Bezpieczeństwo IT

Poradnik

ISBN 978-83-967081-0-6

ISSA POLSKA

The Information Systems Security Association **(ISSA)®** – to Stowarzyszenie non-profit osób związanych zawodowo z branżą bezpieczeństwa systemów informacyjnych liczące ponad 10 000 członków zlokalizowanych w kilkudziesięciu krajach na całym świecie. Centrala Stowarzyszenia znajduje się w mieście Vienna w stanie Wirginia w Stanach Zjednoczonych Ameryki Północnej.

ISSA Polska – Stowarzyszenie do spraw Bezpieczeństwa Systemów Informacyjnych, jest chapter'em (polskim oddziałem) globalnej organizacji ISSA, której celem – 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, a 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 Polska jest największym w Europie i jednym z najszybciej rosnących na świecie oddziałów Stowarzyszenia, wielokrotnie nagradzanym jako najlepszy Chapter Zagraniczny. W dużej mierze wynika to z faktu, że Stowarzyszenie tworzą nie tylko ludzie zawodowo związanych z cyberbezpieczeństwem ale dlatego, że bezpieczeństwo jest ich pasją a działając jako grupa przyjaciół starają się edukować, aby można było bezpiecznie poruszać się w Internecie.

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

Podręcznik, do którego przeczytania zachęcam to poszerzona kontynuacja wydanego w roku 2015 Poradnika dla Kancelarii Prawnych. Tym razem nie ograniczamy się do jednego zawodu ale piszemy szerzej dla wszystkich zainteresowanych bezpieczeństwem informacji. Powody dla których zdecydowaliśmy się na napisania znacznie zmienionej i poszerzonej wersji to sukces poprzedniego podręcznika, który dostępny był tylko w wersji elektroniczniej a sciągnięty został przez ponad 1200 zainteresowanych czytelników.

To wydanie dostępne będzie również w wersji drukowanej oraz dystrybuowane do wybranych bibliotek na terenie całego kraju, jako egzemplarz obowiązkowy, aby zwiększyć dostępność. Kolejny powód to fakt, że od roku 2015 dynamiczny rozwój cyberbezpieczeństwa spowodował, że zmieniło się bardzo wiele począwszy od sposobów zabezpieczenia urządzeń poprzez rozwój rozwiązań chmurowych aż do zmian w prawie – uchwalenie i wdrożenie przepisów dotyczących przetwarzania danych osobowych. Autorzy, którzy zaangażowali się w pisanie tej książki starali się unikać specjalistycznego słownictwa i nie stosowali aparatu matematycznego, ale starali się w sposób obrazowy i poprzez podanie przykładów praktycznych zapoznać czytelnika z problemami bezpieczeństwa informacji. Pamiętajmy że komputer i podłączenie do sieci Internet to z jednej strony szereg ułatwień w dostępie i przetwarzaniu informacji, a z drugiej znacznie większa możliwość wycieku informacji i stworzenia dostępu do posiadanych przez nasze systemy danych. W podręczniku pokazane są przykładowe ataki jak i sposoby im zapobiegania. Ponadto przygotowane są przykładowe listy kontrolne odbioru nowego systemu informatycznego jak i podstawowe informacje dotyczące bezpieczeństwa danych osobowych co może być przydatne w małej i średniej firmie, ale wiedza na ten temat może być pomocna w życiu codziennym.

Podziękowania należą się wszystkim autorom, którzy co warto podkreślić, nie tylko są ekspertami w swoich dziedzinach, ale także pasjonatami, którzy swój czas wolny od zajęć zawodowych poświęcili na pisanie tego podręcznika nie licząc na wynagrodzenie.

Mam nadzieję, że podręcznik spotka się z Państwa uznaniem

Grzegorz Cenkier
Redaktor

Szanowni Państwo,

Oddajemy w ręce Czytelników książkę **'Bezpieczeństwo IT. Poradnik'**, która została napisana przez Członków ISSA Polska – Stowarzyszenia do spraw Bezpieczeństwa Systemów Informacyjnych.

Znajdziecie w niej Państwo liczne tematy związane z bezpieczeństwem teleinformatycznym.

Przedstawiliśmy ogólne zasady bezpieczeństwa oraz kluczowe aspekty dotyczące zabezpieczenia urządzeń czy systemów informatycznych. Znajdziecie tutaj Państwo również informacje dotyczące usług chmurowych oraz przetwarzania danych osobowych. Szczególnie ciekawie prezentują się te rozdziały w których autorzy zamieścili informacje dotyczące ataków wraz z rekomendacjami jak się przed nimi obronić.

Mam nadzieję, że niniejsze opracowanie pomoże lepiej zabezpieczyć systemy komputerowe w firmach oraz domach Czytelników.

Gorąco polecam oraz życzę inspirującej lektury,

Mariusz Belka
Prezes Zarządu ISSA Polska

ISSA POLSKA

SPIS TREŚCI

I. OGÓLNE ZASADY BEZPIECZEŃSTWA: DOBRE PRAKTYKI

[B. Marek, M. Juszczyk, M. Hornowski]

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

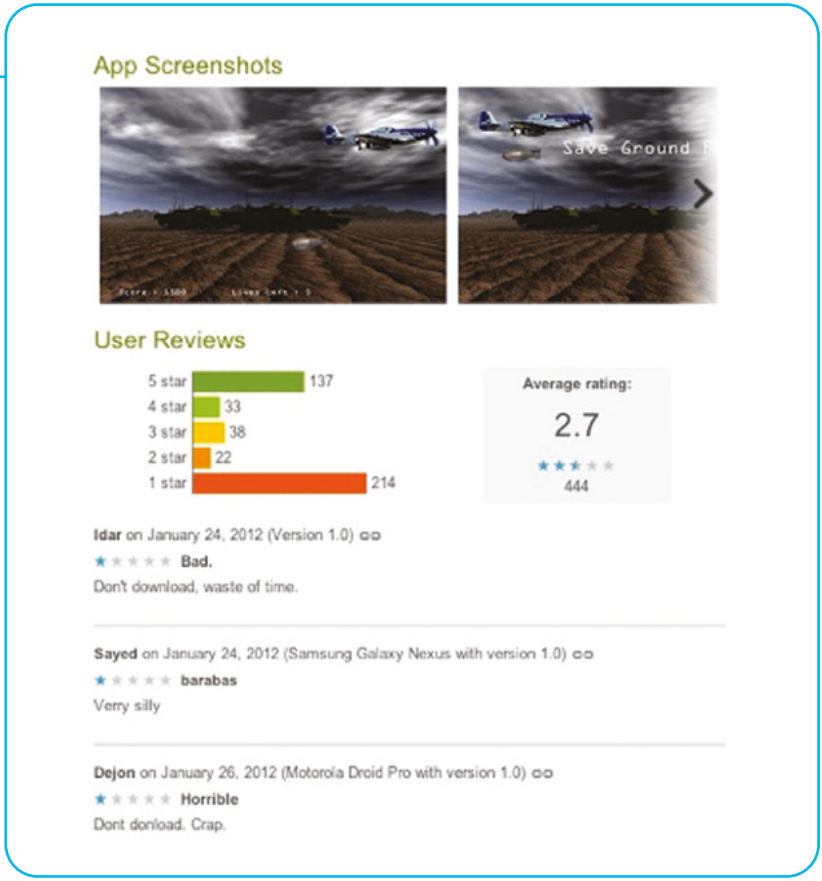
1 Pobieraj pliki tylko z zaufanych stron

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 liczbą ściągnięć i pozytywną ilość komentarzy). Nie pobieraj oprogramowania lub aplikacji z linków przesłanych w SMS. Za niezaufane strony należy uznać inne niż strony producenta. Niekiedy strony te wymagają ściągnięcia dedykowanego programu do instalacji programów komputerowych. Zdarza się, że 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 działania, które mogą prowadzić do szpiegowania Ciebie lub wysyłania ukrytych smsów. Dzięki dobrej praktyce pobierania możesz uchronić się od zainstalowania złośliwego oprogramowania, które podszywa się pod znane oprogramowanie albo jest programem wykonującym w tle nieautoryzowane czynności. Szczególnie uważaj przy pobieraniu darmowych programów. Czy wiesz, że cyberprzestępcy celowo umieszczają w sklepach internetowych takich jak np. Google Play, AppStore lub katalogach stron z różnymi programami komputerowymi, oprogramowanie które jest najczęściej bezpłatne i jednocześnie zainfekowane? Robią to w taki sposób, że tworzą fikcyjne konta w popularnych marke-

tach 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 informują o "wykryciu zagrożenia", potrzebie przyspieszenia komputera albo aktualizacji.

- Przykład aplikacji zainfekowanej, która została umieszczona jako darmowa gra na urządzenia z systemem Android. Użytkownicy wystawiali negatywne opinie oraz komentarze. Firma Symantec po zbadaniu aplikacji zgłosiła, że zawiera złośliwe oprogramowanie i aplikacja została usunięta[1].



1 http://www.computerworld.com/article/2500566/malware-vulnerabilities/massive-android-malware-op-may-have-infected-5-million-users.html

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 w czasie przeglądania Internetu bądź poczty gdy przestępca będzie chciał zainfekować Twój komputer utrudnisz mu to. Zastosuj tę praktykę do wszystkich komputerów w firmie.

Hasło do konta "administratora" powinno być znane tylko informatykowi, który opiekuje się zasobami IT w firmie. Inne osoby nie powinny go znać.

3

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. Zamiast tego do przechowywania haseł korzystaj z programów do tego celu stworzonych, tzw. menedżerów haseł. Hasło nie powinno być także powszechnie znane i dostępne dla wszystkich, którzy korzystają z infrastruktury komputerowej firmy. Daje to bowiem możliwość bezpośredniej ingerencji w zasoby IT organizacji i instalowania dowolnego oprogramowania przez pracowników.

Dzięki tej praktyce osoby nieupoważnione do instalacji 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 komputerze.

4

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

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

5

Szyfruj dane w obrębie całego dysku 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 nie będzie miała dostępu do danych Twoich klientów jeżeli nie będzie znała dodatkowego hasła dostępu.

6

Wykonuj regularnie kopie bezpieczeństwa i kopie zapasowe danych z Twoich urządzeń. W przypadku ważnych danych np. klientów pamiętaj, aby kopia była szyfrowana.

Wykonywane regularnie kopie zapasowe danych z wszystkich urządzeń (komputery stacjonarne, przenośne, urządzenia mobilne) zgodnie z procedurą bezpieczeństwa firmy są warunkiem utrzymania ciągłości działania. Stworzone kopie sprawdzane powinny być pod kątem poprawności wykonania oraz możliwości odtworzenia. W przypadku danych klientów, kopia bezpieczeństwa powinna 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 i przechowywany w bezpiecznym miejscu, innym niż komputer. 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 wykonywane nieregularnie zwiększasz ryzyko. Backup danych 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 - inaczej ułatwisz dostęp do wrażliwych danych osobom nieupoważnionym.

Dzięki tej praktyce będziesz mógł 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 czy gdyby teraz zniknęły dane o klientach, które posiadasz na dysku czy byś mógł 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 oraz decydować kto nie powinien mieć dostępu do niektórych informacji.

8

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

Korzystanie z firmowej poczty e-mail, którą dostarcza zaufany hostingodawca, stosujący protokół TLS oraz wieloskładnikowe uwierzytelnianie (MFA) 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 narażał na niebezpieczeństwo klientów oraz zawsze, w przypadku jakichkolwiek problemów z pocztą, możesz skorzystać ze wsparcia technicznego firmy hostingowej.

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

9

Korzystaj z wiarygodnego oprogramowania zabezpieczającego urządzenia używane w firmie. Pamiętaj by oprogramowanie to było zawsze aktywne (działało w czasie rzeczywistym). Sprawdź czy systemy operacyjne i urządzenia, z których korzystasz mają włączony firewall, czyli zaporę sieciową, chroniącą przed atakami.

Dzięki tej praktyce możesz zminimalizować ryzyko zainfekowania Twojego urządzenia lub zwiększyć szanse wykrycia złośliwego oprogramowania. Dobierz rodzaj oprogramowania zabezpieczającego (antywirusowego) do potrzeb firmy, szczególnie do rodzaju i ilości przetwarzanych danych.

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

Dzięki tej praktyce wypełniasz obowiązek prawny, a jednocześnie masz podstawę do pociągnięcia usługodawcy 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 organizacji spełniają niezbędne kryteria dla bezpiecznego i zgodnego z przepisami przechowywania danych osobowych.

11 Używaj nieoczywistych haseł składających się z co najmniej 12 znaków, w tym małych i dużych liter, cyfr i znaków specjalnych (np. Lubie!Zelki23). Dobrą praktyką jest gdy hasło składa się z niepowiązanych ze sobą wyrazów.

Używaj różnych haseł do każdego ze 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 firmy. W przypadku stosowania wielu silnych haseł pomocne są specjalne menedżery haseł.

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 WiFi, 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 firmy) to koniecznie zmień hasło administratora oraz wybierz w urządzeniu Wi-Fi sposób szyfrowania WPA3 lub WPA2 AES.

Dzięki tej praktyce zminimalizujesz ryzyko powodzenia ataku poprzez router.

14 Pracuj na danych klienta i sprawdzaj pocztę służbową wyłącznie na zaufanym urządzeniu spełniającym wymagania bezpieczeństwa akceptowane przez Twoją organizację.

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

Po odejściu pracownika z firmy upewnij się czy wszystkie dostępy do danych zostały mu zablokowane. 15

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

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

Dzięki tej praktyce będziecie mogli lepiej chronić dane klientów w obrębie firmy. Warto przeprowadzać 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 firmę 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 firmie.

Dzięki tej praktyce wprowadzisz jednolity standard bezpieczeństwa i ochrony danych klientów, a jednocześnie wypełnisz obowiązek prawny, zgodnie z którym każdy pracownik powinien mieć upoważnienie do przetwarzania danych osobowych oraz potwierdzić zapoznanie się i stosowanie się do zasad określonych w Polityce Bezpieczeństwa.

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 (tzw. filtry prywatyzacyjne), 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.

Odbieraj wydruki z drukarek od razu po ich wydrukowaniu, a jeśli to możliwe skonfiguruj drukarkę tak, by zlecenie było drukowane dopiero po zautoryzowaniu się na drukarce (PINem, kartą dostępową itp.). 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

1. Informacje wprowadzające

[K. Pszczółkowki, B. Marek]

Pracownik, 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 powinny być odpowiednio zarządzane i autoryzowane. Zalecane jest, by osoba odpowiedzialna za bezpieczeństwo zdefiniowała wymagania w zakresie bezpiecznego korzystania z urządzeń, zarówno tych należących do firmy jak i prywatnych, wykorzystywanych do pracy. Nie musi być jednak stosowana forma nadzoru nad pracownikiem obejmująca monitoring jego pracy. Chodzi raczej o posiadanie wiedzy nad tym 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 firmy, czy urządzenia służbowe można wynosić poza miejsce pracy, na jakich zasadach można korzystać z aplikacji chmurowych do pracy grupowej). **Źródłami definiowania wymagań bezpieczeństwa są:**

- Wymagania prawne (przepisy prawa);
- Wewnętrzne wytyczne i wymagania organizacyjne;
- Oczekiwania i potrzeby Klientów;
- Szacowanie ryzyka bezpieczeństwa informacji. Zdefiniowanie w jaki sposób korzystanie z urządzeń IT może wpłynąć na bezpieczeństwo danych przetwarzanych w firmie oraz wybranie adekwatnych mechanizmów bezpieczeństwa mających na celu minimalizację prawdopodobieństwa i skutków urzeczywistnienia się ryzyka.

Posiadanie urządzeń IT 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 organizacja miała zawartą umowę o świadczenie usług wsparcia technicznego, w tym zdefiniowanie czasu 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 firmy, a jego działania powinny być możliwe do skontrolowania tzn. wiemy co, gdzie i kiedy robił. Technik, w trakcie wykonywanie 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]

Wszelkie pliki zawierające dane, które nie powinny zostać publicznie udostępnione jak np. dane klienta, szczegóły operacji i inne wrażliwe 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 realnie odczytać jego zwartości (szyfrowanie jest w praktyce możliwe do złamania, jednak jest to bardzo ciężkie w realizacji czasowo i kosztowo ponieważ wymaga potężnych zasobów sprzętowych). Jest wiele metod szyfrowania. Warte uwagi są takie, które zapewniają:

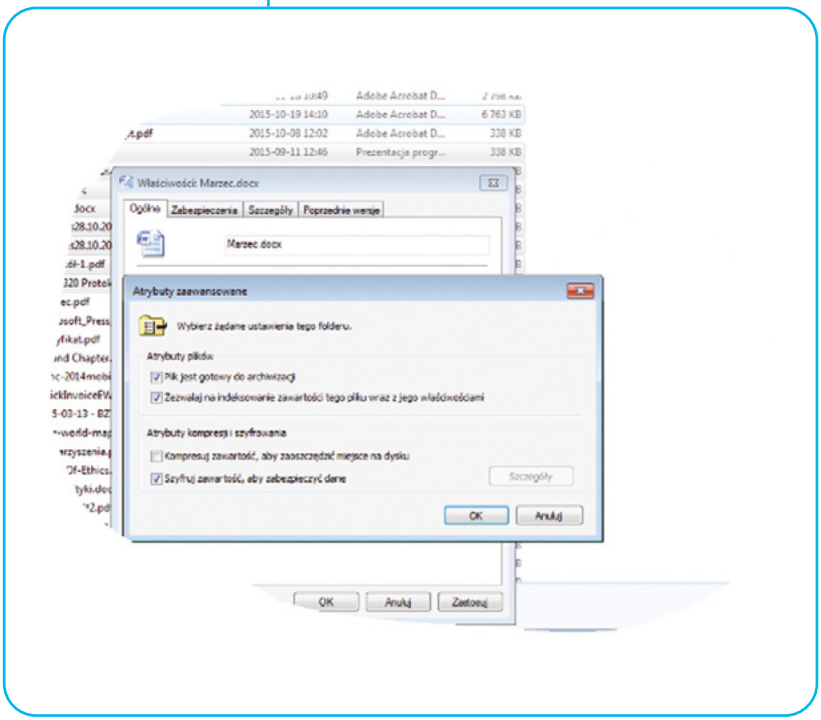
- szyfrowanie z poziomu systemu operacyjnego (dostępne dla Windows, MacOS i Linux),
- przesyłanie plików szyfrowanych programami typu PGP – jednak jest to rozwiązanie bardzo mało spopularyzowane wśród osób nietechnicznych i może prowadzić do wielu problemów natury technicznej,
- w pełni szyfrowane archiwum 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 w tym wypadku hasła do klienta w postaci SMS, a jeszcze lepiej przedyktowane w rozmowie telefonicznej.

Szyfrowanie plików

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 Eksplorator 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 poniżej).



Szyfrowanie folderów

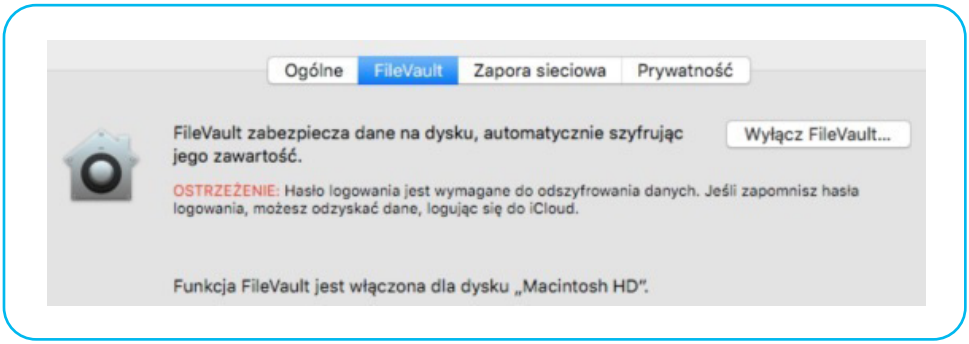
Szyfrowanie folderów jest ważne m.in. w sytuacjach, gdy z jednego komputera korzysta np. kilku pracowników a dokumenty zawierają dane chronione np. teleadresowe klientów. Ważnym jest, aby w takiej sytuacji każdy z pracowników miał własny folder z dokumentami. Folder należy zaszyfrować w taki sam sposób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

Szyfrowanie dysku

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 lub VeraCrypt itp., które szyfruje cały dysk. 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 one 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 sprawującego opiekę na systemem IT w firmie.

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:



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 sąsiada, np. zakupów w sieci na rachunek Twojej organizacji. 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 12 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:

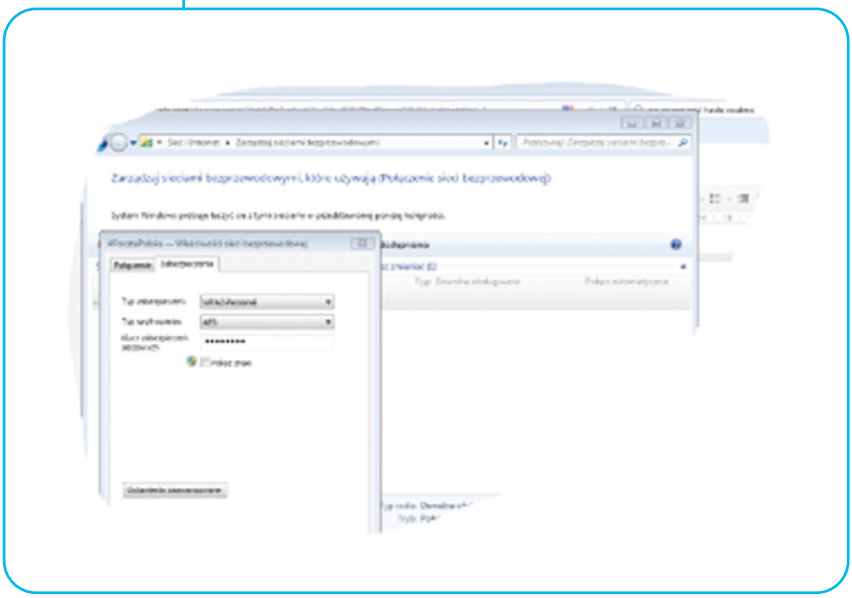
- **D-Link:** z poziomego menu wybieramy **Tools** i w polach **Admin Password** dwukrotnie podajemy nowe hasło. Klikamy na **Save Settings**.
- **Linksys**: z poziomego menu wybieramy **Administration**, a następnie w polu **Router Password** i polu poniżej dwa razy wpisujemy nowe hasło. Klikamy na **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 **WirelessSecurity**. 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** 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 (Default Gateway) – 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 warto uruchomić instrukcję ipconfig/all, aby sprawdzić czy sąsiad nie jest aktywnym klientem naszej sieci lokalnej.

4. Zasady dotyczące haseł

[K. Pszczółkowski]

Wszyscy pracownicy organizacji 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.

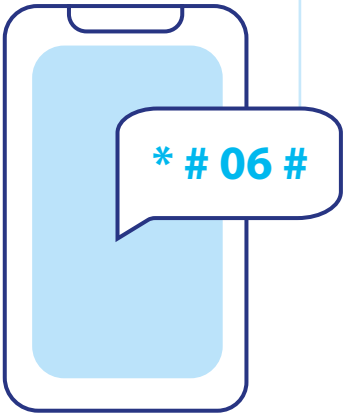
Polityka dot. zarządzania hasłami powinna zawierać następujące wymagania:

1. Hasło powinno składać się z minimum 3 rodzajów znaków tj. litery małe i duże, cyfry i/lub znaki specjalne (@#$%),
2. Minimalna długość hasła akceptowanego powinna wynosić 12 znaków,
3. 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,
4. Nowe hasło nie może być takie samo jak co najmniej 5 poprzednio użytych haseł,
5. Hasło musi być przechowywane w postaci niejawnej, dozwolone metody to silne szyfrowanie lub użycie funkcji skrótu. Administrator Systemu nie powinien znać hasła użytkownika.
6. W przypadku utraty hasła (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.
7. Administrator Systemu powinien się upewnić czy osoba która wnioskuje o zrestartowanie hasła jest osobą, za którą się podaje.
8. Konto użytkownika powinno być blokowane po kilku nieudanych próbach zalogowania się do systemu (nie więcej niż 3).
9. W przypadku braku aktywności użytkownika powinna być ustawiona blokada sesji/komputer powinien przechodzić w stan uśpienia.
10. Użytkownicy są zobowiązani do utrzymywania swoich haseł w tajemnicy. Nie wolno zapisywać haseł na papierze, w pliku lub urządzeniu przenośnym, nie wolno go również przekazywać Administratorowi Systemu, przełożonemu lub osobie zastępującej w czasie nieobecności
11. W przypadku podejrzenia możliwości ujawnienia hasła użytkownik zobowiązany jest je zmienić.

5. Jak wyłączyć skradziony telefon?

[G. Cenkier]

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



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 mieli by powodu 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 Wi-Fi, 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 na **NIE** oznacza to, że powinna zostać przeprowadzona rewizja Systemu Zarządzania Bezpieczeństwem Informacji.

7. Uwierzytelnienie wieloskładnikowe (MFA)

[G. Cenkier]

Jest jednym z najlepszych sposobów zabezpieczenia się przed dostępem osób nieupoważnionych, phishingiem, socjotechniką i kradzieżą uwierzytelnień a także skuteczną weryfikacją tożsamości użytkownika w jednym miejscu z określeniem wymagań pozwalających na udzielenie dostępu do aplikacji. Wykorzystując uwierzytelnienie wieloskładnikowe, co oznacza nie tylko podanie nazwy i hasła dostępu, ale też dodatkowego elementu np. SMSa otrzymanego na smartfon, biometrii czy klucza Yubikey, uzyskujemy wysoki poziom pewności, że dany podmiot jest w rzeczywistości tym, za którego się podaje.

III. USŁUGI CHMUROWE

[K. Grzela]

1. Informacje wprowadzające

Na całym świecie rośnie popularność "Cloud computing" co oznacza "pracę z danymi w zdecentralizowanym środowisku" nazywanych 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. Z uwagi na koszty, najczęściej wybierane są rozwiązania oparte o chmurę publiczną, rzadziej spotykane są rozwiązania hybrydowe. Zgodnie z definicją chmura obliczeniowa (ang. „Cloud Computing") to rozwiązanie oparte o model usługowy, pozwalający odbiorcom/klientom usługi (ang. „Cloud Customer") za pomocą sieci korzystać z zasobów należących do dostawcy usługi (ang. „Cloud Service Provider" – CSP) . Dzięki elastyczności modelu chmury użytkownicy mają dostęp do zasobów firmowych lub prywatnych z dowolnego miejsca na świecie za pośrednictwem urządzenia posiadającego dostęp do Internetu. Użytkownik ma możliwość dopasowania pakietu usług do bieżących potrzeb. Portfolio usług proponowanych przez dostawców ciągle się zmienia, dochodzą nowe usługi, istniejące usługi są konsolidowane w jedną, starsze technologie zastępowane są nowszymi, przez co obszar IT jakim jest chmura obliczeniowa podlega ciągłym zmianom i dlatego bezcelowym jest opisywanie szczegółowo dostępnych obecnie usług chmurowych. W ramach tego wprowadzenia do tematu przedstawiono ogólny model oraz kategorie usług proponowanych przez dostawców. Podejście to pozwoli łatwiej zrozumieć korzyści i zagrożenia wynikające z wykorzystania usług chmurowych w organizacjach, oraz samodzielnie podjąć próbę oceny rzeczywistości związanej z chmurą obliczeniową.

Modele usługi chmurowej

chmura publiczna (ang. „Public Cloud") – model usługi oferowany przez dostawcę dla szerokiego gremium odbiorców, oferowane usługi dostępne są dla wszystkich zainteresowanych. Nie oznacza to jednak, że jeśli organizacja zdecyduje się na ten model to dostęp np. do usługi infrastruktury (komputerów, serwerów, sieci) czy dedykowanych aplikacji będzie otwarty dla wszystkich z publicznego Internetu. Przy odpowiedniej konfiguracji można tak zarządzać dostępami, że będą one możliwe tylko dla

użytkowników, systemów i aplikacji z wewnątrz organizacji. Do głównych zalet tego modelu należy zaliczyć:

- łatwą konfiguracja,
- koszty wejścia w usługę są relatywnie niskie,
- skalowalność dla użytkownika końcowego,
- prawidłowo dobrane zasoby, gdzie klienci płacą jedynie za ich wykorzystanie.

chmura prywatna (ang. „Private Cloud") – to taki rodzaj chmury, który charakteryzuje się ograniczonym dostępem do zasobów. W tym modelu z zasobów chmury korzysta tylko jedna organizacja (firma) lub wybrani użytkownicy. Główne zalety rozwiązania:

- kontrola nad zasobami, może być wymagana dla zapewnienia zgodności z regulacjami i standardami.
- posiadanie rozwiązania w postaci infrastruktury i oprogramowania.

chmura zrzeszająca społeczność (ang. „Community cloud") – model ten powstał, żeby obniżyć koszty usług chmurowych dla organizacji o podobnym profilu działania, operujących na tych samych zbiorach danych i systemach. Ma on zastosowanie np. dla instytucji naukowych czy edukacyjnych.

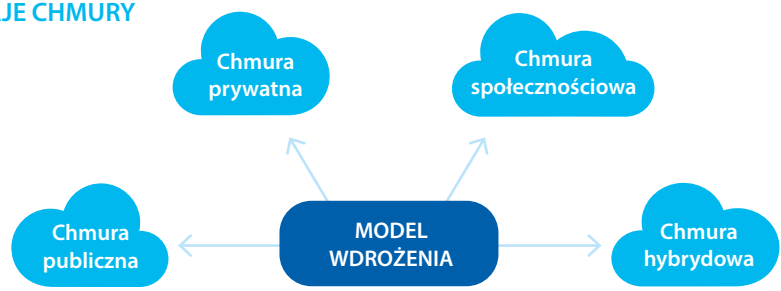
chmura hybrydowa (ang. „Hybrid cloud") – model ten jest połączeniem chmury prywatnej z chmurą publiczną, tak żeby spełnić konkretne wymagania organizacji. Do kluczowych zalet można zaliczyć:

- połączenie modeli w celi optymalizacji kosztowej, wydajnościowej czy w celu uzyskania zgodności z wymogami regulacyjnymi.
- skalowalność – to dotyczy każdego z omawianych modeli i typów usług, można więc powiedzieć, że dotyczy to generalnie chmury.

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.

Wiele jednoosobowych firm korzysta z chmury publicznej, należy jednak pamiętać, że większość tego rodzaju usług nie jest przeznaczona dla biznesu. Rekomendowanym podejściem jest zakup usługi w chmurze prywatnej, dedykowanej dla Twojej organizacji.

RODZAJE CHMURY



Korzystanie z rozwiązań chmury powoduje, iż odpowiedzialność za poszczególne elementy infrastruktury, systemy, aplikacje, obsługę informatyczną spoczywa na dostawcy, zależnie od wybranego modelu usług, np. infrastruktury sprzętowej, platformy do przetwarzania danych czy też aplikacji .

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 jest przechowywanie muzyki i zdjęć na iCloud – chmurze danych Apple, dokumentów na Google, udostępnianie plików przez Dropbox.

Kategorie usług chmurowych:

IaaS (ang. Infrastructure as a Service) – jest to jedna z podstawowych usług chmurowych, pozwalająca klientowi usługi na największą z możliwych dla usług chmurowych personalizację. Kluczowe funkcje oraz korzyści wynikające z korzystania z usług typu IaaS:

- skalowalność pozwalająca zwiększać lub zmniejszać zasoby zgodnie z aktualnymi potrzebami.
- redukcja kosztów TCO (ang. Total Cost of Ownership), jest to przypadek, gdzie klient nie ponosi kosztów związanych z posiadaniem sprzętu fizycznego.
- gwarancja wysokiej dostępności, którą zapewniają dostawcy usług chmurowych poprzez redundancję zasobów.
- dostęp do zasobów bez względu na lokalizację.
- spełnienie wymagań bezpieczeństwa fizycznego (zabezpieczenia fizyczne, klimatyzacja, zasilanie awaryjne),
- wskaźniki mierzalnego zużycia pozwalają klientom na płacenie tylko za te zasoby, które zostały przez nich wykorzystane w danej jednostce czasu.

PaaS (ang. Platform as a Service) – usługa chmurowa opierająca się na dostarczeniu dla klienta platformy napisanej w odpowiednim języku programowania, zawierającej dedykowane biblioteki programistyczne, usługi i narzędzia wspierane w pełni przez dostawcę usługi. Kluczowe funkcje oraz korzyści wynikające z korzystania z usługi typu PaaS:

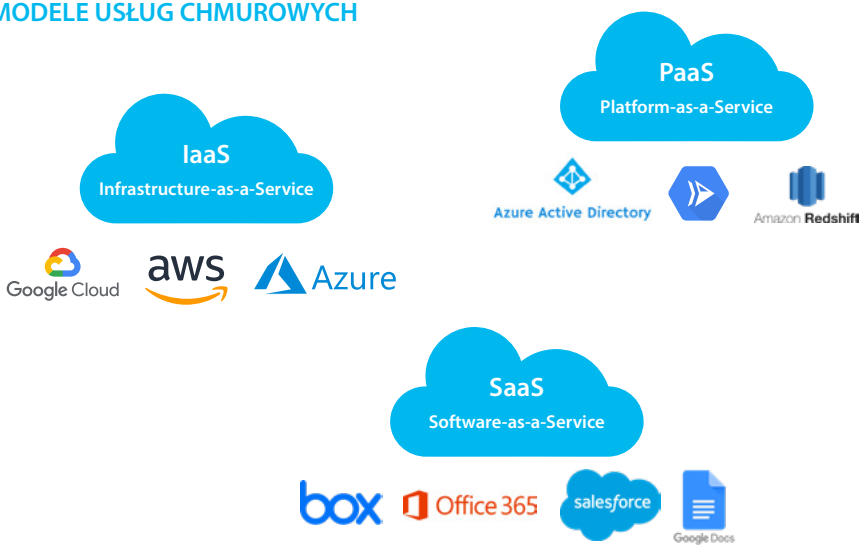
- autoskalowalność, opcja ta pozwala na takie ustawienie usługi chmurowej, że w przypadku jej przeciążenia automatycznie zostaną dodane do niej niezbędne zasoby w postaci procesora, pamięci RAM, dysku.
- elastyczność, która pozwala na przenoszenie usług pomiędzy dostawcami chmurowymi w zależności od potrzeb, pod warunkiem, że usługa spełnia zasadę łatwej przenoszalności pomiędzy platformami.
- łatwość aktualizacji, gdzie cały system operacyjny i platforma są zarządzane i tym samym aktualizowane przez dostawcę usługi w ramach jego odpowiedzialności. Przy tym aktualizacje środowiska nie powodują żadnych przerw technicznych, ani przestoju procesów biznesowych, tak jak ma to miejsce w tradycyjnych środowiskach IT podczas aktualizacji.
- rozwiązanie efektywne kosztowo, ponieważ klient płaci tylko za systemy i platformy, które w danym momencie wykorzystuje.
- licencjonowanie, gdzie to dostawca usługi w pełni odpowiada za dostarczenie odpowiednich licencji oprogramowania zarówno systemów operacyjnych jak i pozostałych komponentów oferowanej platformy.

SaaS (ang. Software as a Service) – jest to w pełni funkcjonalna aplikacja utrzymywana przez operatora usługi chmurowej dostarczana jego klientom w postaci usługi. Poniżej przedstawiono kluczowe korzyści płynące z użytkowania usług typu SaaS:

- redukcja kosztów całościowych, w tym modelu znacząco redukujemy koszty utrzymaniowe, które sprowadzają się do zakupu samej usługi, bez kosztów związanych z utrzymaniem infrastruktury, platformy oraz samej aplikacji.
- licencjonowanie, podobnie jak przy poprzednich typach usług, tu również klient nie odpowiada bezpośrednio za zakup i utrzymywanie licencji na wymagane oprogramowanie. Licencja jest wyliczona w ramach opłaty za usługę.
- łatwość użytkowania i administracji, gdzie administracja całością, począwszy od bezpieczeństwa fizycznego, poprzez wirtualizację, systemy operacyjne, platformę, na której świadczona jest usługa SaaS zostaje w gestii dostawcy usług chmurowych. W tym przypadku klient odpowiedzialny jest jedynie za odpowiednie nadanie dostępów dla użytkowników.
- standaryzacja, benefit ten zapewnia, że każdy użytkownik korzystający z usługi typu SaaS, korzysta przez cały czas z tej samej, zunifikowanej wersji aplikacji.

Dobór typu usługi zależy w dużej mierze od indywidualnych potrzeb klienta, jego dojrzałości oraz kultury organizacyjnej.

MODELE USŁUG CHMUROWYCH



ODPOWIEDZIALNOŚĆ STRON

Chmura prywatna	Infrastruktura jako usługa	Platforma jako usługa	Oprogramowanie jako usługa
Ludzie i dane	Ludzie i dane	Ludzie i dane	Ludzie i dane
Aplikacje	Aplikacje	Aplikacje	Aplikacje
Środowisko	Środowisko	Środowisko	Środowisko
System operacyjny	System operacyjny	System operacyjny	System operacyjny
Maszyna wirtualna	Maszyna wirtualna	Maszyna wirtualna	Maszyna wirtualna
Serwery	Serwery	Serwery	Serwery
Sieć	Sieć	Sieć	Sieć
Przestrzeń	Przestrzeń	Przestrzeń	Przestrzeń

2. Zagrożenia

Zanim organizacja 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 na pewno?

Poniżej 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)
- Publicznie dostępny interfejs zarządzający (poprzez Internet)
- Niepewność dotycząca usunięcia danych (brak kontroli nad nośnikami)
- Niejasne sposoby licencjonowania
- Nieautoryzowany dostęp do danych firmowych i klienckich
- Przenoszenie/przerzucanie 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 jest zbiorem otwartym.

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

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

Sprawdź czy dane, które chcesz przetwarzać w chmurzę 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 powinieneś zobowiązać dostawcę usługi chmurowej do przekazania pełnej informacji o wszystkich fizycznych lokalizacjach serwerów na których przetwarzane są lub mogą być przetwarzane dane, z obowiązkiem zachowania ich w obrębie Europejskiego Obszaru Gospodarczego. Informacja o zmianie lokalizacji powinna być przekazywana z rozsądnym wyprzedzeniem, tak by podmiot ten mógł rozważyć nie tylko wymagania wynikające z zasad ochrony danych osobowych, ale również z zasad ochrony tajemnic prawnie chronionych oraz ewentualnych innych wymagań.

1 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, a nawet ich zawartość. W skrajnych przypadkach osoba zamieszczająca dane zezwala, akceptując regulamin, na wykorzystanie treści dokumentów lub też na ich upublicznienie.

2 Zabezpieczaj dane przed dostępem osób nieuprawnionych

Przed wysłaniem do chmury danych, które mają pozostać poufne, zaszyfruj te dane. Szyfrowanie danych niezależnie od miejsca ich przechowywania zawsze zwiększa ich bezpieczeństwo poprzez zapewnienie ich poufności i integralności.

3 Zabezpieczaj informacje dotyczące dostępu do danych

Nie ujawniaj i zabezpieczaj klucze szyfrujące, nazwy użytkowników i hasła do usług chmurowych. Tak samo jak w przypadku danych gromadzonych lokalnie ich ujawnienie lub pozyskanie przez osoby nieuprawnione może ciebie i twoich klientów narazić na poważne straty finansowe i wizerunkowe.

4 Przeczytaj uważnie umowę określającą podmioty świadczenia usług

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

5 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 podczas transmisji (uwaga – w niektórych krajach zabronione jest przesyłanie i składowanie zaszyfrowanych danych lub też jest gwarancja dostępu do danych przez służby specjalne), 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). Dostawca usługi chmurowej powinien być zobowiązany do raportowania w określonym czasie wszystkich incydentów bezpieczeństwa danych, ze szczególnym uwzględnieniem tych, które dotyczyć mogą danych osobowych przetwarzanych w chmurze, a także powinien udzielić wszelkiej możliwej pomocy przy zwalczaniu skutków takich incydentów bezpieczeństwa.

6 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 płatności 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).

7 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.

8 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.

9 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.

10 Świadomie korzystaj z usług

Jeżeli nie posiadasz wiedzy lub nie rozumiesz działania usług chmurowych, to zanim z nich skorzystasz 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.

11 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 w przestrzeń publiczną 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 dookoła wszystkich co, gdzie i z kim robisz oraz czego używasz – czytają to także przestępcy i twoja konkurencja.

12 Przygotuj plany Ciągłości Działania i Reakcji na Sytuacje Awaryjne

Po migracji, nawet częściowej, danych do chmury twoje obecne plany ciągłości działania i reagowania na sytuacje awaryjne staną się nieaktualne. Przygotuj i przetestuj plany uwzględniające środowisko chmurowe i wszystkie związane z tym zagrożenia (np. brak dostępu do Internetu).

! Stosuj dobre praktyki

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

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 skutkująca 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.

IV. WYMIANA INFORMACJI Z KLIENTEM

1. Dlaczego przesyłanie wiadomości przez formularz na stronie po HTTPS jest bezpieczniejsze niż HTTP?

[M. Hornowski]

Transmisja danych przez Internet jest opisana przez zbiór reguł zwanych protokołami. Dzięki zgodności z protokołami różne produkty różnych firm mogą ze sobą współpracować.

Wszystkie przeglądarki jako postawę obsługują protokół HTTP. Nie jest on jednak dedykowany do systemu obsługi klientów. Do tego celu należy korzystać z protokołu HTTPS

Najważniejszą cechą HTTPS jest fakt że zapewnia:

- uwierzytelnienie odwiedzanej strony (np. że strona „Bank XYZ" należy do tego banku XYZ)
- ochronę tajemnicy, poufność (tylko my i druga strona wiemy jakie dane przesyłamy)
- integralność przesyłanych danych (nikt nie podmieni przesyłanych danych w drodze)

Z technicznego punktu widzenia, w HTTPS, mamy dwa ważne mechanizmy:

- szyfrowanie transmisji
- użycie certyfikatów

Szyfrowanie zgodnie z zasadami TSL jest szyfrowaniem asymetrycznym. System taki używa dwóch kluczy do szyfrowania komunikacji – klucza „publicznego" i klucza „prywatnego". Cokolwiek 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 mogą być 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 kolor paska adresu na zielony.

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 Twoja strona zapewnia także wiarygodność na takim poziomie?

Strony HTTP przekazują informacje otwartym tekstem i wiele osób może je podglądać, a nawet zmieniać po drodze. Jeśli chcesz zdecydować się na szyfrowanie pamiętaj o certyfikacie. Najlepiej jest mieć wystawiony przez powszechnie znaną zaufaną stronę trzecią.

Zmieniając HTTP na HTTPS zyskujesz:

- pewność dla klientów że odwiedzają Twoją stronę
- tajemnicę i pewność wymiany danych
- zwiększoną wiarygodność, ale nie gwarancję, że dana strona jest bezpieczna, ponieważ wiele jest stron wyłudzających dane, podszywających się pod inne strony np. banków, czy zawierających linki do złośliwego oprogramowania.

Jeżeli chcesz skorzystać z HTTPS skontaktuj się z informatykiem czy dostawcą usługi hostingowej – 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 rozszerzeniu ".doc" / ".docx" / ".pdf" etc. Można podzielić je na dwie grupy. Pliki małej wagi i pliki o większym znaczeniu dla klienta. Zastanów się czy w razie wycieku informacji zawartych w danym pliku przy ich przesyłaniu i zapoznaniu się z nimi przez osoby niepowołane klient poniesie szkodę albo dojdzie do naruszenia prawa, np. przepisów o ochronie danych osobowych lub umowy z klientem. Mając to na uwadze pliki o większym znaczeniu, tj. zawierające dane osobowe, poufne czy wrażliwe dla klienta, trzeba szyfrować. Pliki przesyłane pomiędzy serwerem poczty organizacji a poczty klienta przekazywane są co do zasady " tunelem", który

nie jest zabezpieczony. Tylko w wyjątkowych przypadkach, gdy są odpowiednio skonfigurowane serwery pocztowe, jest inaczej. Warto pamiętać także, że fakt, iż serwer poczty firmowej wymaga bezpiecznego połączenia TSL nie oznacza, że wysyłane wiadomości e-mail wraz z załącznikami są zabezpieczone. Dopuszczalne jest wysyłanie prostych dokumentów albo dokumenty zaanonimizowane tj. pozbawione treści zawierających informacje na temat klienta, ale 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 wiele osób może zastanawiać się po co szyfrować dokumenty. Wszystko zależy od analizy ryzyka. Inne wymagania będą w przypadku gdy będą przetwarzane dane o stanie zdrowia pacjentów wraz z ich kartami pacjentów, a inne gdy będzie chodziło o umieszczenie tabeli zawierającej imiona i nazwiska pracowników oraz nr sprzętów do nich przypisanych. Podstawowym wymaganiem jest wybór zaufanego dostawcy, następnie weryfikacja bezpieczeństwa oraz zawarcie umowy powierzenia, a także regulaminu usług. Zwróć uwagę nie tylko na lokalizację siedziby dostawcy, ale na to w jaki sposób przetwarza dane swoich klientów i jak podchodzi do ich zabezpieczenia oraz przekazywania (np. czy dochodzi do przesyłania na serwery w różnych krajach).

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 organizacji. Może być to rozwiązanie komercyjne np. iCloud, OneDrive, czy Dropbox albo typu open source do przesyłania plików. W ten sposób na serwery firmowe będą przesyłane informacje od klienta oraz odwrotnie, a nie za pomocą chmury publicznej i tym samym rozwiązań szczególnie niezalecanych do stosowania w przypadku przekazywania poufnych danych. Jeżeli decydujemy się na przesyłanie plików za pomocą serwera organizacji 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 trwałe usunięcie 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 organizacji, na której znajduje się formularz kontaktowy jest szyfrowana (zaczyna się od https)		
2.	Korzystam z poczty firmowej z zawierającym po znaku @ nazwę domeny organizacji, 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 organizacji 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 zawierająca 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 organizacji.

V. PRZETWARZANIE DANYCH OSOBOWYCH ZGODNIE Z RODO

[B. Marek, G. Cenkier]

1. Obowiązki prawne

[G. Cenkier]

„Dane osobowe" to wszystkie informacje, które umożliwiają zidentyfikowanie osoby fizycznej (osoby, której dane dotyczą") a możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny np. PESEL, adres poczty e-mail czy poprzez inny identyfikator internetowy albo jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Informacje o osobie czyli dane osobowe chronione są na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. we wszystkich krajach Unii Europejskiej, gdzie obowiązuje ogólne rozporządzenie o ochronie danych, zwane w Polsce RODO, a w wersji anglojęzycznej znane jest pod nazwą GDPR (General Data Protection Regulation). Obejmuje ono swoim zastosowaniem wszystkie podmioty zarówno prywatne, jak i publiczne, które przetwarzają dane osobowe w tym także te jednostki, które świadczą usługi e-commerce. W Polsce dodatkowym aktem prawnym dotyczącym przetwarzania danych osobowych jest ustawa z dnia 10 maja 2018 r .o ochronie danych osobowych.

Podstawowe zasady ochrony danych osobowych muszą spełniać poniższe zasady:

- przetwarzane możliwe jest tylko zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (**zgodność z prawem, rzetelność i przejrzystość**);
- zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (**ograniczenie celu**);
- adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (**minimalizacja danych**);
- prawidłowe i w razie potrzeby uaktualniane, a dane osobowe, które są nieprawidłowe

w świetle celów ich przetwarzania, muszą być niezwłocznie usunięte lub sprostowane (**prawidłowość**);

- przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane (**ograniczenie czasu przechowywania**);
- przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (**integralność i poufność**).

Zgodnie z art. 4 pkt 7 rozporządzenie RODO pojęcie **Administrator Danych Osobowych (ADO)** oznacza organ, jednostkę organizacyjną, podmiot lub osobę decydującą o celach i środkach przetwarzania danych osobowych. Dla zapewnienia prawidłowego procesu realizacji powyższych zasad Administrator Danych Osobowych powołuje Inspektora Ochrony Danych Osobowych (IOD), Administrator jest odpowiedzialny za przestrzeganie przepisów dotyczących przetwarzania danych osobowych oraz ma obowiązek wykazać **rozliczalność przetwarzania**. Administrator lub podmiot przetwarzający zapewnia również odpowiednie środki organizacyjne i techniczne służące ochronie interesu lub podstawowych praw i wolności osoby, której dane dotyczą.

Wybór środków technicznych i organizacyjnych, zapewniających bezpieczeństwo przetwarzania danych osobowych uzależniony jest od: charakteru, zakresu, kontekstu i celów przetwarzania danych osobowych. Ważne są też **ryzyka naruszenia praw lub wolności osób fizycznych** oraz poziom wiedzy technicznej oraz koszt wdrażania tych środków. Wybór środków technicznych i organizacyjnych należy przeprowadzić: **na podstawie wyników szacowania ryzyka**, oczekiwanego kosztu wdrożenia i przewidywanych korzyści, wynikających z ich wdrożenia. Ważnym elementem systemu bezpieczeństwa danych osobowych jest poddawanie cyklicznym udokumentowanym przeglądom w sytuacji, gdy zmienia się ryzyko wynikające z operacji przetwarzania danych osobowych oraz aktualizować stosowanie do ryzyka system przetwarzania danych osobowych.

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 organizacji i obejmują dane co najmniej:

- pracowników, w tym aplikantów czy praktykantów,
- kandydatów do pracy albo na staż lub praktykę,
- klientów będących osobami fizycznymi albo osób upoważnionych do kontaktu po stronie klientów firmowych na potrzeby rozliczeń,
- danych o klientach, w tym danych o osobach trzecich, które są przetwarzane w związku z prowadzoną sprawą na rzecz klienta, 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 zbiór dotyczący rekrutacji etc.

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

1. **jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;**
2. **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;**
3. **jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;**
4. **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.**
5. **osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych.**

Obowiązki podstawowe

Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, zapewnić, aby dane te były:

- przetwarzane zgodnie z prawem;
- zbierane dla oznaczonych zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami;
- merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
- przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania;
- spełnienie obowiązków informacyjnych oraz innych opisanych szczegółowo poniżej.

Obowiązki informacyjne

Dane pozyskane bezpośrednio od osoby fizycznej

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

a) swojej tożsamości i danych kontaktowych oraz, gdy ma to zastosowanie, tożsamości i danych kontaktowych swojego przedstawiciela;

b) gdy ma to zastosowanie – danych kontaktowych inspektora ochrony danych;

c) celach przetwarzania danych osobowych, oraz podstawie prawnej przetwarzania;

d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f RODO – prawnie uzasadnionych interesach realizowanych przez administratora lub przez stronę trzecią;

e) informacjach o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

f) gdy ma to zastosowanie – informacji o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46 RODO, art. 47 RODO lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

Poza informacjami, o których mowa powyżej, podczas pozyskiwania danych osobowych administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:

a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

b) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

c) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) RODO lub art. 9 ust. 2 lit. a) RODO – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

d) informacje o prawie wniesienia skargi do organu nadzorczego;

e) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;

f) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informa-

cje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji

Powyższych punktów nie stosuje się, jeżeli:

- przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania;
- osoba, której dane dotyczą, posiada już te informacje.

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

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

- adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku;
- celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych;
- źródle danych;
- prawie dostępu do treści swoich danych oraz ich poprawiania;
- uprawnieniach 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;
- wniesienia sprzeciwu wobec przetwarzania 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:

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

- dane są przetwarzane przez administratora: podmiot niepubliczny realizujący zadania publiczne, organy państwowe, organy samorządu terytorialnego oraz przez państwowe i komunalne jednostki organizacyjne;
- osoba, której dane dotyczą, posiada informacje, o których mowa powyżej.

Wydawanie upoważnień i zawieranie umów powierzenia

Każdy pracownik 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 firmy. 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 firmie 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 podjął środki zabezpieczające proces przetwarzania danych, o których mowa w art. 32 RODO. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych;

Zabezpieczanie danych osobowych

- W celu zachowania bezpieczeństwa ADO lub podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki – takie jak szyfrowanie lub anonimizacja danych minimalizujące to ryzyko. Środki takie powinny zapewnić odpowiedni poziom bezpieczeństwa w tym ryzyko związane z przetwarzaniem danych osobowych – takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych.
- 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)
- jaka zapewniona jest kontrola przetwarzającego;
- co dzieje się z danymi po rozwiązaniu umowy oraz jak jest uregulowana płatność – np. czy powierzenie jest wliczone w cenę świadczonej usługi głównej.

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 Prezes Urzędu Ochrony Danych Osobowych (PUODO) uznał wiążące reguły korporacyjne to właśnie na nich.

2. Wymagania bezpieczeństwa dla systemu teleinformatycznego przetwarzającego dane osobowe

[K. Pszczółkowski]

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

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

B) Uwierzytelnienie z wykorzystaniem identyfikatora użytkownika oraz hasła;

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

D) Rejestrację zmian wykonywanych przez użytkownika na poszczególnych elementach zbioru danych osobowych;

E) Środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych;

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

G) Odnotowywanie daty pierwszego wprowadzenia przez użytkownika danych do systemu teleinformatycznego;

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

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

J) Informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia;

K) Automatyczne odnotowywanie przez system teleinformatyczny wykonywanych operacji na danych przez użytkownika tj.:

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

M) Sporządzanie i drukowanie raportów zawierających powyższe odnotowane informacje.

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

- Zarządzania użytkownikami (w tym zarządzania uprawnieniami);
- Zarządzania kopiami zapasowymi danych;
- Zarządzania przeglądami i konserwacją systemu oraz nośników informacji służących do przetwarzania danych;
- Opisu stosowanych metod i środków uwierzytelniania;
- Opisu przepływu danych (wejście, wyjście) między systemem teleinformatycznym, a innymi systemami teleinformatycznymi zewnętrznymi;
- 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 upoważnienie) tym samym powinna utracić prawo dostępu do tych danych zgromadzonych w systemie teleinformatycznym.

3. Zabezpieczenia organizacyjne dot. przetwarzania danych osobowych

[K. Pszczółkowski]

W celu zapewnienia bezpiecznego przetwarzania danych osobowych w firmie 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, płyt CD, pendrive) 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 opisano poniżej:

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 nowo zatrudniony pracownik przed dopuszczeniem 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 planuje przetwarzać dane osobowe

[K. Pszczółkowski]

a) 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 10 maja 2018 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, odzwierciedlających dane produkcyjne, danych testowych, przygotowanych specjalnie w celu przeprowadzenia testów akceptacyjnych.

b) 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 firmie, 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 zagwaran-

towana 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 firmie 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,testowania i przechowywania 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) nie pozostawianie 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, są uszkodzone lub nie można ich ponownie wykorzystać, muszą być niezwłocznie zniszczone w sposób uniemożliwiający odtworzenie zapisanych na nich danych.

6. 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 powinny być 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, powinny zostać zniszczone przy użyciu niszczarki lub wrzucone do metalowego kontenera przeznaczonego do niszczenia dokumentów.		
3.	Pracownik kończąc swój dzień pracy powinien wyłączyć komputer lub przynajmniej się z niego wylogować.		
4.	Każdy laptop, po zakończeniu dnia pracy, powinien być przypięty do biurka za pomocą stalowej linki, schowany do szafki zamykanej na klucz lub zabrany z sobą.		
5.	Szafki, w których przechowywane są dane osobowe, powinny zostać zamknięte na klucz, a klucz ten powinien zostać zabrany przez osobę upoważnioną lub odpowiednio zabezpieczony.		
6.	Pracownik nie może trzymać zapisanego loginu i hasła do komputera przy swoim stanowisku pracy.		
7.	Hasło do komputera znane jest pracownikowi i prawnikowi zarządzającemu i nie może on udostępniać go innym pracownikom, niezależnie od sytuacji.		
8.	Dokumenty nie są zostawione przy drukarce lub ksero albo skanerze bez opieki.		
9.	Pendrive służy do przeniesienia dokumentu, a nie do prowadzenia na nim archiwum (pendrive powinienem 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 musi pamiętać, aby zamknąć pokój i okna.		
11.	Osoby z poza firmy (tj. goście, kurierzy, dostawcy, serwisanci) nie poruszają się po siedzibie samodzielnie, muszą pozostać pod stałą opieką pracownika.		
12.	W czasie prowadzonej rozmowy w miejscu publicznym nie są wymieniane nazw 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 firmie został wdrożony Rejestr Czynności Przetwarzania Danych Osobowych (art 30 RODO)		
15.	Organizacja 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 ich odejścia zostały one cofnięte i anulowano dostęp do danych osobowych.		
17.	Administrator Danych Osobowych (ADO) wyznaczył osobę, która jest odpowiedzialna za nadzór nad przestrzeganiem przepisów o ochronie danych osobowych, a w razie potrzeby został powołany Inspektor Ochrony Danych Osobowych (IODA).		
18.	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.		
19.	Raz do roku przeprowadzany jest audyt stanu bezpieczeństwa pod kątem przetwarzania danych osobowych – RODO.		

Jeżeli zaznaczyłeś co najmniej jedną odpowiedź na **NIE** oznacza to, że powinna zostać przeprowadzona rewizja procesów przetwarzania i ochrony danych osobowych występujących w firmie pod kątem zgodności z przepisami RODO.

VI. PRYWATNOŚĆ W SIECI

[B. Gębura]

1. Wprowadzenie

Zachowanie prywatności w sieci to sytuacja, kiedy prywatne dane nie są przetwarzane ani ujawniane bez naszej zgody. Nie zawsze zależy nam na ukryciu informacji o sobie. Najlepszym przykładem są chociażby media społecznościowe, w których dzielimy się ze znajomymi (albo i nawet nieznajomymi) fragmentami swojego życia: zdjęciami z wakacji, opowieściami z podróży czy nietypowymi problemami, jakie napotkaliśmy w pracy. Zachowanie pełnej anonimowości w cyberprzestrzeni jest praktycznie niemożliwe, o czym najlepiej przekonało się wielu przestępców, którzy działali w Internecie licząc na to, że sieć zabezpieczy ich przed konsekwencjami swoich czynów. Istotne jest, żebyśmy mieli świadomość kto i jakie informacje zbiera na nasz temat, co z nimi robi i czy mamy wpływ na ograniczenie tych działań. Oczywiście, najczęściej kojarzy się to z ochroną danych osobowych i powszechnie znanym hasłem „RODO". Jest to słuszne skojarzenie, ale w tym kontekście chcę zwrócić uwagę na jeszcze jeden termin, który staje się coraz bardziej znany – doxing. Nazwa „doxing" powstała od angielskiego słowa „documents", w skrócie „docs", z tego powstało „dox" i działania z tym związane nazwano „doxing". Tym terminem określa się publiczne publikowanie prywatnych lub poufnych informacji znalezionych i zgromadzonych za pomocą źródeł, które są swobodnie dostępne w Internecie (tzw. OSINT– **O**pen **S**ource **INT**elligence).

Wśród najczęściej spotykanych celów działań osób zajmujących się doxingiem są:

- zastraszenie
- zniesławienie
- molestowanie
- odwet
- szantaż
- atak „spear phishing"
- dla „żartu"

Co gorsza, działania związane z doxingiem często nie ograniczają się tylko do osoby będącej celem, ale dotyczą także rodziny, przyjaciół i znajomych.

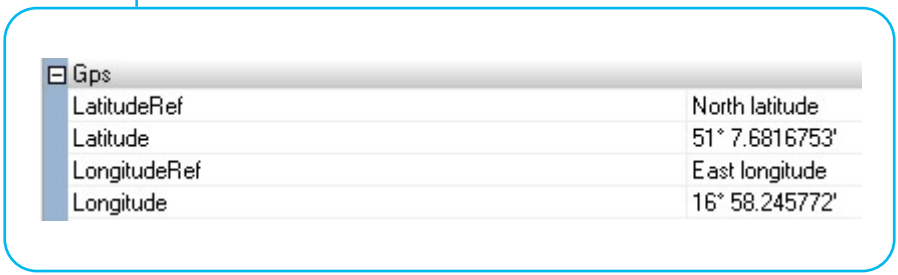
Chcąc chronić swoją prywatność i zapobiec doxingowi należy przede wszystkim zastanowić się, jakie informacje będą interesujące dla „dociekliwych". Dobrze jest samemu przejrzeć sieć szukając informacji, które mogą stać się punktem zaczepienia do kolejnych działań, np.:

- **imię i nazwisko** – może to być twoje prawdziwe imię i nazwisko, ale także wszelkie inne imiona i nazwiska, którymi posługujesz się publicznie (pseudonimy lub nicki),
- **numer telefonu** – często portale społecznościowe umożliwiają wyszukiwanie znajomych za pomocą ich numerów telefonów. Warto pamiętać o numerach służbowych lub dawniej używanych numerach telefonów,
- **adres e-mail** – jest to drugi z głównych sposobów wyszukiwania kontaktów w mediach społecznościowych. Co istotne, adres e-mail jest zazwyczaj elementem, który pozwala połączyć konta. Często adresy zawierają całe imię i nazwisko lub ich część. Należy wziąć również pod uwagę adresy e-mail, do których można łatwo dojść, nawet jeżeli adres nie jest używany publicznie (np. Antoni Góralski, o którym wiadomo że jest członkiem ISSA Polska, będzie miał zapewne adres antoni.goralski@issa.org.pl).

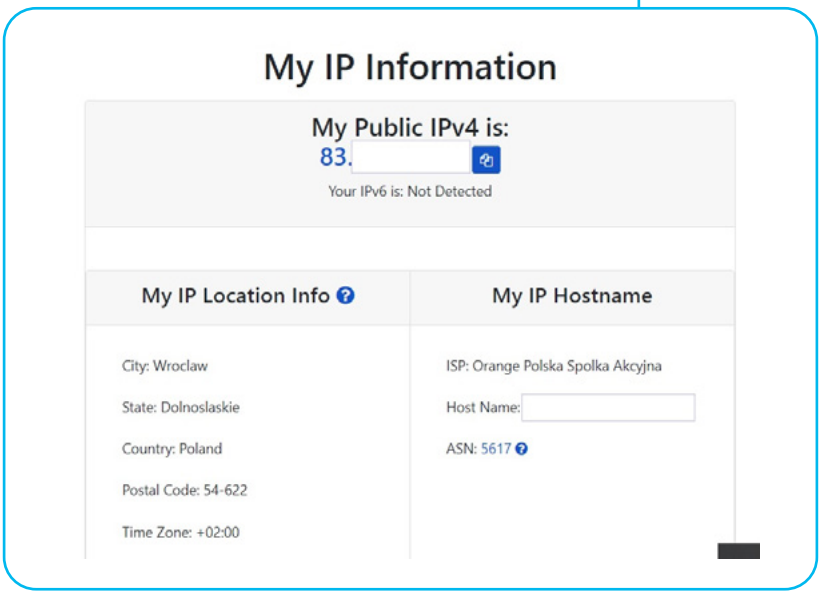
- **media społecznościowe** – nawet jeżeli z ostrożności nie udostępniasz swojego prawdziwego nazwiska lub lokalizacji, to inne informacje o tobie, takie jak miejsce pracy, do jakich grup należysz, kim są Twoi przyjaciele czy twoje zainteresowania pomogą zbudować twój profil.
- **lokalizacja**
- **fotografie** – często dostęp do prywatnych zdjęć jest głównym celem doxingu, ale zdjęcia mogą także posłużyć jako element łączący konta w różnych serwisach. Za pomocą stron takich jak TinEye.com, Yandex czy Google Grafika można zobaczyć gdzie użyto tego samego zdjęcia.
- **historia osoby** – znajomość faktów z przeszłości danej osoby może być pomocna przy zresetowaniu hasła, ale także może być wykorzystana do wyłudzenia informacji (np. „Cześć, pewnie mnie nie poznajesz, ale mieszkaliśmy w tym samym bloku na Krakowskiej").

Należy zwrócić uwagę na informacje pozwalające na tworzenie powiązań oraz na już istniejące powiązania takie jak np. oznaczenie osoby na fotografii w portalu społecznościowym. Pomimo, że osoba nie ujawniła swoich znajomych, dzięki takiemu oznaczeniu można dowiedzieć się z kim się spotyka lub czym się interesuje. Wielu informacji może także dostarczyć wiedza o przynależności do grup w serwisach społecznościowych.

Źródłem wielu ciekawych informacji mogą być opublikowane zdjęcia. Przed umieszczeniem zdjęcia w sieci warto przyjrzeć się szczegółom na drugim planie. Bywały przypadki, że w tle zdjęcia było widać kartkę z zapisanym hasłem lub dokument tożsamości. Także charakterystyczne elementy tła, jak np. budowle mogą pomóc w ustaleniu lokalizacji. Dodatkowo aparaty fotograficzne w telefonach komórkowych często zapisują współrzędne GPS w tzw. metadanych EXIF



W ustaleniu lokalizacji danej osoby mogę być pomocne również inne informacje, np. adres IP. Używając serwisu What Is My IP (https://www.whatismyip.com/) można z dość dużą dokładnością określić miejsce, w których znajdował się użytkownik Internetu



Dosyć często zdarza się, że ciekawe informacje (z punktu widzenia „dociekliwych") można znaleźć w archiwalnych zapisach serwisu internetowego prowadzonego przez daną osobę. Takie zapisy przechowywane są w serwisie Wayback Machine https://archive.org/web/web.php. Jeszcze niedawno nie przykładano dużej wagi do prywatności i publikowano informacje, którymi obecnie nie chcielibyśmy się dzielić, np. numer telefonu komórkowego czy prywatny adres e-mail.

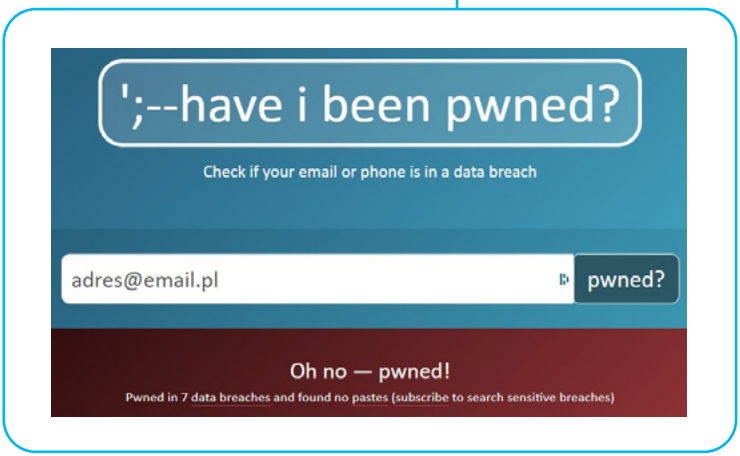
Mówiąc o zbieraniu informacji z otwartych źródeł nie można pominąć tak oczywistej kwestii jak wykorzystanie wyszukiwarek internetowych. Takie działania mają nawet swoją nazwę i są określane jako Google Dorking lub Google Hacking. Dla przykładu - firmy rekrutujące pracowników często przechowują CV kandydatów w plikach PDF o nazwie „imię nazwisko". Może się zdarzyć, że przez pomyłkę lub na skutek włamania taka baza będzie dostępna publicznie i dlatego warto sprawdzić, czy nasze CV również nie jest dostępne dla całego świata. Najprościej będzie wpisać w wyszukiwarce: „Imię Nazwisko" filetype:pdf. W sieci istnieją strony z gotowymi wzorcami zapytań. Kilka najczęściej używanych operatów pomocnych w wyszukiwaniu informacji przedstawiłem poniżej:

Operator	Zastosowanie	Przykład
site	Ogranicza wyniki tylko do określonej domeny	site:issa.org.pl
AND/OR	AND zwraca wyniki zawierające oba słowa (lub wyrażenia), OR zwraca te, w których występuje jedno lub drugie	"Adam Kowalski" AND (Wrocław OR Trzebnica)
gwiazdka (*)	Zastępuje słowo lub słowa	"Adam * Kowalski"
myślnik (-)	Wyklucza tekst następujący po operatorze	"Adam Kowalski" – Warszawa
filetype	Filtruje według rodzaju pliku, np.: DOC/DOCX, XLS/XLXS, PPT/PPTX, TXT, JPG/JPEG/PNG, PD	filetype:xls

Wyszukując informacje warto także skorzystać z wyszukiwarek innych niż Google, np. DuckDuckGo (https://duckduckgo.com/) czy Bing (https://www.bing.com/).

W trosce o swoją prywatność warto rozważyć usunięcie nieużywanych kont w serwisach internetowych (poczta, sieci społecznościowe, fora dyskusyjne itd.). Po latach problemem może okazać się przypomnienie sobie serwisów, w których zostały założone konta oraz to, jakie loginy zostały użyte. Pomocne może być przeszukanie poczty pod kątem wiadomości zawierających wyrażenia takie jak: potwierdź/aktywuj/zweryfikuj konto. Warto również korzystać z menadżera haseł.

Dbając o prywatność swoich danych dobrze jest co pewien czas sprawdzić, czy informacje takie jak hasła czy numer telefonu nie wyciekły. Najpopularniejszym serwisem, w którym można to sprawdzić jest Have I Been Pwned (https://haveibeenpwned.com/). Po podaniu adresu e-mail lub numeru telefonu serwis sprawdza, czy te dane nie figurują w którejś z baz zbudowanych z ujawnionych – zazwyczaj nielegalnie – informacji. W przypadku, gdy np. adres e-mail został znaleziony to zostaniemy poinformowani, z którym incydentem naruszenia danych jest związany ten adres oraz jakie dane zostały ujawnione



Istnieje także możliwość monitorowania całej swojej domeny internetowej i w przypadku, gdy w kolejnym wycieku pojawi się adres z tej domeny, to zostaniemy poinformowani o tym mailowo.

Prywatność w serwisach społecznościowych

Jednym z głównych miejsc, skąd „dociekliwi" mogą zaczerpnąć informacji o nas są serwisy społecznościowe. Często zdarza się, że nieświadomie udostępniamy więcej informacji lub szerszemu gronu odbiorców niż zamierzaliśmy. Z tego powodu warto co pewien czas sprawdzić ustawienia prywatności w wykorzystywanych serwisach. Poniżej przedstawiłem krótkie informacje o ustawieniach prywatności w najczęściej używanych usługach:

- **Google**

Ustawienia prywatności są dostępne pod adresem

https://myaccount.google.com/data-and-privacy

Można zażądać usunięcia z wyników wyszukiwania w Google informacji o sobie zawierających dane osobowe, w tym prywatnych zdjęć i danych kontaktowych (https://support.google.com/websearch/troubleshooter/3111061?hl=pl). Należy jednak pamiętać o tym, że usunięcie z wyników wyszukiwania nie spowoduje usunięcia danych z Internetu – nadal mogą być osiągalne.

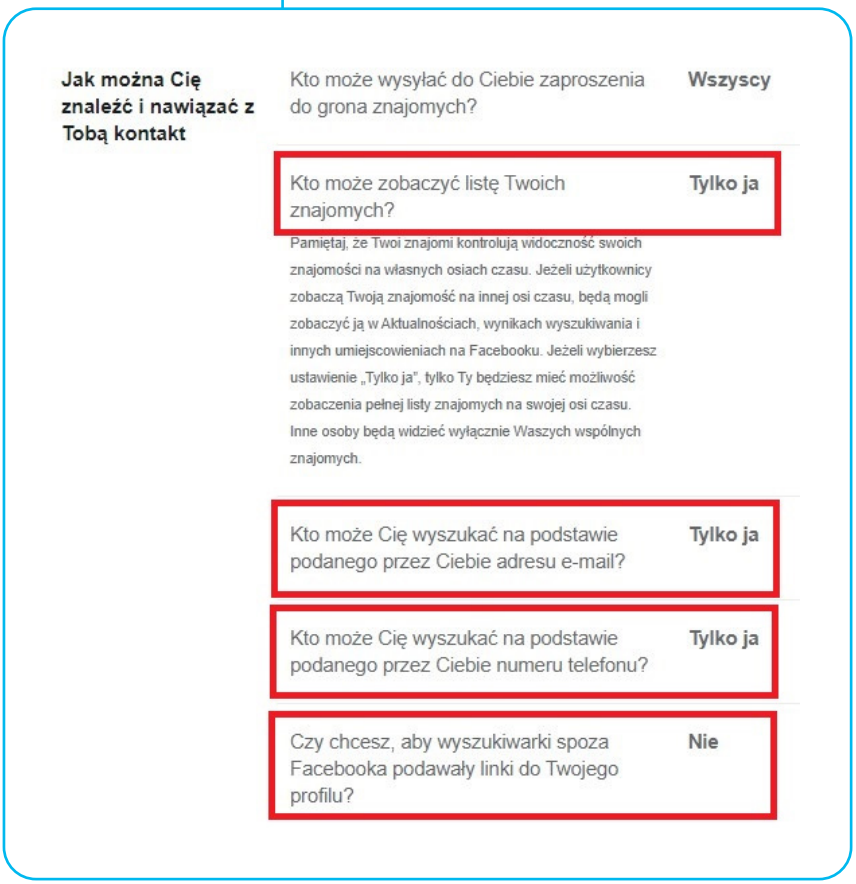
Google umożliwia ustawienie powiadomień w przypadku, gdy w wyszukiwarce Google pojawią się nowe wyniki związane z danym wyrażeniem. Można np. ustawić powiadomienie na imię i nazwisko. Więcej informacji można znaleźć pod hasłem „Alerty Google":

https://support.google.com/websearch/answer/4815696?hl=pl

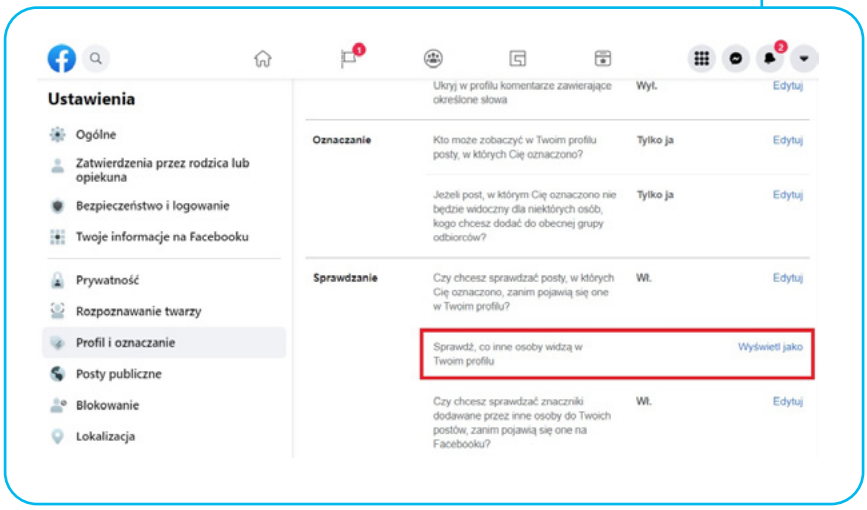
- **Facebook**

Link do ustawień: https://www.facebook.com/settings?tab=privacy

Warto zwrócić uwagę na ustawienie możliwości wyszukania na podstawie adresu e-mail lub numeru telefonu. Mając na uwadze swoją prywatność warto także ograniczyć możliwość wyświetlania listy swoich znajomych – te informacje mogą być bardzo przydatne w przygotowaniu ataków socjotechnicznych.



Facebook umożliwia sprawdzenie jak wygląda nasz profil z punktu widzenia innego użytkownika. Dzięki temu można zobaczyć, czy nie udostępniamy zbyt wielu informacji



- **LinkedIn**

W przypadku tego portalu zazwyczaj bardzo zależy nam na tym, żeby informacje o wpisanych osiągnięciach, umiejętnościach i przebiegu kariery dotarły do jak najszerszego grona odbiorców, z którymi jesteśmy lub możemy być powiązani zawodowo. Warto zwrócić szczególną uwagę na ustawienia profilu publicznego, czyli zdecydować jakie informacje będą dostępne publicznie, poza LinkedIn:

https://www.linkedin.com/public-profile/settings

- **Twitter, Instagram**

W przypadku tych serwisów, oprócz ustawienia prywatności warto sprawdzić co widać publicznie dla wszystkich użytkowników Internetu. Najprościej można to zrobić otwierając przeglądarkę w trybie prywatnym (incognito) i wpisując adres:

https://twitter.com/nazwa-konta lub https://www.instagram.com/nazwa-konta/

Na stronie Stay Safe Online, pod adresem

https://staysafeonline.org/stay-safe-online/managing-your-privacy/manage-privacy-settings/

jest dostępny zbiór linków prowadzących do ustawień prywatności w kilkudziesięciu najbardziej popularnych serwisach i aplikacjach. Warto tam zajrzeć!

Najlepsze praktyki, zalecenia, wskazówki

Ograniczenie udostępnianych informacji Należy pamiętać o tym, że najczęściej ujawniane są te informacje, które sami podaliśmy. Trzeba mieć na uwadze, że to co trafia do sieci, to najpewniej już tam zostanie i nawet jeżeli dostęp do danych został ograniczony (np. do grona bliskich znajomych), to może się zdarzyć, że na skutek ataku lub błędu ludzkiego dane zostaną ujawnione.

- Sprawdzenie ustawień prywatności w portalach społecznościowych, ograniczenie widoczności danych prywatnych tylko dla osób które są w naszej sieci znajomych. Ponadto staranne dobieranie osób który przyjmujemy do naszej sieci znajomych.
- Osobne konta e-mail w zależności od rodzaju danych
- Konto o wysokim priorytecie – szczególnie chronione, koniecznie z użyciem dwustopniowego uwierzytelniania, wykorzystywane do najważniejszej komunikacji.

Konto do odzyskiwania haseł – w niektórych serwisach internetowych można podać, na jakie konto będą wysłane linki do zresetowania hasła w przypadku, gdy zostanie zapomniane. Użycie osobnego konta zabezpiecza przed sytuacją, w której atakujący uzyskawszy dostęp do podstawowego konta pocztowego może zresetować hasła do serwisów internetowych.

- Konto do mediów społecznościowych
- Konto do ofert, programów lojalnościowych itp.

Aktualizacja systemu i przeglądarek – często atakujący uzyskują dostęp do prywatnych danych wykorzystując luki w systemach operacyjnych urządzeń (komputerów, telefonów) lub w oprogramowaniu takim jak np. przeglądarki internetowe. Zazwyczaj systemy same informują o konieczności aktualizacji i warto jest wyrazić na to zgodę. Najpopularniejsze przeglądarki aktualizują się same, ale dobrze jest sprawdzać, czy zainstalowane w nich wtyczki nie wymagają odświeżenia.

Stosowanie unikalnych i mocnych haseł – do każdego serwisu internetowego i konta pocztowego powinno być używane niepowtarzalne hasło. W ten sposób unikniemy sytuacji, w której atakujący po zdobyciu dostępu do jednego konta uzyska dostęp do innych serwisów. Zaleca się, aby hasło miało długość przynajmniej 12 znaków (rekomendacje CERT Polska można znaleźć pod adresem https://cert.pl/hasla/). Oczywiście, niemal nikt nie będzie w stanie spamiętać kilkunastu czy kilkudziesięciu haseł i dlatego zalecane jest stosowanie menedżerów haseł.

Włączenie dwustopniowego uwierzytelniania – polega to na tym, że do potwierdzenia tożsamości używane są dwa elementy z trzech grup:

- coś co wiem – np. hasło
- coś co mam – np. klucz sprzętowy, aplikacja „Authenticator", kod SMS,
- coś czym jestem – np. odcisk linii papilarnych, tęczówka oka

W praktyce najczęściej spotyka się połączenie hasła i kodów przesłanych SMS-em (coś co mam – telefon), kodów wygenerowanych przez aplikację typu „authenticator" (coś co mam – telefon),

klucza sprzętowego (coś co mam – klucz), odcisku palca (coś czym jestem). Stosowanie SMS-ów jest najsłabszym drugim czynnikiem, zdarzało się że oszust był w stanie wyrobić duplikat karty SIM i dzięki temu mógł przechwycić SMS-y. Bezpieczniejsze jest użycie aplikacji takiej jak „Google Authenticator" czy „Microsoft Authenticator". Z grupy „coś co mam" najbezpieczniejsze jest zastosowanie sprzętowego klucza USB takiego jak np. widoczny na zdjęciu klucz Ubikey.

- Blokowanie telefonu i komputera – pozostawianie urządzeń z otwartym dostępem umożliwia nie tylko przejrzenie informacji, które na nim znajdują się, ale także instalację złośliwego oprogramowania, które może być użyte do przechwycenia danych, reset hasła w aplikacjach jeśli dostępna jest poczta.

Źródło: https://www.yubico.com/

- Szyfrowanie nośników danych takich jak dyski, pendrive'y, karty pamięci.
- Sprawdzenie w telefonie uprawnień aplikacji, w szczególności dostępów do lokalizacji, mikrofonu, kamery, wiadomości.
- Skonfigurowanie funkcji antykradzieżowych i zdalnego czyszczenia na koncie Google/iCloud
- Sprawdzenie w sieciach społecznościowych czy ktoś nie podszywa się pod nas.
- Używanie w serwisach internetowych nazw kont, które nie wskazują na osobę

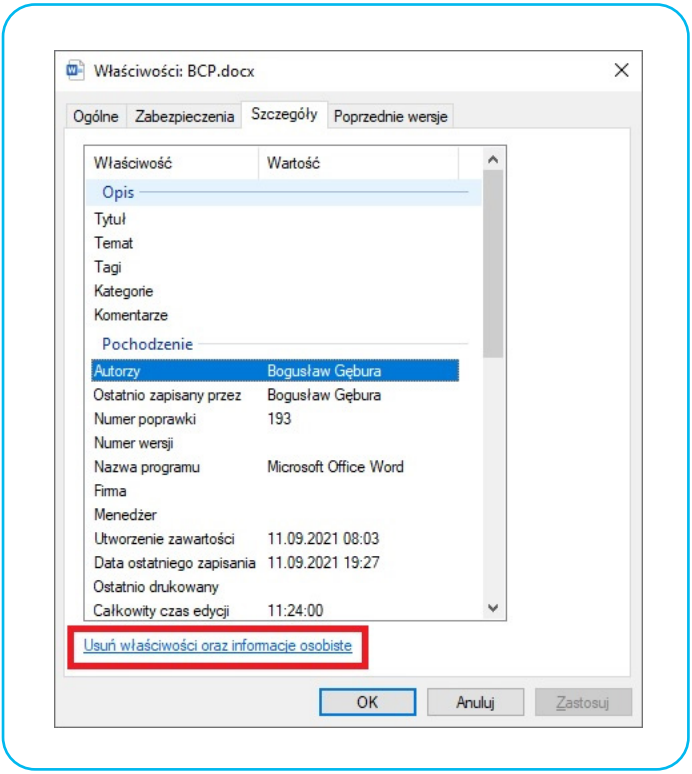
W przypadku podawania w sieci wrażliwych danych (np. haseł) koniecznie trzeba upewnić się, czy połączenie jest szyfrowane. W przypadku przeglądarki będzie to symbol kłódki przy pasku adresu. Samo szyfrowanie nie gwarantuje jednak bezpieczeństwa, ponieważ atakujący może stworzyć fałszywą stronę i stosując różne techniki zachęcić do wprowadzenia na niej poufnych danych.

- Należy bardzo ostrożnie korzystać z nieznanych sieci WiFi – lepiej nie przesyłać przez taką sieć poufnych danych. Gdy nie ma możliwości podłączenia się do zaufanej sieci, to bezpieczniejsze będzie skorzystanie z usług transmisji danych przez sieć komórkową.
- Usunięcie metadanych ze zdjęć i dokumentów – jak wspomniano wcześniej, do dokumentów i zdjęć zazwyczaj dołączane są dodatkowe, niewidoczne informacje, tzw. metadane. Mogą to być np. nazwisko autora dokumentu, nr wersji dokumentu czy czas i miejsce zrobienia zdjęcia. Przed udostępnieniem pliku dobrze jest sprawdzić jakie metadane zostały dołączone przez program, w którym został stworzony lub edytowany dokument. W systemie Windows można to sprawdzić uruchamiając Eksplorator plików – Właściwości pliku – zakładka „Szczegóły". W ten sposób nie zostaną jednak usunięte współrzędne GPS ze zdjęcia i do tego celu należy zastosować oprogramowanie zewnętrzne (np. EXIF Pilot).

- Warto rozważyć skorzystanie w przeglądarce z trybu anonimowego (incognito). W tym trybie przeglądarka nie zapisuje na dysku historii przeglądania, plików cookie ani informacji podanych w formularzach. Nie będą też wyświetlane reklamy dobierane na podstawie przeglądanych wcześniej stron. Należy jednak pamiętać, że tryb incognito nie zapewnia anonimowości – zarówno operator jak i administrator sieci, do której podłączony jest komputer będą mogli zobaczyć, jakie strony były odwiedzane. Większą anonimowość daje przeglądarka Tor, chociaż wyświetlenie strony przy jej użyciu trwa znacznie dłużej i nie wszystkie serwisy internetowe dopuszczają ruch pochodzący z sieci Tor (np. niektóre serwisy bankowe). Rozwiązania takie jak VPN dla ruchu http nie sprawią, że nikt nie będzie wiedział gdzie się łączymy. Wiedzę o tym będzie posiadał dostawca usług VPN.

- Zasłonki kamer wbudowanych w laptopy są już zjawiskiem powszechnym, ale warto jeszcze rozważyć użycie blokera mikrofonu. W ten sposób zostanie sprzętowo odłączony mikrofon wewnętrzny. Będzie to nas chronić przed ewentualnym podsłuchem.

- Jeżeli istotne jest zapewnienie wysokiego poziomu ochrony danych przekazywanych pomiędzy komputerami w sieci lokalnej, to należy za urządzeniem operatora w sieci LAN postawić własny router, do którego będą podłączone wszystkie nasze urządzenia. W ten sposób ruch z naszej sieci będzie widziany na urządzeniu operatora jako pochodzący tylko z naszego routera.



VII. PRZYKŁADOWE ATAKI I JAK SIĘ PRZED NIMI BRONIĆ

[P. Brogowski, G. Cenkier, M. Hornowski, B. Marek]

1. Kradzież sprzętu i wyciek danych

[P. Brogowski]

Utrata laptopa, czy smartfona (kradzież, zagubienie) nie należy do przypadków ataków cybernetycznych, ale jej rezultaty – utrata i przejęcie naszych danych są bardzo bliskie skutkom takich właśnie ataków, poświecimy im więc nieco uwagi. Utrata samego urządzenia, nawet tego z najwyższej półki, może mieć marginalne znaczenie, jak to przedstawiliśmy powyżej, w stosunku do utraty przechowywanych na nim danych.

Co się stało?

Stefan często odbywa podróże służbowe do swoich klientów, w które obowiązkowo zabiera ze sobą służbowego laptopa oraz tablet pomagający mu w codziennej pracy. Niestety w trakcie przerwy obiadowej został skradziony mu z samochodu cały ten sprzęt.

Co teraz się dzieje?

Organizacja w wyniku zajścia poniosła nie tylko straty finansowe w postaci utraty tabletu i laptopa, ale również ma poważne problemy prawne z uwagi, iż dokumenty przechowywane na służbowym sprzęcie posłużyły w szantażu jednego z klientów.

Jak można było tego uniknąć?

1 **Po pierwsze** powinniśmy cały czas zachowywać fizyczną kontrolę nad naszymi urządzeniami. Nie pozostawiajmy więc smartfona na dostępnym dla wszystkich biurku wychodząc do kuchni, czy łazienki, a zostawiając laptopa w pokoju hotelowym zabezpieczmy go przed kradzieżą np. przy pomocy **Kensington Lock**.

2 **Po drugie**, ustawmy odpowiednie zabezpieczenia programowe. A więc np. dla laptopa będzie to silne hasło, zabezpieczenie biometryczne (czytnik linii papilarnych lub sieci naczyń krwionośnych dłoni, rozpoznawanie twarzy), automatyczna blokada przy odchodzeniu od ekranu (czasowa lub lepiej – natychmiastowa przy wykorzystaniu wykrywania obecności naszego sparowanego z komputerem telefonu). Dla smartfona z kolei istotne jest ustawienie zarówno zabezpieczenia biometrycznego (TouchID, FaceID), jak i kodu, który będzie wymagany przy określonych czynnościach. Kod taki, nie powinien być przy tym zbyt krótki np. czte-

rocyfrowy, bo będzie on bardzo łatwy do złamania. Oczywiście bez sensu byłoby ustawianie długiego i złożonego hasła alfanumerycznego, które musielibyśmy wpisywać kilkadziesiąt razy dziennie, ale kod np. 8-cyfrowy wydaje się być rozsądnym kompromisem pomiędzy wygodą, a bezpieczeństwem. Pamiętajmy też o zabezpieczeniu kodem karty SIM, bo będzie to stanowiło dodatkową barierę dla złodzieja. Według Kaspersky Lab ponad połowa użytkowników (52%) nie ma w ogóle ustawionego hasła dla swojego smartfona. W takim wypadku, jeżeli smartfon zostaje skradziony, sprawca ma pełny dostęp do wszelkich naszych danych i kont. Często też w przeglądarkach ustawiamy zapamiętywanie haseł i automatyczne logowanie bez konieczności podawania danych uwierzytelniających, co jest bardzo wygodne, ale tylko do momentu, kiedy nie dojdzie do utraty naszego urządzenia. Zamiast tego należy korzystać z menadżera haseł, zabezpieczonego odpowiednio silnym hasłem.

3 **Po trzecie**, należy bezwzględnie korzystać z szyfrowania danych (zarówno na dysku, jak i na nośnikach zewnętrznych: kartach pamięci, modułach USB), dostępnego standardowo zarówno w Windows (funkcja BitLocker), MacOS (funkcja FileVault), jak i iOS (domyślnie) i Android (od wersji 6.0 powinno być włączone automatycznie, ale zależy to od producenta konkretnego urządzenia; w wersjach wcześniejszych należy tę opcję włączyć). Większość producentów laptopów umożliwia również szyfrowanie na poziomie niższym niż system operacyjny, uruchamianym w BIOS, przy wykorzystaniu zintegrowanego na płycie głównej modułu TPM (Trusted Platform Module). Można również wykorzystać szyfrowanie określonych katalogów lub plików przy pomocy licznych, w tym wielu bezpłatnych, programów (np. VeraCrypt, 7-Zip, AES Crypt i wiele innych). W przypadku korzystania z szyfrowania incydent związany z utratą komputera osobistego będzie wiązał się jedynie ze stratą w postaci sprzętu, a dane będą bezpieczne i niemożliwe do odtworzenia przez osoby niepowołane.

4 **Po czwarte** zabezpieczajmy dodatkowo (PIN'em, hasłem) newralgiczne aplikacje mobilne np. dające dostęp do naszych zasobów finansowych i danych osobowych.

5 **Po piąte** stosujmy wszędzie tam gdzie to tylko możliwe uwierzytelnienie dwu- lub wieloskładnikowe (2FT – Two Factor Authentication, MFA – Multi Factor Authentication). Jak podaje Microsoft tego typu zabezpieczenie zmniejsza prawdopodobieństwo udanego ataku na tożsamość o 99,9%. Istotne jest natomiast jaki czynnik wykorzystujemy dodatkowo przy autoryzacji. SMS-y z kodami nie są idealne, bo ktoś może je przejąć, albo w rezultacie ataku typu SIM-swapping (przejęcie karty SIM, najczęściej poprzez wyrobienie u operatora jej duplikatu), albo infekcji smartfona złośliwym oprogramowaniem. Lepszą, choć też nie idealną (bo podatną na niektóre ataki) opcją są specjalne aplikacje (Google Authenticator, Microsoft Authenticator, Authy), generujące jednorazowy i ważny tylko przez krótki czas kod bezpieczeństwa, który użytkownik musi wprowadzić oprócz loginu i hasła, aby uwierzytelnić się w danej aplikacji. Nawet jeśli uda się komuś uzyskać nasz login i hasło, to nie uzyska on dostępu do serwisu bez podania kodu, który zostanie wygenerowany w aplikacji jedynie na naszym smartfonie. Natomiast optymalnym rozwiązaniem w zakresie 2FA jest wykorzystanie specjalnego klucza zabezpieczającego U2F (Universal 2nd Factor – protokół wykorzystujący kryptografię asymetryczną, opracowany przez Google i Yubico – najbardziej znanego producenta tego typu urządzeń), którego musimy fizycznie dotknąć przy logowaniu. Według obecnego stanu wiedzy klucze takie nigdy nie zostały złamane i są one w stanie w 100% zabezpieczyć użytkownika przed przejęciem kont w serwisach, które rozwiązanie takie wspierają (np. GMail, Facebook, Twitter, Onet, WP, Amazon AWS, Github, Dropbox, Microsoft). Klucz można podpiąć do komputera lub

smartfona po USB (do iPhona przez złącze Lightning), ale zazwyczaj wystarczy zbliżyć klucz do obudowy smartfona, bo większość kluczy wspiera komunikację po NFC. Co istotne, klucze U2F komunikują się bezpośrednio z przeglądarką internetową, co oznacza, że są odporne na ataki z użyciem np. keyloggera, bo użycie klucza nie wymaga wciskania jakichkolwiek klawiszy na klawiaturze i przechwycenie danych tą metodą jest niemożliwe. Potencjalni hakerzy nie mogą też w tym przypadku skutecznie wykorzystać phishingu, bo do zalogowania się trzeba mieć fizyczny dostęp do klucza. Co więcej, ostatnio pojawiły się klucze U2F z dodatkowym zabezpieczeniem biometrycznym – odciskiem palca.

6 **Po szóste** – natychmiast zablokujmy u swojego operatora GSM kartę SIM skradzionego urządzenia. Dzięki temu część aplikacji, które umożliwiały płatność np. za bilety czy parking, nie będzie działać, gdyż wiele z nich powiązanych jest z numerem telefonu, a nie kartą kredytową. Poza tym złodziej nie będzie mógł wykonywać żadnych połączeń telefonicznych, a co ważniejsze nie będzie też miał możności wykorzystania kodów uwierzytelniających przesyłanych SMS'em.

7 **Po siódme** – zanotujmy i przechowujmy w bezpiecznym miejscu numer IMEI (International Mobile Equipment Identity). Jest to unikalny numer identyfikacyjny wszystkich urządzeń wykorzystujących łączność komórkową. Numer IMEI jest na trwałe przypisany do danego telefonu i nie można go zmodyfikować bez specjalnych narzędzi. Jest on niezależny od karty SIM i wykorzystywany w sieciach GSM do rozpoznawania poszczególnych urządzeń, co umożliwia ich trwałe zablokowanie w razie kradzieży lub zagubienia (jednak taka blokada działa tylko na terenie danego kraju). Jeżeli dojdzie do takiej sytuacji należy udać się na Policję i odebrać pisemne zaświadczenie o zgłoszeniu kradzieży telefonu, na którym podany będzie jego IMEI. Następnie trzeba pojawić się osobiście w salonie operatora i zlecić blokadę urządzenia. Numer IMEI jest najczęściej wygrawerowany z tyłu obudowy smartfona, a w niektórych modelach także na ramce do umieszczania karty SIM, ewentualnie pod baterią. Jest on również uwidoczniony na naklejce na fabrycznym opakowaniu urządzenia. Można go też znaleźć w aplikacji Ustawienia (dla iPhonów również w iTunes lub Finder), jak również wyświetlić na ekranie po wybraniu na klawiaturze w aplikacji telefonu kodu *#06#. Co jednak w przypadku jeśli nie zanotowaliśmy numeru IMEI, smartfon nam skradziono, a pudełko po nim dawno wyrzuciliśmy? W przypadku iPhone'a należy zalogować się swoim AppleID na stronie appleid.apple.com i w sekcji Urządzenia znajdziemy dane naszego smartfona. Dodatkowo, jeśli mamy dowolne inne urządzenie z systemem iOS (np. iPad), w jego Ustawieniach znajdziemy dane, w tym numery IMEI, wszystkich urządzeń powiązanych z naszym kontem Apple.

8 **Po ósme** – włączmy opcje znajdowania naszego smartfona. W przypadku telefonów z systemem iOS lokalizacja odbywa się za pośrednictwem chmury iCloud przy włączonej funkcji „Znajdź mój iPhone". Jej wybranie pozwala na: lokalizację urządzenia (nawet jeśli jest ono wyłączone), blokadę telefonu, wymazanie wszystkich danych z iPhone'a oraz towarzyszących akcesoriów. Co istotne funkcja ta nie korzysta z protokołu Bluetooth mającego bardzo ograniczony zasięg, ale z sieci wszystkich podłączonych do Internetu urządzeń z systemem iOS. W przypadku urządzeń z Androidem, należy zainstalować aplikację „Znajdź moje urządzenie", która określa lokalizację telefonu z dokładnością około 150 m. Aplikacja ta pozwala: zablokować zgubiony telefon, zadzwonić na niego, wylogować się z konta Google, skontaktować się z operatorem sieci komórkowej, wykasować dane z urządzenia. Aplikacja musi być jednak włączona zarówno na urządzeniu, z którego korzystamy podczas poszukiwań jak i na utraconym smartfonie, na którym musi być też zalogowane konto Google.

9 **Po dziewiąte** wreszcie – regularnie róbmy backup danych naszego komputera. Taki backup powinien być odpowiednio zabezpieczony (szyfrowanie, silne hasło) i przechowywany w bezpiecznym miejscu. Dobrą praktyką jest przechowywanie jednej kopii lokalnie np. na zewnętrznym dysku, a drugiej w chmurze np. iCloud (iPhone), czy Google Drive (smartfony z Androidem). Istotne jest też, aby oprócz kopii wykonywanej regularnie np. codziennie, dysponować również kopią danych z dawniejszego okresu np. sprzed miesiąca lub nawet kilku miesięcy. Nie ma to znaczenia jeśli odzyskujemy dane po utracie laptopa, czy smartfona, ale może być kluczowe w przypadku zainfekowania naszego urządzenia np. oprogramowaniem ransomware, bo taki fakt możemy wykryć dopiero po kilku tygodniach, czy nawet miesiącach, a to oznacza, że również dane na kopii zapasowej mogą być zainfekowane. Pamiętajmy też, że niektóre dane np. aplikacji autentykujących nie są ze względów bezpieczeństwa archiwizowane i trzeba odrębnie zadbać o możliwość ich odtworzenia poprzez wygenerowanie specjalnych QR kodów.

2. DDoS
[P. Brogowski]

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. Jak podaje Cloudflare, w 2021 roku jednemu na pięć planowanych lub zainicjowanych ataków DDoS towarzyszyło żądanie okupu, a liczba ataków tego typu w IV kwartale 2021 r. wzrosła w porównaniu z poprzednim kwartałem o 175%.

DDoS dla firmy to może być próba:

- zablokowania serwisu internetowego na jakiś dłuższy lub krótszy czas w celu uniemożliwienia pracy organizacji – co może skutkować utratą klientów oraz reputacji albo
- nie tylko zablokowania serwisu, ale także uzyskania dostępu, nieautoryzowanego rzecz jasna, do zasobów firmy. Atak typu DdoS może być pierwszą częścią zaplanowanego ataku.

Co się stało?

Jan, pracownik kancelarii prawnej, po długim oczekiwaniu zalogował się do poczty elektronicznej, gdzie przeczytał mejla z którego wynikało, że nieznana osoba grozi zablokowaniem strony internetowej kancelarii na długo, 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 teraz się dzieje?

Zaczyna panować powoli chaos bo pracownicy nie mogą pracować. Jan zgłasza sprawę do partnera zarządzającego i proponuje by skontaktować się z operatorem. Wcześniej, przeglądając stronę NASK, zapamiętał gdzie można zgłosić cyberatak. Jan otwiera stronę https://incydent.cert.pl 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 w jaki sposób mogą wdrożyć tego typu działania. Przed atakiem DDoS nie da się chronić na poziomie komputera osobistego. Mechanizmy ochronne blokujące niepożądany ruch sieciowy muszą zostać wdrożone na poziomie dostawcy usług internetowych (ISP – Internet Service Provider) lub na styku sieci naszej firmy z Internetem (blokowanie niepotrzebnego i nieprawidłowego ruchu sieciowego, wyłączenie rozgłaszania IP, wdrożenie firewalli aplikacyjnych i systemów wykrywających i blokujących ruch złośliwych botów itp.).

3. Phishing
[G. Cenkier]

Co się stało?

Stefan, pracownik kancelarii prawnej, znalazł w skrzynce poczty elektronicznej wiadomość o zapisaniu adresu e-mail do bazy mailingowej. Widniał napis „Jeżeli ta wiadomość Cię nie dotyczy, kliknij link, aby zapobiec wykorzystaniu tego adresu e-mail". Bez wahania kliknął.

Co teraz się dzieje?

Po kliknięciu w link Stefan został przekierowany na stronę, która przejęła zawartość całej skrzynki pocztowej, a tam znajdowały się przecież informacje o klientach firmy i ostatnio zawarte umowy, w tym inne istotne dla firmy informacje i dane osobowe klientów.

Jak można było tego uniknąć?

Stefan przed kliknięciem powinien sprawdzić czy w sieci ktoś już pisał o e-mailach o takiej treści. Zawsze może także zdefiniować w swojej poczcie ustawienie „To jest spam" i nie będzie otrzymywał wtedy wiadomości od tego nadawcy.

Jak rozpoznać phishing?

Nie jest to łatwe, bo czasem zarówno tekst jaki 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 fałszywe. Należy również przeczytać jakich działań oczekuje nadawca e-maila i ewentualnie potwierdzić telefonicznie żądanie, jeśli 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 7 elementów, które warto sprawdzać w przypadku otrzymania wątpliwego e-maila:

1 Nieprawidłowa nazwa w adresie nadawcy

Zagrożeniem może być mejl, 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 w niej sam tekst. Wiadomość też znacznie różni się 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 aktualizacji 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 wirusa.

Jeśli otrzymałeś fałszywy e-mail to:

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

4. Ransomware

[M. Hornowski, B. Marek]

Phishing opiera się na socjotechnice. Jest to takie stworzenie wiadomości by zachęcić do wykonania określonej czynności przez odbiorcę, np. kliknięcia w link, pobranie 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 Ryszard otworzył.

Co teraz się 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 email. 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 organizacja 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.

Informacja.

Twoja paczka nie zostala doreczona pod adres wysylki w dniu 2 grudzien 2015, poniewaz nikogo nie bylo w domu. Odebrac przesylke mozesz w dowolnym najblizszym biurze, pod warunkiem podania wydrukowanej informacji o przesylce.

Prosze zobaczyc pliku zalacznika. Nie klikaj ! Pobierzesz złośliwe oprogramowanie

Uwaga!

W razie jezeli paczka nie zostanie odebrana w okresie 30 dniu, firma nalicza oplate z tytulu przechowywania. W celu otrzymania dodatkowej informacji dotyczacej przechowywania i pobierania oplat, odwiedz nasza witryne.

Z powazaniem,
Poczta Polska.

To jest przykład masowych maili wysyłanych w celu nakłonienia do szybkiego kliknięcia zwykle w link lub pobrania pliku. Pobierając plik z załącznika tej wiadomości dane na Twoim dysku mogą zostać skasowane albo zaszyfrowane bez możliwości ich odzyskania nawet po zapłacie okupu dla przestępców. Przestępcy mogą także dostać się na Twoje konto bankowe lub/i podglądać Cię przez kamerę Twojego urządzenia lub nagrywać to co mówisz!

Przestrzegaj i edukuj znajomych

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 rzekomo nadawcą była organizacja 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 organizacja zdecydowała się na podjęcie szerokiej kampanii, w tym prasowej w celu wyjaśnienia tego zdarzenia w celu poprawienia swojego wizerunku.

6. Cyberstalking
[P. Brogowski]

Cyberstalking to używanie Internetu oraz wszelkiego rodzaju mediów elektronicznych do uporczywego nękania drugiej osoby. Cyberstalking może przyjmować różne formy i najczęściej będzie to: wysyłanie obraźliwych wiadomości e-mail, groźby lub obraźliwe komentarze przesyłane za pomocą komunikatorów lub mediów społecznościowych, groźby lub obraźliwe komentarze wypisywane na forach, kanałach tematycznych, grupach dyskusyjnych, podawanie się za kogoś i wysyłanie w jego imieniu wiadomości e-mail do znajomych, rodziny lub współpracowników, zachęcanie innych osób do prześladowania, zagrażania lub zniewagi, próby monitorowania czyichś działań poprzez zainstalowanie oprogramowania śledzącego, poszukiwanie wszelkich informacji o ofierze w Internecie mające na celu znalezienie takich, które mogą wprowadzić ofiarę w zażenowanie, ośmieszyć ją publicznie czy zepsuć jej kontakty zawodowe, rodzinne, towarzyskie, kradzież tożsamości związana nie tylko z podszywaniem się pod daną osobę, ale z próbą całkowitego przejęcia jej cech i właściwości. Stalking (po ang. „skradanie się", „podchody") w sieci jest formą przemocy. Jeżeli zatem spotykasz się z przynaj-

mniej jedną z poniższych sytuacji i nie jest to sytuacja incydentalna, to prawdopodobnie stałeś/stałaś się ofiarą cyberstalkera:

- ktoś wysyła do Ciebie wiadomości zawierające obelgi lub umieszcza na Twoim profilu obraźliwe komentarze,
- ktoś zachęca innych do blokowania Twojego konta lub zgłaszania administratorowi treści, które publikujesz,
- ktoś przerabia Twoje posty lub zdjęcia i publikuje je bez Twojej zgody w celu ośmieszenia cię,
- ktoś nęka Cię wiadomościami, SMS'ami i telefonami, mimo próśb, by tego nie robił,
- ktoś podszywa się pod Ciebie i publikuje treści, które Cię kompromitują, czy ośmieszają,
- ktoś rozpowszechnia nieprawdziwe informacje o Tobie,
- ktoś udostępnia w sieci Twoje dane osobowe, poufne informacje, intymne zdjęcia,
- ktoś kieruje pod adresem Twoim lub osób Ci bliskich groźby (nawet pośrednie lub zawoalowane).

Stalkerem jest najczęściej były partner, współpracownik, kolega z klasy. Jednakże może to być osoba zupełnie obca, w takim przypadku stalker wytwarza zazwyczaj wyimaginowany związek uczuciowy ze swoją ofiarą. Szczególnie narażone są osoby publiczne, gwiazdy filmu czy sportu, ale ofiarą mogą to być również osoby, które przypadkowo pojawiły się na drodze prześladowcy.

Jak można było tego uniknąć?

Należy pamiętać, że nie jesteśmy anonimowi w sieci. Trend udostępniania informacji, zdjęć swoich i swoich bliskich w Internecie powoduje, że potencjalny sprawca może z łatwością dowiedzieć się o wielu szczegółach naszego życia: z kim się spotykamy, kogo lubimy, a kogo nie, jakie są nasze poglądy polityczne, w jakich miejscach bywamy, jakie są nasze zainteresowania itp. Nie powinniśmy więc ujawniać w Internecie swojego adresu (pamiętaj, że metadane zdjęć, które zamieszczasz w Internecie zawierają standardowo koordynaty geograficzne miejsca wykonania zdjęcia), numeru telefonu, danych osobowych. Absolutnie nie należy używać jednego hasła do różnych uwierzytelnień (stron, portali, aplikacji), bo wyciek danych w jednym miejscu spowoduje kompromitacje naszych danych uwierzytelniających do wszystkich zasobów. Należy stosować uwierzytelnienie wieloskładnikowe, zwłaszcza z użyciem kluczy U2F, bo to zabezpieczy nas przed przejęciem przez cyberstalkera naszego konta mailowego lub w mediach społecznościowych. Trzeba być podejrzliwym w stosunku do e-maili i wiadomości od nieznanych nam osób oraz nie odpisywać na tego typu wiadomości, gdyż nawet odpowiedź z żądaniem zaprzestania korespondencji na co dziesiąty e-mail może być dla stalkera potwierdzeniem chęci utrzymywania z nim kontaktu. Najlepiej w sposób bezpośredni i zdecydowany wyrazić brak chęci dalszych relacji, zerwać wszelkie kontakty, a następnie nie odpowiadać już

na żadne wiadomości. Zachowanie tych kroków bezpieczeństwa uniemożliwi bądź poważnie utrudni cyberstalkerowi śledzenie naszych ruchów w cyberprzestrzeni. Ofiara cyberstalkingu powinna złożyć zawiadomienie o popełnieniu przestępstwa na Policji lub w prokuraturze. Należy jednak pamiętać, że aby doszło do skutecznego skazania sprawcy przestępstwa stalkingu sąd i organy ścigania muszą dysponować materiałem dowodowym potwierdzającym fakt przestępstwa. Dowodem takim będą SMS'y, e-maile, rejestr i ewentualne zapisy połączeń telefonicznych, nie należy więc kasować korespondencji elektronicznej otrzymywanej od sprawcy i dobrze jest nagrywać rozmowy telefoniczne z nim. W przypadku nękania na portalach społecznościowych, forach i czatach należy zrobić zrzuty ekranu (print screeny), oraz cyfrowe zapisy rozmów. Stalking oraz cyberstalking są karalne na podstawie art. 190a kodeksu karnego, zgodnie z którym:

§1 Kto przez uporczywe nękanie innej osoby lub osoby jej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności do lat 3.

§2 Tej samej karze podlega, kto, podszywając się pod inna osobę, wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej.

§3 Jeżeli następstwem czynu określonego w § 1 lub 2 jest targnięcie się pokrzywdzonego na własne życie, sprawca podlega karze pozbawienia wolności od roku do lat 10.

§4 Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

Należy jednak pamiętać, że stalking, aby podlegał penalizacji, musi mieć charakter ciągły i trwać przez dłuższy (choć nie zdefiniowany prawnie) czas. „Ustawodawca kryminalizuje tylko takie zachowania odpowiadające nękaniu, które mają charakter długotrwały. O uporczywym zachowaniu się sprawcy świadczyć bowiem będzie z jednej strony jego szczególne nastawienie psychiczne, wyrażające się w nieustępliwości nękania, tj. trwaniu w swego rodzaju uporze, mimo próśb i upomnień pochodzących od pokrzywdzonego lub innych osób o zaprzestanie przedmiotowych zachowań, z drugiej natomiast strony – dłuższy upływ czasu, przez który sprawca je podejmuje" („Kodeks karny. Komentarz", red. prof. dr hab. Alicja Grześkowiak, prof. dr hab. Krzysztof Wiak, 2021, wyd. 7). Oprócz uporczywości, działanie stalkera musi też wywoływać u pokrzywdzonego uzasadnione poczucie zagrożenia, poniżenia lub udręczenia lub istotnie naruszać jego prywatność. Istotne jest w tym kontekście, że poczucie zagrożenia musi być oceniane z obiektywnego punktu widzenia, nie zaś subiektywnego odczucia ofiary. Jak zaznaczył Sąd Najwyższy w uzasadnieniu wyroku z 29 marca 2017 r., sygn. akt IV KK 413/16 „…subiektywne odczuwanie zagrożenia przez osobę należy konfrontować z wiedzą, doświadczeniem i psychologią reakcji ogółu społeczeństwa, obiektywizować poprzez poczucie zagrożenia w danych okolicznościach, jakie towarzyszyłoby przeciętnemu człowiekowi, o ile oczywiście działania sprawcy nie zmaterializowały się w konkretnym skutku". Nie ma natomiast znaczenia motywacja sprawcy. Zgodnie z postanowieniem Sądu Najwyższego z 12 grudnia 2013 r., sygn. akt III KK 417/13 „prawnie irrelewantne jest w kontekście strony podmiotowej tego przestępstwa czy czyn sprawcy powodowany jest żywionym do pokrzywdzonego uczuciem miłości, nienawiści, chęcią dokuczenia mu, złośliwością czy chęcią zemsty".

VIII. CYBERHIGIENA

[P. Brogowski]

Cyberhigiena to zbiór zasad, zachowań i działań, które podnoszą nasz poziom bezpieczeństwa cybernetycznego. Podobnie jak w ramach ogólnych zasad higieny staranne mycie rąk chroni w znacznej mierze przed chorobami zakaźnymi, takimi jak choćby COVID-19, tak samo stosowanie w ramach cyberhigieny unikalnych haseł o odpowiedniej sile chroni przed nieuprawnionym dostępem do kont poczty elektronicznej czy serwisów społecznościowych. Keith Kirkpatrick w "Cyber policies on the rise", Communications of the ACM, vol. 58 (10) definiuje cyberhigienę jako „wdrażanie i egzekwowanie polityki ochrony prywatności i bezpieczeństwa danych, procedur i kontroli w celu zminimalizowania ryzyka potencjalnych szkód i naruszenia bezpieczeństwa danych". Z kolei Virgilio F. Almeida i współautorzy „Cyberwarfare and digital governance", IEEE Internet Computing, vol. 21 (2) określają cyberhigienę, jako „zbiór najlepszych praktyk, dotyczących bezpiecznego korzystania z sieci i ochrony urządzeń podłączonych do Internetu".

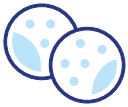
Wiele zaleceń dotyczących cyberhigieny zostało zawartych w rozdziale VII Przykładowe ataki i obrona przed nimi, przy okazji omawiania działań koniecznych do ustrzeżenia się przed określonymi zagrożeniami i atakami cybernetycznymi. W związku z tym poniżej przedstawimy jedynie te zasady, które nie zostały ujęte lub zostały tylko pobocznie wspomniane w powyższym rozdziale.

Ochrona prywatności. Zasada czystego biurka.

Zasadę tę, przywoływaną przede wszystkim w zakresie ochrony danych osobowych i zgodności z RODO, należy odnosić również do cyberbezpieczeństwa. W tym kontekście oznacza ona nie udostępnianie i nie pozostawianie „na widoku" istotnych, poufnych informacji takich jak np. dane logowania. A więc jeśli wpisujesz dane uwierzytelniające, rób to tak, aby osoby postronne tego nie widziały. Wylogowuj się z zasobu (serwisu, aplikacji, e-sklepu), z którego przestajesz aktualnie korzystać (strony powinny wylogować Cię automatycznie po pewnym czasie braku aktywności, ale nie wszystkie to robią). Blokuj dostęp do komputera, kiedy od niego odchodzisz. Ustaw automatyczne uruchamianie zabezpieczonego hasłem wygaszacza ekranu po określonym, krótkim czasie braku aktywności. Sparuj w ustawieniach konta swój smartfon z komputerem, z opcją automatycznej blokady tego ostatniego, kiedy od niego od-

chodzisz (mówiąc precyzyjniej – kiedy Twój smartfon oddali się od niego). Przesłaniaj kamerę komputera, kiedy z niej nie korzystasz, bo jeśli cyberprzestępcy przejmą dostęp do niej, będą widzieć wszystko co robisz, w tym jakie hasła wprowadzasz.

Nie udostępniaj swoich danych (osobowych, finansowych itp.) w sieci. Pamiętaj, że każda informacja wprowadzona do Internetu tam pozostanie i nie łudź się, że zdołasz ją skutecznie usunąć. Każdorazowo zastanów się nad tym, co umieszczasz w Internecie i kieruj się zasadą: „Im mniej, tym lepiej!" Pamiętaj, że wiele rzeczy może zawierać informacje, którymi niekoniecznie chciałbyś się dzielić. Np. udostępniając na portalu społecznościowym zdjęcie swojego psiaka bawiącego się w ogrodzie, udostępniasz tym samym (w metadanych) współrzędne geograficzne, a więc dokładną lokalizację, swojego domu. Im więcej danych o sobie przesyłasz do Internetu, tym więcej informacji mogą o Tobie (o Twoich nawykach, zwyczajach, zainteresowaniach itp.) zebrać cyberprzestępcy. Kasuj regularnie niepotrzebne pliki .tmp i historię przeglądarek internetowych.



Pamiętaj, że gdy odwiedzasz strony internetowe, moduły do śledzenia online i sama strona mogą Cię zidentyfikować np. za pomocą ciasteczek. Ciasteczka, czyli cookies są standardowo wykorzystywane m.in. w celu efektywniejszego świadczenia usług, oferowania spersonalizowanych reklam, czy opracowywania statystyk. Zwykłe ciasteczka zwiększają komfort korzystania z sieci. Używamy ich np. napełniając koszyk w e-sklepie, czy logując się do strony bez konieczności powtórnego wpisywania hasła. Mogą one jednak służyć również do zbierania informacji o naszej wcześniejszej aktywności w sieci. Są również tzw. evercookies – czyli „wieczne ciasteczka" oparte na JavaScript. Są one zapisywane jednocześnie w kilku miejscach w systemie i oferują wiele możliwości nieuprawnionego dostępu do informacji, przy czym im więcej metod zagnieżdżenia takich obiektów zostanie zastosowanych, tym trudniej się ich pozbyć. Witryny internetowe wykorzystują też specjalistyczne programy (np. Panopticlik) lub techniki (np. Canvas Fingerprinting) śledzące informacje, które są przesyłane z naszej przeglądarki do sieci i tworzące w oparciu o te dane jednoznaczny identyfikator naszego systemu (fingerprint, czyli „cyfrowy odcisk palca").

Przed instalacją nowych aplikacji, czy utworzeniem konta w nowym serwisie zapoznaj się z się z treścią regulaminu określającego na jakich zasadach można z tych zasobów korzystać oraz czego ich właściciele oczekują od nas w zamian, a zwłaszcza kto ma prawo do zapisanych danych: zdjęć, plików, maili, czatów. Pamiętaj, że nie wszystkie regulaminy zawierają pełne informacje o tym, co dzieje się z naszymi danymi. Niefrasobliwość w tym względzie może doprowadzić nawet do kradzieży tożsamości. Np. dostępna w Google App i Apple Store – FaceApp, reklamowana jako jedna z najlepszych aplikacji mobilnych do edycji zdjęć w oparciu o sztuczną inteligencję i pozwalająca na „postarzenie" wizerunku w bardzo wiarygodny sposób (a więc zobaczenia jak dana osoba będzie najprawdopodobniej wyglądała np. za 30 lat) wymaga jak się okazuje przesłania naszego zdjęcia na serwery zlokalizowane w Petersburgu, a zgodnie z polityką prywatności, którą użytkownik musi zaakceptować, twórcy aplikacji mają dostęp i prawo do tych zdjęć. Aplikacja zbiera też bardzo istotne dane użytkowników: ciasteczka, dane analityczne, logi, identyfikatory urządzeń oraz metadane zdjęć. Pamiętaj, że jeśli korzystasz z tłumaczy lub słowników online (Google Translator, DeepL, Diki itp.), albo asystentów głosowych (Apple Siri, Amazon Alexa, Microsoft Cortana, Google Assistant), to wprowadzane przez Ciebie informacje tekstowe lub głosowe są przesyłane na serwery producentów tych aplikacji.

Usuwaj newralgiczne dane z pamięci urządzeń (dysku twardego, pamięci flash, karty SD) przy pomocy specjalistycznych programów tzw. wiperów (np. Eraser, Hardwipe, czy File Shredder). Pamiętaj, że usuwając plik z dysku twardego (również Kosza) standardową komendą lub formatując dysk, wcale fizycznie nie usuwasz danych, a jedynie odbierasz systemowi operacyjnemu informacje o ich położeniu na dysku (ścieżce dostępu). Każdy taki plik można stosunkowo łatwo odzyskać. Firma Kroll Ontrack w ramach eksperymentu zakupiła za pośrednictwem różnych serwisów aukcyjnych 64 używane dyski twarde. W wypadku połowy z nich udało się bez większych problemów odzyskać wszystkie znajdujące się na nich, a pozornie skasowane dane, takie jak: e-maile, filmy, muzykę, zdjęcia, w tym pornografię, imiona, nazwiska, prywatne adresy, numery telefonów, dane kart kredytowych, loginy, hasła, deklaracje podatkowe, plany inwestycyjne, faktury, umowy, a nawet wyniki badań medycznych.

Hasła.

Używaj odpowiednio silnych (długich, złożonych) haseł. Pamiętaj, że im dłuższe hasło, tym trudniejsze będzie do złamania. Zgodnie z zaleceniem FBI (https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday-building-a-digital-defense-with-passwords) zamiast używać krótkiego złożonego hasła, które jest trudne do zapamiętania rozważ raczej używanie jako hasła dłuższego „zdania" (passphrase). Wystarczy tylko połączyć kilka słów w jedno duże hasło, które powinno mieć ponad 12 znaków. Tak więc np. hasło „ZWoloszynamipoczciweyrozmowyniemasz,boplemiezłodzieyskieiplugawe,tedywszelkagadkezaczynaydawszywprzodywpysk" (cytat z dzieła „Tarcza Żołnierza y Rycerza Ziemie Koronney, Instrukcya, iako z różne nacye gadać", Zamość, 1669) będzie znaczne trudniejsze do złamania niż „Z@m0sc^t". Wiele serwisów wymaga użycia w haśle małych i dużych liter, cyfr oraz znaków specjalnych, ale minimalna wymagana długość hasła to często tylko 8 znaków, a to zdecydowanie za mało. Chroń swoje hasła i nigdy nikomu ich nie udostępniaj. Nie używaj w hasłach powszechnie znanych określeń, które łatwo z Tobą skojarzyć (data urodzenia, imię partnera, dziecka, czy ulubionego zwierzęcia, PESEL, itp.). Nie używaj też sekwencji alfabetycznych lub rzędu sąsiadujących klawiszy. Jeśli Twoje hasło jest dostatecznie silne i nie zostało skompromitowane – nie zmieniaj go! Niektóre serwisy wymagają zmiany hasła (niekiedy bardzo często), ale tę praktykę obecnie zdecydowanie się odrzuca (tak np. Microsoft – „Security baseline for Windows 10 v1903 and Windows Server v1903", OWASP – „Application Security Verification Standard 4.0", czy NIST – „Digital Identity Guidelines, 800-63-B). Wymóg częstych zmian powoduje, że użytkownicy tworzą słabe hasła lub po prostu nieznacznie modyfikują swoje obecne. Istnieje wiele badań pokazujących, że użytkownicy, którzy są zobowiązani do zmiany swoich haseł, często wybierają słabsze hasła, a następnie zmieniają je w przewidywalny sposób np. poprzez zwiększanie liczby, zmiany litery na podobnie wyglądający symbol, usuwanie znaku specjalnego, albo przełączanie kolejności cyfr lub znaków specjalnych. Natomiast zmień hasło natychmiast jeśli dowiesz się o kompromitacji serwisu, w którym tego hasła używałeś. Według danych Atlas VPN w 2021 r. wyciekły na świecie dane 5,9 mld kont! A są to jedynie kradzieże, które wykryto. Na stronie https://haveibeenpwned.com/ możesz sprawdzić, czy Twój email pojawił się w którymś z wycieków danych. Jeśli tak było, to powinieneś natychmiast zmienić hasła w tych serwisach, z których wyciek nastąpił. Nigdy nie używaj tego samego hasła do różnych zasobów. Jeśli tak zrobisz, to kompromitacja jednego z nich spowoduje zagrożenie wszystkich serwisów,

w których takiego hasła użyłeś. Stosuj wszędzie tam gdzie to możliwe uwierzytelnienie wieloskładnikowe (MFA). Zastosuj jako element zabezpieczający klucz sprzętowy U2F, bo tylko on skutecznie uchroni Cię przed przejęciem konta. Nie pokładaj nadmiernej wiary w zabezpieczeniu biometrycznym, zwłaszcza odciskiem palca. Jak pokazują badania, w wielu przypadkach implementacji takiej technologii zabezpieczenie tego typu jest stosunkowo łatwo złamać. Jedno dobre zdjęcie dłoni wystarczy, by przechwycić wzór odcisku palca i przetworzyć go na klucz biometryczny, który posłuży do złamania zabezpieczeń. Znacznie pewniejszym zabezpieczeniem jest obraz tęczówki, czy układu naczyń krwionośnych w dłoni. Trzeba też pamiętać, że cechy biometrycznej, która została skompromitowana (wyciekła) nie można, w przeciwieństwie do hasła, zmienić. Używaj menadżera haseł (np. 1Password, Dashlane, LastPass, Keepass, Keeper, Bitwarden i wiele innych) zabezpieczonego odpowiednio silnym hasłem. Rozwiązanie takie pozwala na przechowywanie w bezpieczny sposób zaszyfrowanych haseł do naszych zasobów. W związku z tym dostęp do wszystkich używanych haseł wymaga zapamiętania jedynie jednego hasła – do ich menadżera. Co więcej, przechowywanie tych haseł w chmurze powoduje, że hasło wprowadzone do menadżera na jednym urządzeniu np. smartfonie będzie natychmiast dostępne na dowolnym innym naszym urządzeniu np. laptopie. Menadżer daje również możliwość automatycznego generowania bardzo silnych, złożonych, pseudolosowych haseł, a także automatycznego podstawiania haseł przy logowaniu do witryny internetowej lub aplikacji. Ta ostatnia funkcja zapewnia dodatkowy poziom ochrony, bowiem menadżera nie da się oszukać przez podstawienie zmodyfikowanego adresu strony internetowej jak np. zastąpienie litery cyfrą (l na 1, O na 0), jednej litery innymi (m na rn, w na vv, d na cl), czy literą z innego alfabetu (a na ŕ, czy s na ş).

Nie pracuj na koncie z uprawnieniami administratora, jeśli nie masz potrzeby wykonywania działań zastrzeżonych dla takich uprawnień.

Internet Rzeczy – IoT.

Z raportu Juniper Research wynika, że liczba urządzeń Internetu Rzeczy osiągnęła na świecie w 2021 r. 46 miliardów. Według Gartnera do 2025 roku będzie ich 75 miliardów. Urządzenia te bardzo często zawierają niestety szereg słabych punktów stanowiących idealny punkt dostępowy dla potencjalnego aktora zagrożeń. Należą do nich m.in.: działanie na starych systemach operacyjnych, dostęp bez uwierzytelnienia, słabe uwierzytelnianie, ustawienia domyślne, brak szyfrowania lub przestarzałe metody szyfrowania, występowanie tzw. backdoor'ów, czyli specjalnie pozostawionych przez programistów luk w zabezpieczeniach systemu, brak uaktualnień systemu i łat bezpieczeństwa, zwłaszcza do starszych urządzeń. Jak wynika z opublikowanego w sierpniu 2021 r. raportu firmy Mandiant, co najmniej 83 miliony urządzeń Internetu rzeczy na całym świecie może być zagrożonych włamaniem, potencjalnie umożliwiając cyberprzestępcom podsłuchiwanie prywatnych rozmów i oglądanie strumieni wideo na żywo z elektronicznych niań i inteligentnych kamer. W 2018 r. hakerzy włamali się do jednego z amerykańskich kasyn poprzez grzałkę w akwarium, kradnąc przy tym ponad 3 mln dol. W 2019 r. badacze bezpieczeństwa z firmy SEC Consult podali, że życie i zachowania seksualne co najmniej 50 000 osób zostały publicznie odarte z tajemnicy w wyniku udostępnienia w Internecie danych (w tym zdjęć) pozyskanych przez seks-zabawki „Vibratissimo Panty Buster". Innym przykładem nietypowego ataku wymierzonego w sprzęt IoT było zablokowanie ogrzewania w miejscowości

Lappeenranta w Finlandii, gdzie mieszkańcy dwóch budynków przez blisko tydzień marzli w swoich domach na skutek przeprowadzonego za pośrednictwem termostatów ataku DDoS na systemy kontroli środowiska. Atak ów, po ponownym uruchomieniu systemu sterowania, doprowadził do zapętlania się funkcji sterowania centralnym ogrzewaniem oraz instalacją ciepłej wody. NordVPN podaje przykład pewnej rodziny z USA, która korzystała z bezprzewodowego systemu kamer, aby obserwować zachowania dziecka. Niestety, do takiej infrastruktury dostał się haker, który znając zwyczaje domowników zażądał okupu pod groźbą porwania potomka. W sierpniu 2021 r. badacze bezpieczeństwa z firmy IoT Inspector znaleźli błąd w czipie Realtek RTL819xD, który umożliwiał hakerom dostęp do hosta i jego systemu operacyjnego. Podatnych okazało się tysiące produktów (routerów, kamer, bram sterowanych elektronicznie, oświetlenia inteligentnego czy zabawek łączących się z siecią) 65 firm w tym Huawei, Logitec, AsusTEC, D-Link, ZTE, TCL, LG, Hama i oczywiście Realtek.

Jak wobec tego ustrzec się przed zagrożeniem ze strony urządzeń IoT? Należy w tym celu:

- Wprowadzić segmentację sieci, czyli odseparować sieć obsługującą IoT od sieci Wi-Fi, w ramach której funkcjonują nasze smartfony czy komputery.
- Nadać sieci dla IoT mylącą nazwę, a więc niech to nie będzie np. SmartDom.
- Regularnie aktualizować system operacyjny urządzeń IoT i niezwłocznie wgrywać wszystkie poprawki bezpieczeństwa udostępniane przez producenta.
- Pozmieniać nazwy urządzeń, żeby utrudnić ewentualnemu hakerowi identyfikację urządzeń w naszej sieci.
- Ustalić silne hasło dostępu, odmienne od (co najmniej równie silnego) hasła administratora.
- Wyłączyć możliwość dostępu (jeśli nie jest on konieczny) do naszych urządzeń IoT spoza sieci, w której się one znajdują.
- Włączyć, jeśli to tylko możliwe, szyfrowanie danych.
- Wyłączyć funkcje, których nie używamy.

IX. SCAM, CZYLI JAK NIE DAĆ SIĘ OSZUKAĆ I JAK BEZPIECZNIE ROBIĆ ZAKUPY W SIECI

[P. Brogowski]

Scam jest techniką socjologiczną polegającą na wzbudzeniu zaufania u drugiej osoby, dzięki czemu możliwe jest łatwe sterowanie jej wyborami i zmuszenie jej do powierzenia np. swoich pieniędzy czy danych osobowych. Oszust w korespondencji obiecuje coś, na co liczy druga strona, np. dobrą cenę za sprzedawany przedmiot. Prowadzenie w taki sposób komunikacji sprawia, że wiele osób podejmuje działania, do których nakłania je nieznana osoba.

Scammerzy tworzą strony internetowe wyłącznie w celu wyłudzania pieniędzy czy danych osobowych użytkowników, podszywając się pod e-sklepy, firmy kurierskie, urzędy czy serwisy z ogłoszeniami sprzedaży. Scam jest dość mocno połączony z phishingiem, ponieważ oba zjawiska dotyczą wyłudzeń danych osobowych i innych wrażliwych informacji za pomocą Internetu. Bardzo często oszuści posługują się portalami społecznościowymi – tam informacje bardzo szybko się rozchodzą, zyskują duże zainteresowanie i zasięg, oraz komunikatorami, zwłaszcza WhatsApp i Messenger. Często schemat oszustwa polega na tym, że oszust kontaktuje się telefonicznie z osobą wystawiającą np. na OLX jakiś przedmiot i po kilku pytaniach o aktualność oferty i stan sprzedawanego przedmiotu przesyła informację, że zrobił przelew z załączonym linkiem. Ofiara przez kliknięcie w link ma jedynie potwierdzić przyjęcie płatności. Kliknięcie takie otwiera stronę bardzo często bliźniaczo podobną do tej, na której ogłoszenie zostało dodane. Cyberprzestępcy zachęcają tam, by wprowadzić dane swojej karty kredytowej lub swojego konta. Po tej czynności sprzedający ma otrzymać pieniądze za przedmiot z ogłoszenia. Często też oszuści zapewniają, że po otrzymaniu środków na konto przyjedzie do sprzedawcy kurier odebrać przedmiot. W rzeczywistości przestępcy wykorzystują podane dane do wyprowadzenia wszystkich środków z karty lub konta ofiary. Typowe przykłady scamu to oferty produktów w zaskakująco korzystnych cenach, niespodziewane nagrody bez udziału w konkursach, prośby o wsparcie dla biednych rodzin, które nie mają za co żyć i proszą o przelew za pomocą karty kredytowej, historie o spadku, który możesz otrzymać, jeśli wpłacisz konkretną kwotę prowizyjną, czy też opłatę za przelew (tzw. oszustwo nigeryjskie, „Nigerian scam"), czy wreszcie przypadki rzekomych żołnierzy amerykańskich na misjach zagranicznych szukających miłości i możliwości przekazania ukochanej osobie znacznych środków. W tym ostatnim przypadku nieświadoma ofiara spotyka „idealną połówkę", która jest wrażliwa, czuła, romantyczna i ma świetną pracę. Jak się później okazuje, oszust, wymyślając najróżniejsze kłamstwa, pozyskuje, z reguły stopniowo, kolejne pieniądze od zakochanej osoby.

12:39

WITAJCIE POTRZEBUJĘ TWOJEJ życzliwości Odebrane

Marika Heikkilä 11:43
do UDW: mnie

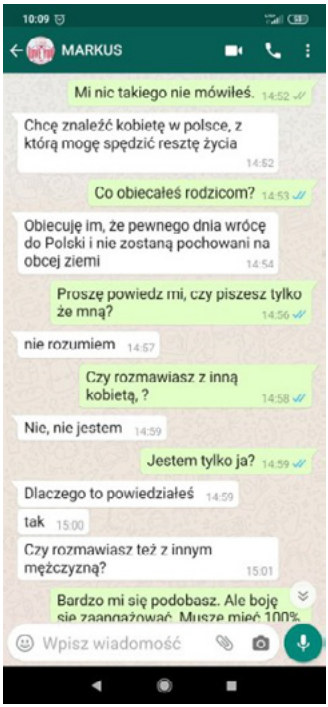
WITAJCIE POTRZEBUJĘ TWOJEJ życzliwości

Nazywam się Marika Heikkilä Grieger, proszę, mam fundusz w wysokości 1,5 miliona euro, który chcę przekazać przez was na sierociniec, wdowę i dom dobroczynny. Piszę ze szpitala, w którym zdiagnozowano u mnie raka od bardzo dawna i boję się, że mogę stracić ten fundusz na rzecz rządu tutaj, jeśli umrę, bo chcę, żeby fundusz był dla biednych w społeczeństwie. Chcę, żebyś wykorzystał 30 procent funduszu na siebie, a pozostałe 70 procent na siebie i swoją rodzinę

Będę wdzięczny za twoją uczciwość i odwagę w obsłudze tego funduszu, aby pomóc sierotom i domu charytatywnym. Jak tylko otrzymam twoją wiadomość dotyczącą twojego zainteresowania tymi funduszami, aby pomóc domu charytatywnym i mniej przywilejów, podam ci więcej szczegółów na temat tego funduszu. co dalej muszę zrobić.

Pozdrowienia,
Pani Marika Heikkilä Grieger

Odpowiedz | Odpowiedz wszystkim | Przekaż dalej



10:09

MARKUS

Mi nic takiego nie mówiłeś. 14:52

Chcę znaleźć kobietę w polsce, z którą mogę spędzić resztę życia 14:52

Co obiecałeś rodzicom? 14:53

Obiecuję im, że pewnego dnia wrócę do Polski i nie zostaną pochowani na obcej ziemi 14:54

Proszę powiedz mi, czy piszesz tylko że mną? 14:56

nie rozumiem 14:57

Czy rozmawiasz z inną kobietą, ? 14:58

Nie, nie jestem 14:59

Jestem tylko ja? 14:59

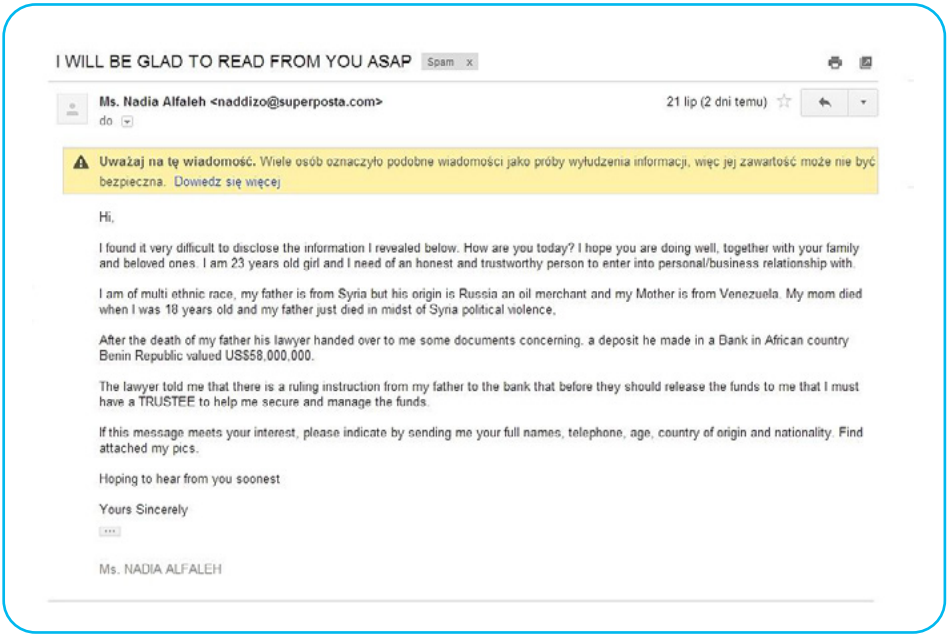
Dlaczego to powiedziałeś 14:59

tak 15:00

Czy rozmawiasz też z innym mężczyzną? 15:01

Bardzo mi się podobasz. Ale boję się zaangażować. Muszę mieć 100%

Wpisz wiadomość



I WILL BE GLAD TO READ FROM YOU ASAP Spam x

Ms. Nadia Alfaleh <naddizo@superposta.com>
do

21 lip (2 dni temu)

Uważaj na tę wiadomość. Wiele osób oznaczyło podobne wiadomości jako próby wyłudzenia informacji, więc jej zawartość może nie być bezpieczna. Dowiedz się więcej

Hi,

I found it very difficult to disclose the information I revealed below. How are you today? I hope you are doing well, together with your family and beloved ones. I am 23 years old girl and I need of an honest and trustworthy person to enter into personal/business relationship with.

I am of multi ethnic race, my father is from Syria but his origin is Russia an oil merchant and my Mother is from Venezuela. My mom died when I was 18 years old and my father just died in midst of Syria political violence,

After the death of my father his lawyer handed over to me some documents concerning, a deposit he made in a Bank in African country Benin Republic valued US$58,000,000.

The lawyer told me that there is a ruling instruction from my father to the bank that before they should release the funds to me that I must have a TRUSTEE to help me secure and manage the funds.

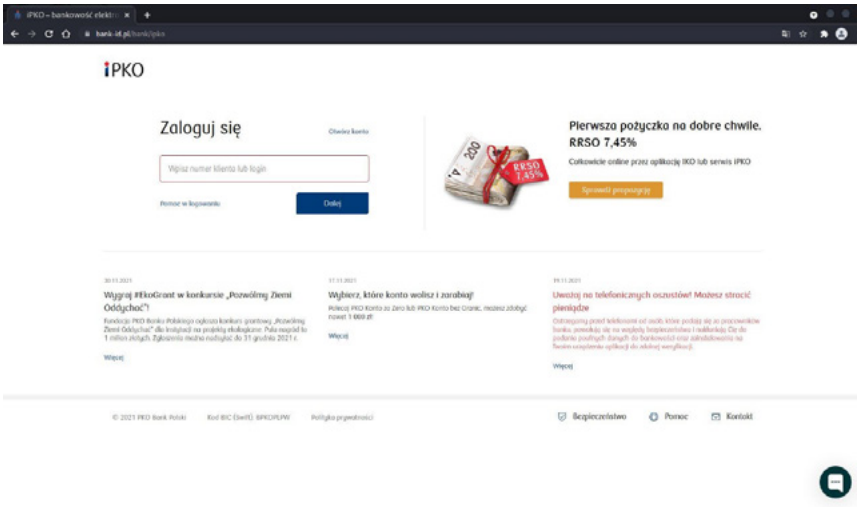
If this message meets your interest, please indicate by sending me your full names, telephone, age, country of origin and nationality. Find attached my pics.

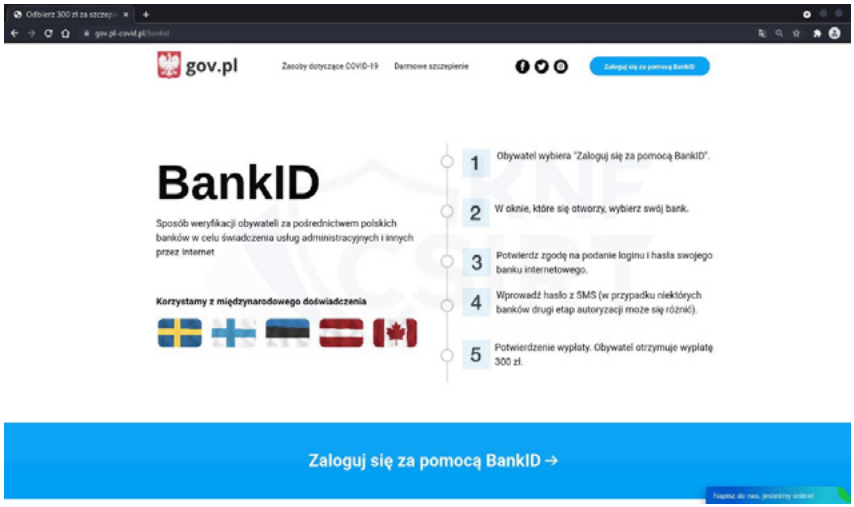
Hoping to hear from you soonest

Yours Sincerely

Ms. NADIA ALFALEH

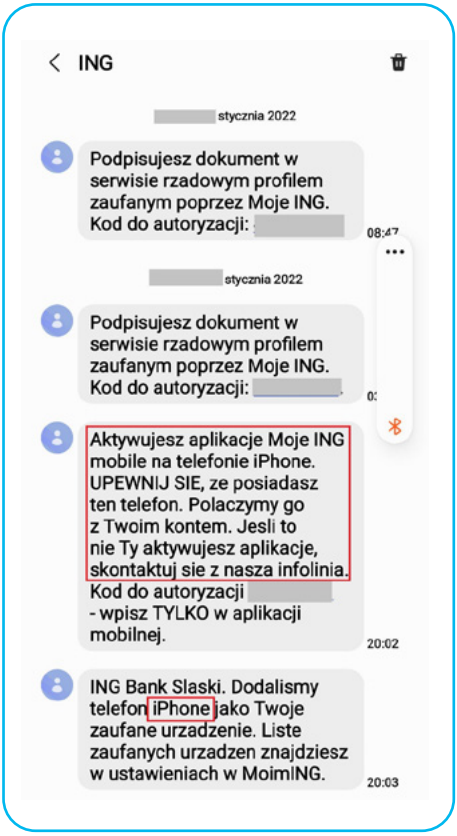
Nie wierz zatem, że to właśnie z Tobą pracownik banku w Burkina Faso postanowił się podzielić zawartością konta jakiegoś milionera, który wraz z całą rodziną zginął w katastrofie lotniczej, albo że wysoki rangą oficer US Army właśnie Tobie chce przesłać kilkaset tysięcy dolarów, albo kilkadziesiąt kilo złota, które przypadkiem znalazł pełniąc swoją misję w Iraku, czy Afganistanie. Nie wierz w rzekome superokazje, jak np., że jeśli natychmiast przelejesz pieniądze, albo podasz dane swojej karty kredytowej, to kupisz za 1500 zł iPhone'a, którego rynkowa cena wynosi 4500 zł. Takich okazji po prostu nie ma. To albo oszustwo, albo – w najlepszym razie – pomyłka oferenta. Pamiętaj, że niekiedy oszuści tworzą sklepy internetowe, które przez pewien czas sprzedają towary (zwłaszcza elektronikę oraz markowe ubrania, czy obuwie) w atrakcyjnych, ale realnych cenach, by nagle wystawić w cenie niesłychanie niskiej pożądane produkty, na które natychmiast rzucą się klienci. Klienci, którzy oczywiście nigdy już nie zobaczą ani swoich pieniędzy, ani zamówionych przedmiotów. Często też oszuści wykorzystują nośne tematy, takie jak COVID-19. W styczniu 2022 r. pojawiła się np. fałszywa strona internetowa gov.pl-covid.pl, na której oszuści oferowali rzekomy zwrot 300 zł za szczepienie. Oczywiście po wprowadzeniu na tej stronie wymaganego hasła do banku, trafiało ono bezpośrednio do oszustów, którzy wykorzystywali je do kradzieży środków z konta ofiary.


iPKO
Zaloguj się
Pierwsza pożyczka na dobre chwile.
RRSO 7,45%
Całkowicie online przez aplikację IKO lub serwis iPKO
Wygraj #IkoGrant w konkursie „Pozwólmy Ziemi Oddychać"!
Wybierz, które konto wolisz i zarabiaj!
Uważaj na telefonicznych oszustów! Możesz stracić pieniądze
Bezpieczeństwo
Pomoc
Kontakt


gov.pl
Zasoby dotyczące COVID-19
Darmowe szczepienie
BankID
Sposób weryfikacji obywateli za pośrednictwem polskich banków w celu świadczenia usług administracyjnych i innych przez Internet
Korzystamy z międzynarodowego doświadczenia
1 Obywatel wybiera "Zaloguj się za pomocą BankID".
2 W oknie, które się otworzy, wybierz swój bank.
3 Potwierdz zgodę na podanie loginu i hasła swojego banku internetowego.
4 Wprowadź hasło z SMS (w przypadku niektórych banków drugi etap autoryzacji może się różnić).
5 Potwierdzenie wypłaty. Obywatel otrzymuje wypłatę 300 zł.
Zaloguj się za pomocą BankID →

Jak można było tego uniknąć?

Po pierwsze zawsze zachowuj czujność i nie daj się omamić. Pamiętaj, że scam opiera się na zaufaniu, a Internet nie jest miejscem, które można nazwać w pełni bezpiecznym. Pamiętaj, że osoba, która z Tobą koresponduje przez Internet wcale nie musi być tą, za którą się podaje, nawet jeśli jest bardzo przekonująca. Dlatego uważaj, jakie działania podejmujesz. Nie wierz, że wszystko, co widzisz w Internecie, jest prawdą (najczęściej jest odwrotnie). Instaluj aplikacje mobilne pobrane wyłącznie z wiarygodnych źródeł: Google Play lub App Store. Przed pobraniem takiej aplikacji dokładnie zapoznaj się z jej opisem i opiniami na jej temat, ponieważ niektóre z nich mogą być stworzone przez hakerów. Kiedy spotyka Cię jakaś nadzwyczajna okazja, sprawdź starannie, ile jest w tym prawdy. Nie wierz, że otrzymałeś super nagrodę w konkursie, w którym nie brałeś udziału. Jeżeli zauważysz, że strona, na której jesteś, nie korzysta z zaszyfrowanego połączenia SSL (brak kłódeczki przed adresem) – nie ryzykuj, podając swoje dane osobowe lub numer karty kredytowej. Pamiętaj, że sama kłódeczka też nie gwarantuje, że nie jest to strona podstawiona przez oszustów (patrz rozdział VII.3 Phishing). Nie klikaj w wątpliwe linki. Zawsze sprawdzaj, czy to faktycznie bliski znajomy z Facebooka prosi Cię o pomoc, a może jednak ktoś się pod niego podszywa. Nigdy nie udostępniaj nikomu danych do logowania w bankowości elektronicznej i mobilnej, haseł do konta lub danych karty (poza płatnościami na zaufanych i sprawdzonych stronach). Nie klikaj w linki przesłane od potencjalnego kupującego – ten nigdy nie powinien mieć takiej potrzeby, żeby wysyłać sprzedającemu coś w linku. Często taki link może zawierać nazwę serwisu, gdzie ogłoszenie zostało dodane. To także może uśpić czujność. Pamiętaj, że otrzymany od obcej osoby link może mieć nieznaną zawartość, która bez naszej zgody zainstaluje na komputerze lub smartfonie złośliwe oprogramowanie. Nie autoryzuj przelewów, których sam nie zleciłeś. Kupujący nigdy nie potrzebuje informacji, że przelew został potwierdzony przez sprzedającego. Czytaj uważnie SMS'y z banku lub komunikaty w aplikacji mobilnej, zanim zatwierdzisz daną transakcję; sprawdź, czy zgadza się kwota i numer konta odbiorcy. Jak np. widać na poniższym przykładzie ofiara używa smartfona z Androidem, a ktoś próbuje skonfigurować jej bankową aplikację mobilną na iPhone (na zupełnie innym numerze). Jeśli zatem zobaczysz tego typu komunikat, od razu skontaktuj się ze swoim bankiem. Pamiętaj, że żadne zabezpieczenia, w tym najlepszy bankowy system antyfraudowy nie pomoże, jeśli zaakceptujesz przestępcom aktywację bankowości mobilnej na ich urządzeniu.



Jeżeli decydujesz się na wysyłkę sprzedawanego przedmiotu, wybierz opcję za pobraniem lub wysyłaj towar dopiero, gdy upewnisz się, że środki wpłynęły na Twoje na konto. Nie zgadzaj się na to, aby to kupujący zamówił kuriera. Uważaj, jeśli osoba zainteresowana transakcją nawiązuje z Tobą kontakt poza portalem sprzedażowym, na przykład pisze na WhatsAppie lub wysyła Ci SMS'y. Unikaj takich sytuacji. Jeśli przenosisz transakcję poza portal sprzedażowy, zawsze jest to ryzykowne. Nie akceptuj propozycji, jeśli osoba, której nie znasz, sugeruje Ci zainstalowanie dodatkowej aplikacji, żeby zrealizować transakcję między Wami lub zamówić przesyłkę. Nigdy nie pobieraj i nie instaluj aplikacji, które polecają Ci nieznajomi. Bardzo często takie programy, mające rzekomo np. umożliwić bardzo intratne inwestycje w kryptowaluty, to w rzeczywistości aplikacje do zdalnej kontroli pulpitu, takie jak TeamViewer. Jeśli je zainstalujesz w powyższych okolicznościach, oddasz całkowitą kontrolę nad swoim komputerem w ręce oszustów. Zachowaj szczególną czujność zwłaszcza wtedy, gdy mail od serwisu transakcyjnego oprócz odnośnika do logowania zawiera: groźbę zablokowania lub usunięcia konta, prośbę o potwierdzenie swoich danych, informację o podejrzanych transakcjach na Twoim koncie, zapytanie o niewystawianą przez Ciebie ofertę. Groźby i informacje tego typu mają zaniepokoić odbiorcę i uśpić jego czujność, by nie zwrócił uwagi na to, że loguje się na fałszywej stronie, służącej do wyłudzania danych. Jeśli masz wątpliwości odnośnie autentyczności takiego maila prześlij go do serwisu, z którego rzekomo pochodzi (np. do Allegro mailem na adres: phishing@allegro.pl, do OLX na stronie internetowej – https://pomoc.olx.pl/hc/pl/articles/210631869-Zg%C5%82aszanie-narusze%C5%84, do Amazona na stronie – https://www.amazon.pl/gp/help/customer/display.html?nodeId=201909130). W serwisie OLX możesz też samodzielnie sprawdzić podejrzany link wklejając go na stronie: https://pomoc.olx.pl/hc/pl.

Sprawdzaj wiarygodność sklepu internetowego przed dokonaniem w nim zakupu. Uważnie zapoznaj się z regulaminami i zawartością strony. Poszukaj informacji i opinii na temat firmy na forach, grupach czy stronach internetowych. Sprawdź, czy sklep ma na swojej stronie podany adres, e-mail i numer telefonu oraz czy można się tymi kanałami z nim porozumieć. Pamiętaj, że nawet robiąc zakupy online w dużych i popularnych sklepach, nie zawsze jesteśmy w pełni bezpieczni: oszuści potrafią stworzyć łudząco podobne kopie takich witryn. Jeżeli więc na stronę docelową zostaliśmy przekierowani z innego źródła, warto upewnić się, że znajdujemy się właśnie w tym miejscu, w którym chcieliśmy. Robiąc zakupy internetowe zawsze zastanów się jakie dane wprowadzasz na stronie e-sklepu. Płać za zakupione towary korzystając z pośrednictwa sprawdzonych operatorów płatniczych takich jak PayU, czy PayPal. Płatność dokonywana jest wówczas na stronie tej właśnie firmy, a sprzedawca nie otrzymuje żadnych Twoich danych uwierzytelniających płatność (numeru karty, jej terminu ważności, kodu CVV). Warto też skorzystać z mobilnych aplikacji płatniczych, takich jak Apple Pay i Google Pay, dzięki którym również nie podajesz sprzedawcy swoich danych związanych z płatnością. Ciekawą alternatywą jest płatność wirtualnymi kartami oferowanymi przez niektóre banki i organizacje (np. Revolut). W ciągu kilku sekund możesz wygenerować taką kartę i korzystać z niej podczas zakupów online tak samo jak z fizycznie istniejącej karty. Potem wystarczy ją dezaktywować, aby nie obawiać się o bezpieczeństwo swoich środków po dokonaniu zakupów w tanim sklepie internetowym, którego wiarygodność trudno było Ci, mimo wszystkich starań, ocenić. Jeśli podejrzewasz, że ktoś próbuje dokonać oszustwa, zawiadom Policję.

X. NIGDY NIE WIERZ, ZAWSZE SPRAWDZAJ – ZERO TRUST

[G. Cenkier]

Architektura Zero Trust powstała w celu zapewnienia bezpiecznego zdalnego dostępu do aplikacji dla pracowników, partnerów i kontrahentów, niezależnie od tego, gdzie znajduje się aplikacja: w siedzibie organizacji, w środowiskach chmury prywatnej lub publicznej, a użytkownicy mogli pracować z domu, z pracy, z kawiarni lub z lotniska. Coraz więcej aplikacji migruje do chmury, co powoduje, że rosną wymagania do przepustowości sieci i szybkiego dostępu do informacji. Model Zero Trust zakłada, że każdy użytkownik i każde urządzenie, które ma dostęp do aplikacji, stanowi potencjalne zagrożenie. Konieczna jest weryfikacja tożsamości użytkownika w jednym miejscu z określeniem wymagań pozwalających na udzielenie dostępu do aplikacji. Wymagane jest wieloskładnikowe uwierzytelnianie użytkownika, co oznacza nie tylko podanie nazwy i hasła dostępu, ale też dodatkowego elementu np. smsa otrzymanego na smartfon, biometrii czy klucza Yubikey zapewniającego wieloskładnikową autentykację.

Należy także zweryfikować czy połączenie jest z typowego miejsca pobytu użytkownika, a nie z Wysp Zielonego Przylądka czy z Wietnamu, jeśli klient aplikacji standardowo pracuje z Polski. Takie połączenie może sugerować próbę nieuprawnionego dostępu. Wątpliwości może budzić połączenie realizowane w późnych godzinach nocnych lub w dni wolne od pracy, co nie znajduje uzasadnienia w typowych sytuacjach. Kolejnym elementem jest uwierzytelnianie urządzenia z którego podejmujemy próbę dostępu do aplikacji: czy jest zgodne z obowiązującymi zasadami, bo można zabronić dostępu ze smartfonów, jaki jest stan urządzenia, czyli np. czy urządzenie ma aktualny/dopuszczony przez organizację system operacyjny albo właściwy system antywirusowy i zaktualizowane łatki oraz natywne mechanizmy szyfrowania. Następnym ważnym elementem ZT są zasady autoryzacji dostępu do aplikacji – czy każdy i zawsze ma do niej dostęp, czy może dokonywać zmian w danych lub czy wolno mu je kopiować.

Należy weryfikować uprawnienia i udzielać dostępu do aplikacji na podstawie analiz w czasie rzeczywistym, a wszystkie działania użytkowników na danych powinny być monitorowane i kontrolowane. Użytkownik powinien mieć dostęp tylko do tych aplikacji, których potrzebuje do efektywnego wykonywania swojej pracy i do niczego więcej – dostęp najmniej uprzywilejowany. Optymalnym rozwiązaniem

jest schowanie aplikacji przed dostępem z Internetu za punktem proxy, co eliminuje je jako widoczny cel potencjalnego ataku. Niezbędne logi z urządzeń i aplikacji muszą być agregowane i analizowane za pomocą automatycznego system do zarządzania informacjami i zdarzeniami np. SIEM - Security Information and Event Management. Istotne jest również aby aplikacje, oprogramowanie pośredniczące w dostępie do aplikacji, systemy operacyjne i infrastruktura przeszły oceny podatności na zagrożenia, testy bezpieczeństwa.

Ostatnim elementem architektury zerowego zaufania jest sieć. Ogólnie rzecz biorąc, sieci można podzielić, ze względów funkcjonalnych na dwa rodzaje: sieć wewnętrzną, gdzie są hostowane aplikacje, dane i pozostała infrastruktura lokalna lub chmurowa oraz publiczna sieć Internet używana do łączenia się z siecią organizacji użytkownika. Nie trzeba dodawać, że cała komunikacja między punktem końcowym – użytkownikiem a siecią firmową musi być szyfrowana przy użyciu bezpiecznego protokołu jak TLS/HTTP. Należy pamiętać o tym, aby urządzenia i użytkownicy nie byli traktowani jako zaufani tylko dlatego, że znajdują się w sieci wewnętrznej. Cała komunikacja w sieci wewnętrznej powinna być szyfrowana, dostęp ograniczony na podstawie przyjętych zasad oraz struktura sieci zbudowana w oparciu o mikrosegmentację i ciągle aktywna funkcja wykrywania zagrożeń w czasie rzeczywistym.

Podsumowując model Zero Trust to jedno silne źródło kontroli dostępu, które wymaga:

- Uwierzytelnianie użytkownika
- Uwierzytelnianie maszyny
- Dodatkowy kontekst, taki jak zgodność z zasadami i stan urządzenia
- Zasady autoryzacji dostępu do aplikacji
- Zasady kontroli dostępu w aplikacji
- Mikrosegmentacji sieci

ZASADY KORZYSTANIA Z PUBLIKACJI

- Niniejsza publikacja stanowi zbiór dobrych zasad i nie jest oficjalnym dokumentem rekomendowanym przez jakąkolwiek organizację. Tym samym stosowanie się do zasad w niej wyrażonych jest dobrowolne 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 wersji drukowanej i 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 – **www.issa.org.pl**

ISSA POLSKA

ISSA POLSKA