżeli państwo docelowe zapewnia na swoim terytorium odpowiedni poziom ochrony danych osobowych. Jeżeli Komisja Europejska zaaprobowała poziom ochrony przetwarzania danych i została wydana stosowna decyzja, możliwe jest oparcie relacji na podstawie ważnej i obowiązującej decyzji Komisji. W innym razie należy oprzeć przetwarzanie na standardowych klauzulach umownych albo, jeżeli Generalny Inspektor uznał wiążące reguły korporacyjne, to właśnie na nich.

Zmiany w obowiązkach od 2018 r.

Przepisy o ochronie danych osobowych zmienią się diametralnie od 2018 r., pod względem zarówno obowiązków, jak i sankcji dla administratorów danych, w tym także pozycji i roli krajowych organów nadzorczych. Stanie się tak za sprawą jednolitego rozporządzenia o ochronie danych osobowych. Z uwagi na ograniczenia objętościowe niniejszego poradnika nie zostaną one omówione w tym miejscu. Jednak można się z nimi szczegółowo zapoznać na stronach typu Pomocnik RODO.

2. Wymagania bezpieczeństwa dla systemu teleinformatycznego przetwarzającego dane osobowe (K. Pszczółkowski)

System teleinformatyczny, w którym planowane jest przetwarzanie danych osobowych, przed uruchomieniem powinien zapewnić:

1. Mechanizmy kontroli dostępu do danych – użytkownik ma dostęp tylko do takich informacji, jakie mu są niezbędne do realizacji zadań służbowych;

2. Uwierzytelnienie z wykorzystaniem identyfikatora użytkownika oraz hasła;

3. Uniemożliwienie nadania identycznego identyfikatora dwóm użytkownikom, nawet wtedy, gdy pierwszy z nich przestanie pracować;

4. Rejestrację zmian wykonywanych przez użytkownika na poszczególnych elementach zbioru danych osobowych;

5. Środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych;

6. Mechanizmy wymuszające okresowe, co 30 dni, zmiany haseł dostępu do zbioru danych osobowych;

7. Szyfrowanie połączeń w przypadku wykorzystywania sieci publicznej (np. Internet) do komunikacji z systemem teleinformatycznym;

8. Odnotowywanie daty pierwszego wprowadzenia przez użytkownika danych do systemu teleinformatycznego;

9. Odnotowywanie identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;

10. Odnotowywanie źródła danych, w przypadku zbierania ich od osoby innej niż ta, której dane dotyczą;

11. Informacje o odbiorcach, którym dane osobowe zostały udostępnione, datę i zakres tego udostępnienia;

12. Automatyczne odnotowywanie przez system teleinformatyczny wykonywanych przez użytkownika operacji na danych, tj.:

a) Daty pierwszego wprowadzenia danych do systemu;

b) Identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu teleinformatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;

13. Sporządzanie i drukowanie raportów zawierających powyższe odnotowane informacje.

System teleinformatyczny, w którym planowane jest przetwarzanie danych osobowych, przed uruchomieniem powinien posiadać dokumentację dotyczącą:

1. Zarządzania użytkownikami (w tym zarządzania uprawnieniami);

2. Zarządzania kopiami zapasowymi danych;

3. Zarządzania przeglądami i konserwacją systemu oraz nośników informacji służących do przetwarzania danych;

4. Opisu stosowanych metod i środków uwierzytelniania;

5. Opisu przepływu danych (wejście, wyjście) między systemem teleinformatycznym a innymi systemami teleinformatycznymi zewnętrznymi;

6. Wykazu danych osobowych (tzn. pól informacyjnych) przetwarzanych w ramach funkcjonowania systemu teleinformatycznego (np. imię i nazwisko, adres, e-mail, nazwa firmy, nr identyfikatora).

Każda osoba, która traci prawo do przetwarzania danych (np. cofamy jej upoważnienie) tym samym powinna utracić prawo dostępu do tych danych zgromadzonych w systemie teleinformatycznym.

3. Zabezpieczenia organizacyjne dotyczące przetwarzania danych osobowych (K. Pszczółkowski)

W celu zapewnienia bezpiecznego przetwarzania danych osobowych w Kancelarii, w tym zapewniania poufności, integralności i rozliczalności przetwarzanych danych, należy określić niezbędne środki organizacyjne i techniczne. Należy pamiętać, iż środki, o których mowa, powinny być określone po uprzednim przeprowadzeniu analizy i oceny ryzyka bezpieczeństwa informacji.

Analiza zagrożeń powinna uwzględniać cały proces przetwarzania danych, od ich pozyskania lub wytworzenia po przekazanie, archiwizację lub znaczenie. Powinna uwzględniać również identyfikację podatności (luk), umożliwiających urzeczywistnienie się zagrożeń np. włamania do systemu i utraty poufności danych oraz identyfikację aktualnie stosowanych zabezpieczeń. Na postawie tak przeprowadzonej analizy jesteśmy w stanie ocenić prawdopodobieństwo i skutki identyfikowanych ryzyk i dobrać do nich adekwatne zabezpieczenia zapewniające minimalizację tych ryzyk.

Poniżej przedstawiona została lista rekomendacji i dobrych praktyk najczęściej wykorzystywanych do ochrony przetwarzanych informacji w organizacji.

1. Rekomendacje dotyczące zabezpieczania pomieszczeń, w których przetwarzane są dane osobowe:

a) pomieszczenia, w których przetwarzane są dane osobowe, należy zabezpieczyć przed niepowołanym dostępem np. kurierami, dostawcami, interesariuszami;

b) przebywanie osób nieuprawnionych (np. gości) w pomieszczeniach, w których przetwarzane są dane osobowe, jest dopuszczalne tylko w obecności osób zatrudnionych w organizacji, które posiadają upoważnienia do przetwarzania tych danych;

c) budynki lub pomieszczenia, w których przetwarzane są dane osobowe, na czas nieobecności osób zatrudnionych przy ich przetwarzaniu, są zamykane

w sposób uniemożliwiający dostęp do danych osobom nieuprawnionym;

d) personel sprzątający wykonuje swoje zadania tylko w obecności osób uprawnionych do przetwarzania danych osobowych.

2. Rekomendacje dotyczące przechowywania zbiorów danych osobowych w postaci papierowej np. kartotek, ksiąg, wykazów i innych form papierowych:

a) zbiory danych osobowych w postaci kartotek, ksiąg, wykazów czy innych postaci papierowych powinny być przechowywane w warunkach uniemożliwiających dostęp osobom nieuprawnionym;

b) należy stosować politykę czystego biurka, polegającą na niepozostawianiu żadnych nośników zawierających zbiory danych (np. dokumentów papierowych, dyskietek, płyt CD) na stanowisku pracy po jej zakończeniu w danym dniu roboczym, uniemożliwiając tym samym dostęp do informacji osobom nieupoważnionym;

c) po zakończeniu pracy wszelkie nośniki informacji zawierające zbiory danych powinny być przechowywane w zamykanych na klucz biurkach, szafkach, szafach lub pojemnikach;

d) wszelkie nośniki zawierające zbiory danych osobowych, które nie będą już wykorzystywane (np. brudnopisy), należy niszczyć w niszczarkach lub przekazywać do zniszczenia, umieszczając je w specjalnie do tego przeznaczonych, zabezpieczonych pojemnikach dostarczanych przez firmę zewnętrzną; zabrania się ręcznego niszczenia jakichkolwiek dokumentów i wyrzucania ich w całości do kosza na śmieci.

3. Wymagania szczegółowe, dotyczące przechowywania zbiorów danych osobowych w postaci elektronicznej, np. plików pochodzących z programów do edycji, arkuszy kalkulacyjnych, baz danych:

a) wszystkie zbiory danych w postaci elektronicznej należy przechowywać w specjalnie do tego przeznaczonych i zabezpieczonych przed dostępem osób nieupoważnionych folderach na serwerze plików lub komputerze;

b) w celu ochrony przetwarzane na komputerach przenośnych pliki elektroniczne zawierające zbiory danych powinny być zaszyfrowane.

4. Wymagania dotyczące osób zatrudnionych przy przetwarzaniu danych osobowych:

a) każdy nowozatrudniony pracownik, przed dopuszczeniem go do pracy przy przetwarzaniu danych osobowych, obowiązkowo zapoznawany jest z zasadami bezpiecznego przetwarzania i ochrony informacji;

b) pracownik, który odbył szkolenie, potwierdza ten fakt na piśmie, podpisując zobowiązanie do zachowania w poufności informacji, do których uzyska dostęp w trakcie zatrudnienia;

c) dane osobowe z określonego zbioru mogą być przetwarzane jedynie przez pracowników posiadających upoważnienie do przetwarzania danych osobowych;

d) pracownicy mający dostęp do danych osobowych powinni być zobowiązani do:

- zachowania tych danych w tajemnicy, również po ustaniu zatrudnienia;
- przestrzegania bezwzględnego zakazu udzielania innym podmiotom informacji wewnętrznych, w tym danych osobowych (np. udzielania informacji przez telefon, email, samodzielnego udzielania odpowiedzi na pisma);
- bezzwłocznego zawiadamiania bezpośredniego przełożonego o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych i systemu informatycznego przetwarzającego te dane;
- bezzwłocznego zawiadomienia przełożonego w przypadku naruszenia bezpieczeństwa danych osobowych.

4. Zasady odbioru nowego systemu teleinformatycznego, który ma przetwarzać dane osobowe (K. Pszczółkowski)

Testy akceptacyjne

Dopuszczenie do produkcji zaprojektowanego, nabytego lub zmodyfikowanego systemu teleinformatycznego może nastąpić jedynie po pozytywnym przejściu testów akceptacyjnych w ramach odbioru systemu IT.

W ramach testów akceptacyjnych dla nowych systemów teleinformatycznych powinny być przeprowadzone:

a) testy funkcjonalne i pozafunkcjonalne;

b) testy wydajnościowe;

c) testy penetracyjne;

d) testy bezpieczeństwa (na podstawie zdefiniowanych wymagań bezpieczeństwa, np. ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych).

Narzędzia i programy służące do testowania mogą być używane wyłącznie przez upoważnionych pracowników organizacji do celów testowych i rozwojowych. Dostęp do tych narzędzi i programów musi być ściśle kontrolowany.

Testy akceptacyjne przeprowadzane są na podstawie zdefiniowanych wcześniej scenariuszy testowych. Scenariusze testowe mogą być opracowane przez dostawcę oprogramowania, jednakże wymagają weryfikacji i akceptacji przez zamawiającego.

Testowanie akceptacyjne nie może być przeprowadzane przez dostawcę oprogramowania.

Wszystkie opracowywane aplikacje muszą być ulokowane na przeznaczonych do tego celu serwerach, nie zaś na stacjach roboczych.

Testy dla nowych lub istniejących systemów przeprowadzane są jedynie na danych testowych, odzwierciedlających dane produkcyjne, przygotowanych specjalnie w celu przeprowadzenia testów akceptacyjnych.

Odbiór systemu lub usługi IT

Decyzja o przeniesieniu nowego lub zmodyfikowanego systemu informatycznego ze środowiska testowego do środowiska produkcyjnego jest podejmowana przez osobę odpowiedzialną za IT w kancelarii, po uzyskaniu pozytywnej opinii osoby odpowiedzialnej za bezpieczeństwo (jeśli są to dwie różne osoby).

Środowisko produkcyjne powinno być fizycznie odseparowane od środowiska testowego i programistycznego poprzez jego lokalizację na osobnym serwerze. Jeśli nie jest to możliwe, musi być zapewnione pełne rozdzielenie zasobów sprzętowych i dyskowych lub zagwarantowana minimalna dostępność zasobów niezbędnych do funkcjonowania środowiska produkcyjnego.

Uprawnienia osób pracujących w środowiskach produkcyjnym, testowym i programistycznym powinny być zróżnicowane. Najszersze uprawnienia posiadają osoby pracujące w środowisku programistycznym. Uprawnienia w środowiskach testowym i produkcyjnym są ściśle ograniczone.

Pracownicy zajmujący się opracowywaniem oprogramowania wykorzystywanego do prowadzenia działalności operacyjnej nie mogą mieć dostępu do informacji użytkowanych w środowisku produkcyjnym, z wyjątkiem informacji niezbędnych do prawidłowego opracowania oprogramowania oraz z wyłączeniem sytuacji awaryjnych, w zakresie do tego niezbędnym. W przypadku sytuacji awaryjnych wyznaczeni programiści powinni otrzymać dostęp do przydzielonych im osobistych kont awaryjnych. Dostępem do kont awaryjnych powinien zarządzać administrator systemu.

Musi zostać zastosowana konwencja nazewnictwa umożliwiająca wyraźne odróżnienie plików/bibliotek używanych w środowisku produkcyjnym od plików używanych dla celów testowych i/lub szkoleniowych.

Osoba odpowiedzialna za IT w kancelarii ma obowiązek zapewnić właściwy podział obowiązków we wszystkich obszarach związanych z rozwojem systemu, administracją systemem i bieżącymi operacjami systemowymi. Pracownicy zaangażowani w opracowanie oprogramowania wykorzystywanego do prowadzenia działalności operacyjnej nie mogą być władni do przenoszenia oprogramowania do środowiska produkcyjnego.

Przed odbiorem systemu osoba odpowiedzialna za bezpieczeństwo w organizacji musi otrzymać udokumentowaną informację, czy wszystkie wytyczne zapewniające bezpieczeństwo zostały spełnione.

5. Zasady tworzenia i testowania kopii zapasowych (K. Pszczółkowski)

W celu zapobiegania utratom danych na skutek awarii bądź błędów eksploatacyjnych należy opracować harmonogram wykonywania kopii zapasowych oraz wyznaczyć osoby odpowiedzialne za wykonywanie tych czynności.

Administrator Systemu zobowiązany jest do opracowania, przyjęcia i stosowania określonego planu wykonywania kopii zapasowych systemu i danych. Plan ten powinien zostać sporządzony w formie pisemnej i przechowywany w bezpiecznym miejscu.

Administrator odpowiadający za urządzenia sieciowe jest zobowiązany do wykonywania oraz przechowywania kopii zapasowych konfiguracji urządzeń aktywnych.

Osoba odpowiedzialna za wykonanie kopii bezpieczeństwa zobowiązana jest do prowadzenia dokumentacji z wykonywanych kopii bezpieczeństwa, która powinna zawierać co najmniej:

a) datę i godzinę rozpoczęcia wykonywania kopii zapasowej;

b) datę i godzinę zakończenia wykonywania kopii zapasowej;

c) jednoznaczne określenie nośnika, na którym została wykonana kopia;

d) oznaczenie typu kopii będącej odnośnikiem do procedury wykonywania kopii zapasowych (np. kopia pełna, przyrostowa, trzecia w cyklu);

e) datę i czytelny podpis osoby wykonującej kopię zapasową.

Na administratorze wykonującym kopie zapasowe spoczywa obowiązek każdorazowego weryfikowania poprawności wykonania kopii zapasowej. W przypadku niepoprawnego zapisu kopii zapasowej należy sprawdzić stan techniczny nośnika, na którym zapisywane są kopie zapasowe oraz ponownie przeprowadzić proces wykonywania kopii zapasowej.

Należy okresowo przeprowadzać operację odzyskiwania danych z wykonanych kopii zapasowych w celu weryfikacji procesu wykonania kopii. Podczas odtwarzania kopii zapasowych należy określić zakres przywracanych danych oraz numer nośnika kopii zapasowej, z którego przywracano dane.

Nośniki informacji należy przechowywać w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem (np. szafy pancerne, szafy ogniotrwałe).

Dopuszcza się możliwość przechowywania dodatkowych kopii zapasowych w obszarze przetwarzania danych (np. serwerowniach), gdy konieczność ich utworzenia i przechowywania wynika z zastosowanych narzędzi i metod archiwizacji, pod warunkiem zastosowania zabezpieczeń technicznych, uniemożliwiających dostęp do danych osobom trzecim.

W przypadku transportowania nośników z kopiami zapasowymi poza obszar organizacji, należy zapewnić bezpieczne warunki transportu poprzez:

a) zapewnienie poufności danych poprzez zaszyfrowanie nośnika;

b) przewożenie kopii bezpieczeństwa w postaci niezaszyfrowanej wyłącznie w obecności dwóch pracowników organizacji;

c) niepozostawianie kopii bezpieczeństwa bez nadzoru;

d) umieszczanie nośników w bezpiecznych pojemnikach, uniemożliwiających ich zniszczenie.

Nośniki zawierające kopie zapasowe należy przechowywać tak, aby dostęp do nich osób trzecich był ograniczony. Zaleca się przechowywać je w zamykanych szafach bądź sejfach, poza siedzibą lokalizacji podstawowej (off-site), aby w przypadku sytuacji kryzysowej (np. pożar budynku) zniszczeniu nie uległy zarówno urządzania jak i kopie zapasowe.

Nośniki kopii zapasowych, które zawierają dane archiwalne i są uszkodzone lub nie można ich ponownie wykorzystać, muszą być niezwłocznie zniszczone w sposób uniemożliwiający odtworzenie zapisanych na nich danych.

6. 12 NAJWAŻNIEJSZYCH ZASAD OCHRONY DANYCH OSOBOWYCH (K. PSZCZÓŁKOWSKI)

Mając na uwadze konieczność ochrony danych osobowych, wynikającą z obowiązujących przepisów prawa oraz zobowiązań wobec klientów, w kancelarii powinny być stosowane najważniejsze zasady bezpieczeństwa danych osobowych; ich wykaz znajduje się poniżej.

1. Wszystkie dokumenty lub materiały zawierające dane osobowe (w tym: umowy, notatki, wizytówki, ankiety, pieczątki, faktury itp.) powinny być przechowywane w zamykanych szafkach.

2. Dokumenty lub materiały robocze zawierające dane osobowe, które nie są już potrzebne i nie będą wykorzystywane do dalszej pracy, powinny zostać zniszczone przy użyciu niszczarki.

3. Pracownik, opuszczając stanowisko pracy, powinien pozostawić komputer wylogowany lub wyłączony.

4. Po zakończeniu pracy każdy laptop powinien być schowany do szafki lub zabrany ze sobą.

5. Szafki, w których przechowywane są dane osobowe, powinny zostać zamknięte na klucz, a klucz ten powinien zostać zabrany przez pracownika.

6. Pracownik nie może trzymać zapisanego loginu i hasła do komputera przy swoim stanowisku pracy.

7. Hasło do komputera znane jest tylko pracownikowi i nie może on udostępniać go innym pracownikom, niezależnie od sytuacji.

8. Karty wejścia do budynków powinny być stale przy pracowniku.

9. Należy pamiętać, aby nie zostawiać żadnych dokumentów przy drukarce.

10. W przypadku gdy dany pracownik jest ostatnią osobą wychodzącą z pokoju, a pokój ten jest zamykany na klucz, wówczas pracownik musi pamiętać, aby zamknąć pokój na klucz.

11. Osoby spoza kancelarii (tj. goście, kurierzy, dostawcy, serwisanci) nie mogą poruszać się po siedzibie spółki samodzielnie, zawsze muszą pozostać pod opieką pracownika.

12. Dane osobowe wysyłane mailem powinny zostać zaszyfrowane, a hasło do pliku powinno zostać przekazane inną drogą niż mailowa np. SMS-em.

Wszelkie zauważone incydenty, dotyczące naruszenia ochrony danych osobowych, powinny zostać natychmiastowo zgłoszone do osoby odpowiadającej za bezpieczeństwa w organizacji.

7. Lista kontrolna (K. Pszczółkowski, B. Marek)

Zaznacz odpowiedź TAK albo NIE przy każdej czynności:

	WYKONYWANA CZYNNOŚĆ	TAK / NIE
1.	Wszystkie dokumenty lub materiały zawierające dane osobowe (tj. umowy, notatki, wizytówki, ankiety, pieczątki, faktury itp.) po zakończeniu dnia pracy są przechowywane w szafkach zamykanych na klucz.	
2.	Dokumenty lub materiały robocze zawierające dane osobowe, które nie są już potrzebne i nie będą wykorzystywane do dalszej pracy, są niszczone przy użyciu niszczarki lub wrzucane do metalowego kontenera przeznaczonego do niszczenia dokumentów.	
3.	Pracownik, kończąc swój dzień pracy, wyłącza komputer lub przynajmniej się z niego wylogowuje.	
4.	Każdy laptop, po zakończeniu dnia pracy, zostaje przypięty do biurka za pomocą stalowej linki, schowany do szafki zamykanej na klucz lub zabrany z sobą.	

	WYKONYWANA CZYNNOŚĆ	TAK / NIE
5.	Szafki, w których przechowywane są dane osobowe, są zamykane na klucz, a klucz ten zostaje zabrany przez prawnika lub odpowiednio zabezpieczony.	
6.	Pracownik nie trzyma zapisanego loginu i hasła do komputera przy swoim stanowisku pracy.	
7.	Hasło do komputera znane jest pracownikowi i prawnikowi zarządzającemu i nie mogą oni udostępniać go innym pracownikom, niezależnie od sytuacji.	
8.	Dokumenty nie są zostawiane przy drukarce lub ksero albo skanerze bez opieki.	
9.	Pendrive służy do przeniesienia dokumentu, a nie do prowadzenia na nim archiwum (pendrive powinien być "czyszczony" po udostępnieniu pliku).	
10.	W przypadku gdy dany pracownik jest ostatnią osobą wychodzącą z pokoju, a pokój ten jest zamykany na klucz lub na kartę, wówczas pamięta, aby zamknąć pokój i okna.	
11.	Osoby spoza firmy (tj. goście, kurierzy, dostawcy, serwisanci) nie poruszają się po siedzibie samodzielnie, pozostają pod stałą opieką pracownika.	
12.	W czasie prowadzonej rozmowy w miejscu publicznym nie są wymieniane nazwy firm, imiona i nazwiska oraz kwoty – nigdy nie wiadomo, kto może słuchać.	
13.	W przypadku podejrzenia naruszenia zasad bezpieczeństwa ochrony danych osobowych, bezpośrednio informowany jest przełożony.	
14.	W kancelarii został wdrożony System Zarządzania Bezpieczeństwem Informacji (Polityka Bezpieczeństwa, Instrukcja Zarządzania Systemem Informatycznym z elementami planu ciągłości działania).	
15.	Kancelaria ma zawarte umowy powierzenia przetwarzania danych osobowych z hostingiem i innymi usługodawcami, którzy mają dostęp do danych osobowych.	
16.	Pracownikom zostały wydane upoważnienia do przetwarzania danych osobowych, a w razie odejścia zostały one cofnięte i anulowano dostęp do danych osobowych.	
17.	Zbiory danych osobowych zostały zgłoszone do Generalnego Inspektora Ochrony Danych Osobowych.	

	WYKONYWANA CZYNNOŚĆ	TAK / NIE
18.	W kancelarii została wyznaczona osoba, która jest odpowiedzialna za nadzór nad przestrzeganiem przepisów o ochronie danych osobowych, a w razie potrzeby został powołany Administrator Bezpieczeństwa Informacji.	
19.	Dane osobowe są archiwizowane na zaszyfrowanych nośnikach danych, innych niż dyski wirtualne lub chmura, a zawartość nośników kopiowana jest na nowe nośniki co najmniej raz na trzy lata.	
20.	Raz do roku przeprowadzany jest audyt stanu bezpieczeństwa kancelarii pod kątem przetwarzania danych osobowych.	

Jeżeli zaznaczyłeś co najmniej jedną odpowiedź na NIE – oznacza to, że powinna zostać przeprowadzona rewizja Systemu Zarządzania Bezpieczeństwem Informacji w kancelarii.

VI. Scenariusze ataków

1. Kradzież sprzętu i wyciek danych (A. Ziaja)

Co się stało?

Karol jako pracownik kancelarii często odbywa podróże służbowe do swoich klientów i obowiązkowo zabiera ze sobą służbowego laptopa oraz tablet pomagający mu w codziennej pracy. Wszystko trzyma w torbie na laptopa. Właśnie udał się na jedno z takich spotkań. Zanim dotarł do klienta zatrzymał się by coś zjeść. Wychodząc z samochodu zostawił tam torbę a zabrał podręczną teczkę. Niestety w trakcie przerwy obiadowej został skradziony mu z samochodu cały ten sprzęt. Zorientował się po wyjściu z restauracji.

Co się teraz dzieje?

Karol zgłosił sprawę w lokalnej komendzie. Jednak kancelaria w wyniku zajścia poniosła nie tylko straty finansowe w postaci utraty tabletu i laptopa, ale również ma poważne problemy prawne. W ciągu niecałej godziny przestępcy skontaktowali się z jednym z klientów, którego dane dotyczące sprawy były przechowywane na służbowym sprzęcie i posłużyły w szantażu, że zostaną ujawnione opinii publicznej. Karol otrzymał telefon od zdenerwowanego klienta i próbuje na szybko wymyślić jak ujawnienie tych danych wpłynie na dalszy bieg postępowania.

Jak można było tego uniknąć?

Sytuacji tej można by było zapobiec jeśli firmowy sprzęt byłby szyfrowany. W dzisiejszych czasach nawet tablet czy telefon komórkowy posiada wbudowane funkcje szyfrujące zawartość urządzenia oraz karty pamięci tak samo jak i komputery przenośne. W przypadku korzystania z szyfrowania i wykonywania kopii zapasowych taki incydent wiązałby się jedynie ze stratą w postaci sprzętu, a dane byłyby bezpieczne i realnie niemożliwe do odtworzenia przez osoby niepowołane.

2. DDoS (A. Ziaja, G. Cenkier)

W uproszczeniu – DDoS jest atakiem, którego celem jest zablokowanie dostępu do danej usługi przez wysłanie do niej dużej ilości danych. Najczęściej występującym rodzajem ataków DDoS jest atak na serwery WWW celem zablokowania dostępu do danej strony internetowej. Dla osób postronnych, jeśli atak będzie wystarczająco silny, strona, która jest atakowana, będzie ładować się zdecydowanie dłużej, a często będzie również niedostępna z uwagi na to, że atakowany serwer będzie miał problemy z przepustowością sieci lub z możliwościami obliczeniowymi sprzętu.

DDoS w przypadku kancelarii może być próbą:

- zablokowania serwisu internetowego na dłuższy lub krótszy czas, w celu uniemożliwienia pracy kancelarii – utrata klientów oraz reputacji;
- nie tylko zablokowania serwisu, ale także uzyskania dostępu, nieautoryzowanego rzecz jasna, do zasobów kancelarii. Atak typu DDoS

Co się stało?

Jan, pracownik kancelarii prawnej, po długim oczekiwaniu zalogował się do poczty elektronicznej, gdzie przeczytał maila o dziwnej treści. Wynikało z niej, że nieznana osoba grozi zablokowaniem strony internetowej kancelarii na rok, i to pod każdą domeną jaka zostanie utworzona, jeśli nie zostanie wpłacona kwota 10 000 zł. Pocztę odbierał wyjątkowo długo, a także odebrał kilka telefonów od współpracowników, że mają problemy z zalogowaniem się do systemu informatycznego kancelarii.

Co się teraz dzieje?

Powoli zaczyna panować chaos, bo pracownicy nie mogą pracować. Jan zgłasza sprawę do partnera zarządzającego i proponuje by skontaktować się z operatorem. Wcześniej, przeglądając stronę Ministerstwa Cyfryzacji, zapamiętał gdzie można zgłosić cyberatak. Jan otwiera stronę https://mc.gov.pl/zglos-cyberatak i kontaktuje się z operatorem sieci. Czekają na wsparcie. Nie płacą okupu.

Jak można było tego uniknąć?

Przed tym atakiem nie da się chronić inaczej, aniżeli poprzez wykupienie blokady niepożądanego ruchu sieciowego (eliminacja podejrzanych pakietów). Usługi takie świadczą operatorzy telekomunikacyjni. Prawnik zarządzający powinien poprosić informatyka albo skontaktować się z firmą hostingującą i dowiedzieć w jaki sposób można wdrożyć tego typu działania.

3. Phishing (G. Cenkier)

Jak rozpoznać phishing?

Nie jest to łatwe, bo czasem zarówno tekst, jak i grafika, odzwierciedlają rutynowe maile od znanych dostawców. Zawsze jednak warto sprawdzić adres nadawcy i/lub adres konta bankowego, na które należy wpłacić pieniądze, jeśli jest to faktura, bo może być ona fałszywa. Należy również przeczytać, jakich działań oczekuje nadawca e-maila i ewentualnie potwierdzić telefonicznie żądanie, jeśli coś budzi wątpliwości, lub skontaktować się z administratorem systemu, czy nie zaobserwował dużego napływu e-maili od tego samego nadawcy. Nie należy otwierać załączników, jeśli treść e-maila budzi wątpliwości, bo załącznik może być zainfekowany, a jego otwarcie może spowodować np. zaszyfrowanie całego dysku.

Poniżej znajduje się 7 elementów, które warto sprawdzać w przypadku otrzymania wątpliwego e-maila:

1. Nieprawidłowa nazwa w adresie nadawcy

Zagrożeniem może być mail, który zawiera błędnie zapisaną nazwę nadawcy, np. polska_poczta.pl, lub w ogóle nie zawiera nazwy firmy/instytucji. Najprawdopodobniej oznacza to, że pochodzi od nieznanej domeny (firmy/instytucje przeważnie mają własne, zarejestrowane domeny) i jest wynikiem oszustwa.

2. Brak Twojego adresu w polu DO: (lub TO:)

Podejrzenia może wzbudzić zarówno brak twojego adresu mailowego, jak i komunikat „undisclosed recipients" (chociaż nie jest to warunek wystarczający, bo czasem np. zaproszenia na wydarzenie rozsyła się do wielu adresatów, a niekoniecznie chcemy ujawniać adresy innych zaproszonych gości) w polu OD: (TO:) – fałszywe maile wysyłane są do wielu potencjalnych ofiar jednocześnie. Mejle od zaufanych nadawców skierowane są tylko i wyłącznie do Ciebie.

3. Nieprawidłowy adres strony internetowej nadawcy – URL

W treści fałszywego mejla możesz np. znaleźć link do strony, przez którą np. masz dokonać aktualizacji swoich danych. Nigdy nie korzystaj z linków, podawanych w mejlach, a jeśli chcesz sprawdzić URL, wklej adres do nowego okna przeglądarki i zobacz, czy zawiera poprawną nazwę firmy/instytucji (może różnić się jedną literą od oryginalnej, jak np. http://mrbank.pl) oraz czy jej adres wymusza szyfrowaną certyfikatem SSL komunikację z serwerem (https://).

4. Błędy w temacie i treści wiadomości

Popularną techniką stosowaną przez hakerów jest używanie w tytułach mejli słów z błędami ortograficznymi i gramatycznymi, a także cyframi zamiast liter i dużymi literami w środku wyrazów. Ma to na celu ominięcie filtrów antyspamowych. Celowe jest także zamieszczanie błędów w treści maila. Hakerzy stosują tę metodę, aby trafić do mniej doświadczonych użytkowników, ponieważ często prowadzą rozpoznanie przy wyborze potencjalnych ofiar ataku. Wiedzą, że jeśli otrzymają odpowiedź na mejla z błędami, to będą mogli włożyć mniej wysiłku w pozyskanie od niego istotnych dla ich procederu informacji.

5. Brak logo instytucji w treści maila

Może się zdarzyć, że w sfałszowanym mejlu nie będzie grafiki i logo firmy/instytucji, pod którą podszywa się nadawca; obecnie to już rzadkość, ale czasem znajduje się tam sam tekst. Wiadomość znacznie różni się też od tych przesyłanych do tej pory przez zaufanego nadawcę krojem czcionki lub kolorem tła.

6. Prośba o podanie informacji

Często mejle od fałszywych nadawców zawierają polecenia do natychmiastowego wykonania jakiejś czynności, np. „musisz kliknąć w ten link teraz". Mogą też zawierać prośbę o podanie i/lub aktualizację informacji osobistych, np. numeru PESEL lub numeru konta bankowego albo haseł dostępu do bankowości internetowej. Należy pamiętać, że instytucje finansowe, w tym banki, nie będą żądać podania osobistych informacji pocztą elektroniczną.

7. Podejrzane załączniki

Jeśli otrzymałeś mejla z załącznikiem, to sprawdź czy ten załącznik nie zawiera pliku z rozszerzeniem: .exe, .scr, .zip, .com, .bat. Jeśli otrzymasz taki załącznik – nie otwieraj go. To prawdopodobne, że zawiera wirus.

4. Phishing + ransomware (M. Hornowski, B. Marek)

Jeśli otrzymałeś fałszywy e-mail to:

1. Prześlij załącznik do wiadomości do producenta oprogramowania antywirusowego.
2. Poproś swojego informatyka o stworzenie reguł filtrujących korespondencję pod kątem nazwy zainfekowanego załącznika.
3. Jeśli to był e-mail od rzekomo uznanego dostawcy (np. banku) prześlij informację do tej firmy oraz poinformuj współpracowników o takim wydarzeniu.

Phishing opiera się na socjotechnice. Jest to takie stworzenie wiadomości, by zachęcić do wykonania określonej czynności przez odbiorcę, np. kliknięcia w link, pobrania pliku, podania danych. Zostało ono opisane dokładnie powyżej. Natomiast ransomware to złośliwe oprogramowanie, które najczęściej dostaje się na urządzenie w wyniku pobrania pliku (np. rzekomo niezapłaconej faktury). Następnie uruchomiona zostaje zawartość programu, którego zadaniem jest wyświetlać komunikat i następuje proces zaszyfrowania dysku bądź usuwania danych.

Co się stało?

Ryszard otrzymał e-mail, rzekomo wysłany przez Pocztę Polską, w którym była informacja o nieodebranej przesyłce. Należało kliknąć w link, by dowiedzieć się o jaką przesyłkę chodzi. Ryszard kliknął. Na jego komputer pobrał się plik, który otworzył.

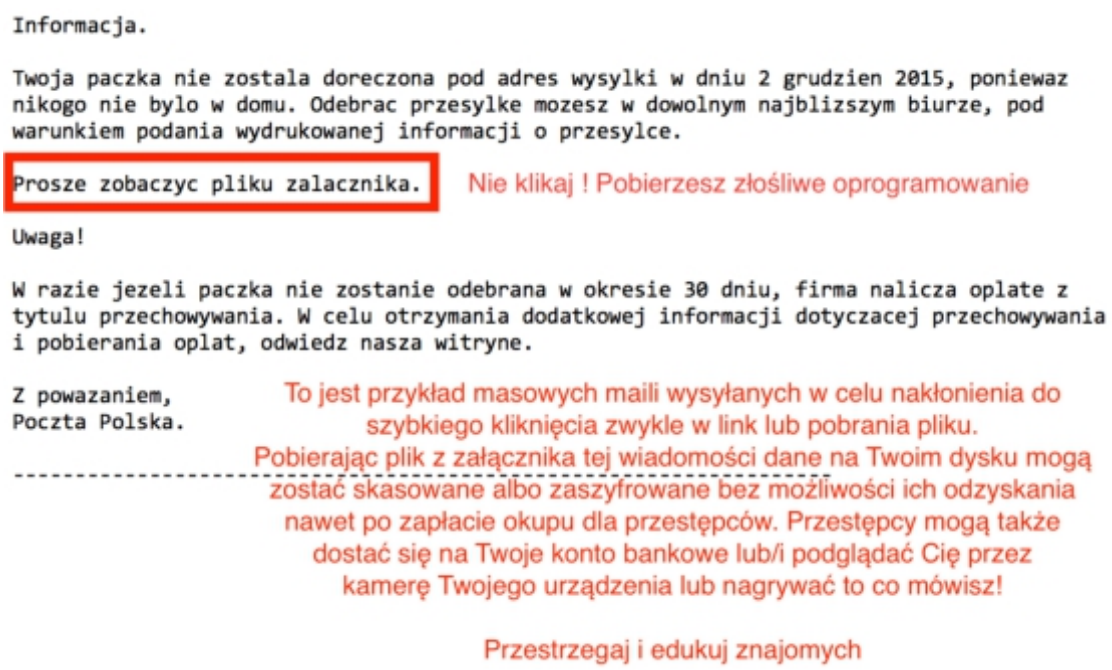
Co się teraz dzieje?

Po chwili ukazał się komunikat, że dane zostały zaszyfrowane i, jeżeli chce je odzyskać, musi zapłacić 250 USD. Sposób zapłaty miał zostać podany po wysłaniu wiadomości na podany adres e-mail. Ryszard zastanawiał się co zrobić. Jeden z pracowników powiedział by szybko wyłączył komputer i natychmiast skontaktował się z informatykiem, który polecił bezzwłocznie wyłączyć zasilanie komputera i nie włączać bez nadzoru specjalisty. Komputer trafił w ręce profesjonalisty, który odzyskał większość dokumentów z dysku. Ryszard dowiedział się, że gdyby wyłączył komputer natychmiast i odłączył zasilanie szybciej, można byłoby zatrzymać proces szyfrowania. Teraz część plików zniknęła bezpowrotnie, bo kancelaria nie wykonywała kopii danych.

Jak można było tego uniknąć?

Warto wysyłać pracowników na szkolenia. Warto ich edukować. Gdyby Ryszard przeszedł szkolenie, wiedziałby, że nie należy klikać w linki w e-mailach ani pobierać plików czy podawać danych bez potwierdzenia tożsamości nadawcy. Jednocześnie gdyby w kancelarii były wykonywane kopie bezpieczeństwa i kopie zapasowe, tego typu atak nie wyrządziłby poważnej szkody. Dane wystarczyłoby tylko przywrócić.

Poniżej przykład wraz z opisem dokonanym na potrzeby omówienia.



5. Socjotechniczna ucieczka (G. Cenkier)

28-letni Neil Moore z Londynu odsiadywał wyrok w więzieniu Wandsworth za kradzież blisko 2 milionów funtów. Kradzieży dokonywał, podszywając się pod pracowników znanych banków (Barclays, Lloyds, Satander), kradnąc ich tożsamości. Podobną technikę wykorzystał, aby uciec z więzienia.

W niejasny sposób, władze więzienia nie potrafią tego wyjaśnić, zdobył smartfona. Wykorzystując zdalny dostęp do Internetu, kupił domenę o nazwie podobnej do sądowej. W ramach tej domeny zbudował pocztę elektroniczną, która posłużyła mu do wysłania do komendanta więzienia e-maila z informacją, że należy niezwłocznie wypuścić więźnia Moore'a. Nadawcą e-maila był rzekomo jeden z prowadzących jego sprawę, powiedzmy, urzędników. Polecenie wykonano i Moor wyszedł na wolność.

Ucieczka wyszła na jaw dopiero po kilku dniach. Moora złapano po jakimś czasie i osadzono z powrotem w więzieniu. Sprawa była szeroko komentowana w mediach brytyjskich. Szczegóły wydarzenia: http://www.bbc.com/news/uk-england-london-32095189

Fałszywe e-maile dostarczyły również sporo problemów jednej z wiodących polskich kancelarii we wrześniu 2015 r.

W e-mailach, których rzekomym nadawcą była kancelaria prawna, rozsyłano informacje do osób prawnych i fizycznych o przekazaniu przeciwko nim aktu oskarżenia. Ponadto e-maile zawierały szkodliwe oprogramowanie i mogły być celowym działaniem, skierowanym na zakłócenie pracy systemu komputerowego.

E-maile były wysłane z adresu różniącego się przestawieniem 1 litery w porównaniu z prawidłowym adresem, ale rzekomo podpisane przez jednego z prawników związanych z kancelarią. Jak wielu odbiorców zwróciło na taki szczegół uwagę? Zapewne nie tak dużo, skoro poszkodowana kancelaria zdecydowała się na podjęcie szerokiej kampanii, w tym prasowej, w celu wyjaśnienia tego zdarzenia, w celu poprawienia swojego wizerunku.

VII. Informacje o autorach

Grzegorz Cenkier,
Poczta Polska S.A.

Absolwent Uniwersytetu Warszawskiego i EDV Schule w Edingen (Niemcy) w zakresie sieci komputerowych. Ukończył studia podyplomowe na Uniwersytecie Ekonomicznym w Krakowie w zakresie Zarządzania Audytem i Kontrolą Wewnętrzną. Od ponad 30 lat pracuje w branży informatycznej, a od roku 2007 w audycie i kontroli, zajmując się audytem systemów informatycznych. Ekspert Komisji Europejskiej ds administracji CIP Policy Support Programme – Cyfrowej Agendy dla Europy. Wieloletni pracownik Politechniki Warszawskiej i Instytutu Podstaw Informatyki PAN. Od 1990 do 1995 roku pracował w United Nations Development Programme – Organizacji Rozwoju ONZ, jako Programme Officer w Turcji, Rumunii i Słowacji oraz Polsce, gdzie odpowiadał za systemy informacyjne monitorujące realizację programów w tej Organizacji. Uczestniczył w realizacji projektu CAPERS IST-1999-20733- Key Action 2 – New Ways of Working and Electronic Commerce projects and activities, którego celem było wdrożenie technologii RFID. W latach 2002-2004 kierownik programu ACTIN Acquis Communautaire Training Initiative w Brukseli. Jest wiceprezesem ACFE Chapter Poland #183 i członkiem Polskiego Towarzystwa Informatycznego oraz ISSA Polska.

Michał Hornowski
Inżynier centrum danych
Grupa PZU

Pracował jako: konstruktor układów scalonych, programista, administrator bezpieczeństwa informacji w firmach ubezpieczeniowych, nauczyciel akademicki, administrator systemów operacyjnych i baz danych. Stale współpracuje z organizacjami pozarządowymi: ISSA Polska, Polskie Stowarzyszenie Pedagogów i Animatorów KLANZA. Dewiza informatyczna: "Miej logi i patrzaj w logi."

Beata Janiuk

Prawnik, wieloletni i doświadczony pracownik w administracji samorządowej, mający w swym doświadczeniu zawodowym pracę na stanowisku legislatora, a obecnie pracownik wydziału zamówień publicznych. Absolwentka Wyższej Szkoły Handlu i Prawa im. R. Łazarskiego, ukończyła także Szkołę Główną Handlową – Podyplomowe Studium Zakupów i Zarządzania, Szkołę Wyższej Psychologii Społecznej – Podyplomowe Studium Bezpieczeństwa Wewnętrznego, Szkołę Główną Gospodarstwa Wieskiego – Podyplomowe Studia Zamówienia Publiczne. Ogromnie zaangażowana w pomoc w procesie resocjalizacji i readaptacji społecznej, realizuje zadania kuratora sądowego, co stanowi trudną i ciężką pracę – ale, jak mówi, jest to jej żywioł. Lubi podróże i literaturę kryminalną.

Mariusz Juszczyk

Członek ISSA Polska, związany z branżą ICT od siedmiu lat. Na co dzień pracownik Hostersi Sp.z o.o., firmy zajmującej się zarządzaniem serwerami, wdrażaniem chmury obliczeniowej i cyberbezpieczeństwem. Autor cyklicznych badań szybkości ładowania najczęściej odwiedzanych serwisów internetowych w Polsce.

Beata Marek
Cyberlaw.pl

Beata specjalizuje się w prawie nowych technologii ze szczególnym uwzględnieniem prawa IT, prawa własności intelektualnej, ochrony danych osobowych i tajemnic prawnie chronionych oraz prawa kontraktowego w obrocie krajowym i zagranicznym. Posiada ponad 5-letnie doświadczenie w obszarze cyber-

przestępczości, cyberzagrożeń oraz bezpieczeństwa informacji. Zajmuje się przede wszystkim szacowaniem ryzyka prawnego (ocena zgodności) oraz obsługą prawną projektów jak i całych spółek z sektora TMT (Technologie, Media, Telekomunikacja). Jeden z pierwszych prawników w Polsce wprowadzających na polskim rynku rozwiązania biznesowe oparte o bitcoin i blockchain i poruszających zagadnienia odpowiedzialności i funkcjonowania e-pomocników (maszyn samouczących się). Beata zo-stała wyróżniona m.in. współpracą z Berkman Center for Internet & Society na Harvard University. Dyrektor ds. prawnych w ISSA Polska – Stowarzyszeniu do spraw Bezpieczeństwa Systemów Informacyjnych, wiceprezes Cloud Security Alliance Polska, członkini Fundacji Bezpieczna Cyberprzestrzeń, a także International Cyber Threat Task Force. Pomysłodawca bloga dla przedsiębiorców i programistów – **cyberlaw.pl**

Maksymilian Michalski

Od wielu lat zajmuje się szeroko rozumianym bezpieczeństwem przetwarzania informacji. Przez większość pracy zawodowej związany jest z projektami informatycznymi i nowinkami technologicznymi wprowadzanymi do firm gdzie dba o ich bezpieczeństwo. Swoją pasję związaną z różnymi obszarami bezpieczeństwa IT realizuje także jako członek Stowarzyszenia Administratorów Bezpieczeństwa Informacji oraz ISSA Polska.

Kamil Pszczółkowski
Stillsec

Ekspert ds. Bezpieczeństwa, posiada 12-letnie doświadczenie w projektowaniu, wdrażaniu i audytowaniu systemów Zarządzania bezpieczeństwem informacji (zgodnych ISO 27001), Zarządzania danymi osobowymi (zgodnych z UODO oraz aktualnie z RODO), Zarządzania ryzykiem (zgodnych z ISO 27005 i ISO 31000), Zarządzania ciągłością działania (zgodnych z ISO 22301 oraz Ustawą o zarządzaniu kryzysowym), Zarządzania usługami IT (zgodnych z ISO 20000 i ITILv3), Zarządzania tożsamością i kontrolą dostępu (IAM, IDM). Wykładowca Akademii Sztuk Wojennych (dawniej Akademii Obrony Narodowej) na Wydziale Bezpieczeństwa Narodowego, Instytut Inżynierii Systemów Bezpieczeństwa. Pełnił obowiązki Administratora Bezpieczeństwa Informacji w podmiotach z branży: medycznej, teleinformatycznej, informatycznej, administracji publicznej i e-commerce. Odpowiadając za bezpieczeństwo danych ponad 500 tys. Klientów oraz nadzorując ponad 6 tys. podmiotów, którym dane zostały powierzone. Kamil zarządzał projektami informatycznymi zgodnie z metodologią PRINCE2 dla organizacji zatrudniających powyżej 100 tys. pracowników oraz budżetów projektowych powyżej 30 mln PLN. Wdrożył ponad 80 systemów zarządzania bezpieczeństwem informacji, opartych o analizę i ocenę bezpieczeństwa przetwarzanych danych. Posiada następujące certyfikaty potwierdzające jego kompetencje: Audytor Wiodący ISO27001, Audytor Wiodący ISO22301, Audytor Wiodący ISO2000, CompTIA Advanced Security Practitioner (CSAP), ITILv3 Foundation, Lean IT Foundation, PRINCE2 Practitioner, Certified Internal Controls Auditor (CICA), Data Protection Coordinator, Inspektor BTI (ABW), IBM Security Qradar SIEM, UML Professional Advanced. Członek ISSA Polska.

Adam Ziaja

Od kilkunastu lat zajmuje się bezpieczeństwem IT od strony etycznych ataków jak i obrony. Aktualnie pracuje jako starszy konsultant cyberbezpieczeństwa w jednej z firm z tzw. wielkiej czwórki. Jest biegłym sądowym z zakresu informatyki z listy Sądu Okręgowego w Warszawie. W trakcie swojej kariery zawodowej pracował w informatyce śledczej, zespole reagowania na incydenty naruszające bezpieczeństwo (CERT) oraz jako tester penetracyjny (etyczny haker) w jednej z największych na świecie grup bankowych. Jest współautorem materiałów dydaktycznych Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA) poświęconych m.in. informatyce śledczej oraz cyberprzestępczości. Brał udział w ćwiczeniach ENISA Cyber Europe 2014 gdzie jako zespół zdobył pierwsze miejsce (ponad 100 zespołów z całej Europy). Posiada liczne podziękowania, za znalezione luki w zabezpieczeniach powszechnie znanych firm i instytucji, z którymi można zapoznać się na prywatnej stronie internetowej http://adamziaja.com. Członek ISSA Polska.

VIII. Zasady korzystania

Niniejsza publikacja stanowi zbiór dobrych zasad i nie jest oficjalnym dokumentem rekomendowanym przez jakąkolwiek organizację prawniczą. Tym samym stosowanie się do zasad w niej wyrażonych jest dobrowolne dla prawników i powinno zostać poprzedzone konsultacją z firmą informatyczną, w szczególności w zakresie stosowania zabezpieczeń.

Wydawca jak i autorzy nie odpowiadają za stosowanie się albo brak stosowania się do treści zawartej w niniejszej publikacji. Każdy czytelnik korzysta z zawartości na własny użytek i na własne ryzyko.

Publikacja dostępna jest nieodpłatnie w formacie .pdf, drogą elektroniczną. Zabrania się odsprzedaży czy wprowadzenia do obrotu, w tym rozpowszechniania w jakikolwiek sposób inny niż ustalony i zaakceptowany przez wydawcę. Zabrania się dokonywania samodzielnie jakichkolwiek zmian w dokumencie, przeróbek, modyfikacji, adaptacji bez pisemnej zgody wydawcy.

Zawarte treści nie stanowią oficjalnych, wiążących stanowisk firm, w których pracują autorzy. Jednocześnie jeżeli jakiś z tematów bardziej interesuje czytelnika, zalecany jest kontakt bezpośredni do autora lub ze Stowarzyszeniem ISSA.

Jeśli temat security jest Ci bliski albo chciałbyś, by zostało przeprowadzone szkolenie/warsztat w Twojej kancelarii, skontaktuj się e-mailem: **info@issa.org.pl**

Patronaty medialne

RADCA PRAWNY DWUMIESIĘCZNIK

specfile.pl

specprawnik.pl

HOSTERSI

FBI Polska
FUNDACJA BEZPIECZEŃSTWA INFORMACJI POLSKA