RODO – jak się przygotować

Szkolenie w zakresie zmian w przepisach dotyczących ochrony danych osobowych

PRZEPISY PRAWA O OCHRONIE D.O.

- Ustawa o Ochronie danych osobowych
- Rozporządzenie MSWiA z dnia 29 kwietnia 2004
- Rozporządzenie MAiC (powołania i odwołanie ABI)
- Rozporządzenie MAiC (rejestru zbiorów danych)
- Rozporządzenie MAiC z dnia 11 maja 2015 (zadania ABI)

- **ROZPORZĄDZENIE PE I RADY (UE) 2016/679** z dnia 27 kwietnia 2016 r. (Start – 25.05.2018)
- NOWA Ustawa o Ochronie danych osobowych (w Sejmie)
- Nowelizacja ponad **130** ustaw (lipiec?)

PRZEPISY PRAWA O OCHRONIE D.O.

NOWA Ustawa o Ochronie danych osobowych:

- Zasady powołania Prezesa Urzędu Ochrony Danych Osobowych
- PUODO będzie nadal przeprowadzać kontrole
- PUODO będzie doradzać
- PUODO będzie kwalifikować Kodeksy postępowania (branżowe standardy ochrony danych osobowych)
- PUODO będzie kwalifikować jednostki certyfikujące
- PUODO będzie nakładać kary administracyjne

RODO (Art.32) Bezpieczeństwo przetwarzania

Naruszenie praw i wolności osób

•szkoda majątkowa, finansowa, znaczna szkoda gospodarcza lub społeczna

•dyskryminacja, kradzież tożsamości, oszustwo dot. tożsamości

•naruszenie dobrego imienia

•naruszenie poufności / tajemnicy zawodowej

•**poczucie utraty kontroli nad swoimi danymi**

•ujawnianie danych wrażliwych: *poch. rasowe, etniczne, poglądy polityczne, wyznanie, światopogląd, przynależność związkowa, dane genetyczne, dotyczące zdrowia, seksualności, wyroków skazujących i naruszeń prawa*

RODO - nowe podejście do ochrony danych

Art 24 Obowiązkiem administratora jest wdrożenie odpowiednich środków technicznych i organizacyjnych adekwatnych do ryzyka naruszenia praw lub wolności osób fizycznych.

Powyższe środki (zabezpieczenia) muszą wynikać z przeprowadzanej cyklicznie oceny ryzyka.

UODO będzie rozliczać Administratorów z zasadności stosowania zabezpieczeń !!!

Domyślna ochrona danych - dane osobowe nie mogą być domyślnie powszechnie dostępnie i muszą być zabezpieczone

RODO - nowe podejście do ochrony danych

- **Obecna ustawa** stawia konkretne minimalne wymagania systemom informatycznym oraz żąda opracowania konkretnych procedur
- **RODO**
  - nie stawia żadnych konkretnych wymagań systemom i nie wymienia żadnych obowiązkowych procedur
  - nakłada na ADO obowiązek **samodzielnej** oceny własnych operacji przetwarzania i dokonania odpowiednich zabezpieczeń
  - nie wymienia żadnych obowiązkowych zabezpieczeń
  - wymaga, by wdrożone przez ADO lub procesora zabezpieczenia były adekwatne do ryzyka i żeby proces prowadzący do wdrożenia takich a nie innych zabezpieczeń był udokumentowany

Definicje

Dane osobowe – wszelkie dane osoby, której **tożsamość można (bez nadmiernego wysiłku) bezpośrednio lub pośrednio, jednoznacznie określić.**

Dane osobowe zwykłe:

- Identyfikujące:
  - imię, nazwisko, adres, telefon, PESEL, nr dokumentu tożsamości itp.
- Pozostałe (wszystko co jest związane z już zidentyfikowaną lub możliwą do zidentyfikowania osobą):
  - stan majątkowy, wykształcenie, kariera zawodowa, preferencje konsumenckie, rodzina, wygląd, historia zakupów, miejsca pobytu itd. itd. itd.

Definicje

Dane osobowe wrażliwe:

- pochodzenie rasowe lub etniczne
- poglądy polityczne, religijne, światopogląd
- przynależność związkowa
- stan zdrowia (fizycznego i psychicznego)
- kod genetyczny
- życie i preferencje seksualne
- dane biometryczne
- dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym

Definicje

Przetwarzanie danych – operacje na danych osobowych, jak: wgląd, zbieranie, tworzenie, modyfikowanie, usuwanie archiwizacja, łączenie, udostępnianie, przesyłanie, itp.

Profilowanie – grupowanie danych osób np. ze względu na majętność, zdrowie, preferencje zakupowe, zainteresowania, lokalizację lub przemieszczanie się (*Clubcard Tesco, reklamy googla, profile bezrobotnych w PUP)*

Pseudonimizacja – zamiana danych osobowych na kod, aby „nikt z zewnątrz” nie mógł przypisać go do konkretnej osoby bez użycia zabezpieczonego „klucza” (*wysyłanie zakodowanych próbek dawców do badań laboratoryjnych)*

Definicje

Organ Nadzorczy = Prezes Urzędu Ochrony Danych Osobowych

Administrator - organ, jednostka organizacyjna, podmiot lub osoba, decydująca o celach i środkach przetwarzania danych osobowych *(osoba, przedsiębiorca, firma, organizacja)*

Legalność przetwarzania

Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

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

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

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

5) jest to niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej

6) 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.

Obowiązek informacyjny (art. 12/13/14)

Klauzule informacyjne (bez względu na podstawę prawną)

•nazwa i adres administratora
•cel przetwarzania
•dobrowolność czy obowiązek podania danych
•podstawa prawna przetwarzania i okres przechowywania
•informacje o prawie do żądania usunięcia, ograniczenia przetwarzania, do przenoszenia danych, cofnięcia zgody
•informacje o prawie wniesienia skargi do GIODO
•informacje o profilowaniu

Administrator nie wykonuje obowiązku informacyjnego, gdy:

• osoba była już kiedyś zapoznana z klauzulą informacyjną
• poinformowanie jest niemożliwe lub utrudni przetwarzanie
• ujawniłby tajemnicę zawodową lub złamał prawo UE

Jak wykonać wobec osób obowiązek informacyjny?

klauzula w umowie, na kwestionariuszu, na internetowym formularzu rejestracyjnym, jako broszura lub ulotka, ew. ustnie

Definicje

Udostępnianie/ujawnianie - przekazanie danych pomiędzy Administratorami

- **jest czynnością przetwarzania**
- **musi odbywać się na jakiejś podstawie prawnej**

Powierzenie – zlecenie przetwarzania D.O. Podmiotowi przetwarzającemu (**w imieniu Administratora**)

- pisemna umowa powierzenia lub inny instrument prawny
- w umowie należy określić: przedmiot, charakter, cel i czas trwania przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą, obowiązek świadczenia przez podmiot przetwarzający pomocy administratorowi w wykonywaniu jego obowiązków, zasady kontroli podmiotu przetwarzającego przez administratora
- w umowie należy zawrzeć obowiązki i prawa administratora
- podpowierzenie wymaga pisemnej zgody Administratora

Pozostałe prawa wynikające z RODO

Prawo do usunięcia danych („prawo do bycia zapomnianym”)

Osoba ma prawo żądać usunięcia danych, jeżeli:

- ustał cel przetwarzania
- odwołała zgodę, zgoda wygasła, wyraziła sprzeciw
- dane osobowe były przetwarzane niezgodnie z prawem
- muszą zostać usunięte z powodów przepisów prawa
- dane zebrano w związku z oferowaniem usług komercyjnych

Prawo do przenoszenia danych

Osoba ma prawo uzyskać swoje dane od administratora w formie sformatowanego dokumentu/pliku i ma prawo nakazać przesłanie lub przesłać te dane innemu administratorowi, jeżeli: przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy lub w sposób zautomatyzowany(przeniesienie danych z banku do banku, od operatora internetu do innego operatora, z urzędu do urzędu)

Pozostałe prawa wynikające z RODO

- **Prawo do prostowania danych**
- **Prawo do dostępu do danych i uzyskania kopii**
- **Prawo do ograniczenia przetwarzania**
  - **zamiast usunięcia**
  - ***„przechowuj ale nic więcej”***

- **Prawo do sprzeciwu**
  - **w niektórych sytuacjach**

Rejestracja czynności w RODO

Rejestr czynności przetwarzania (art. 30)

•obowiązkowy dla podmiotów z ryzykiem naruszenia praw osób

• obowiązkowy dla danych wrażliwych

• zalecany dla każdego

• poufny

Dane w rejestrze:

a) dane administratora / współadministratorów

b) cele przetwarzania

c) opis kategorii osób oraz kategorii danych osobowych

d) kategorie odbiorców ujawnione lub planowane

e) ew. przekazanie danych osobowych do państwa 3-go

f) planowane terminy usunięcia danych

g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

Podmiot przetwarzający także prowadzi rejestr, ale ubższy w infromacje

Incydenty

(z Rozp. UE) **incydent / naruszenie ochrony danych:** przypadkowy lub niezgodny z prawem incydent taki, jak:

•zniszczenie, utrata, modyfikacja danych
(*awaria dysku, nadpisanie plików, kryptowirus*)

•nieuprawnione ujawnienie danych
(*wyrzucenie na śmietnik, wyciek internetowy*)

•nielegalny dostęp do danych osobowych
(*kradzież / sprzedaż danych)*

(z Rozp. UE) **Postępowanie z incydentami**

• incydenty naruszające prawa i wolności osób będą wymagać zgłoszenia do GIODO w ciągu 72 godzin. *(sfałszowanie danych, utrata kontroli nad własnymi danymi osobowymi*)

• treść zgłoszenia: opis incydentu, konsekwencje, rozwiązania

• jeśli skutki incydentu dotykają ofiarę, Administrator musi ją poinformować o incydencie

• obowiązek wewnętrznej **rejestracji incydentów**

Kary

Od 2018 r. UODO będzie nakładać administracyjne kary pieniężne za naruszenia Rozporządzenia UE

Kary do 10 mln. EUR lub do 2 % jego całkowitego rocznego światowego obrotu za naruszenia w zakresie: *rejestrowania czynności przetwarzania, współadministrowania, współpracy z UODO oraz z podmiotem przetwarzającym, upoważniania, wdrożenia zabezpieczeń, zgłaszania naruszeń, oceny skutków, pracy IOD*

Kary do 20 mln. EUR, a w przypadku przedsiębiorstwa - w wysokości do 4 % jego całkowitego rocznego światowego obrotu za naruszenia w zakresie: *legalności przetwarzania, warunków zgód, celowości, adekwatności, czasowości, obowiązku informacyjnego, praw osób, niezgodnego z prawem przetwarzania oraz ochrony przed utratą, zniszczeniem lub uszkodzeniem danych*

Kary do 100.000 PLN dla podmiotów publicznych

Rozporządzenie UE - upoważnienia

Obecnie - informację przetwarzają wyłącznie osoby upoważnione. Administrator danych (lub wskazane przez niego osoby) nadaje i odbiera upoważnienia do przetwarzania danych osobowych oraz prowadzi Ewidencję Osób Upoważnionych.

RODO – każda osoba podporządkowana administratorowi i mająca dostęp do danych osobowych przetwarza te dane wyłącznie według jego instrukcji.

Rozporządzenie UE - upoważnienia

RODO – każda osoba podporządkowana administratorowi i mająca dostęp do danych osobowych przetwarza te dane wyłącznie według jego instrukcji

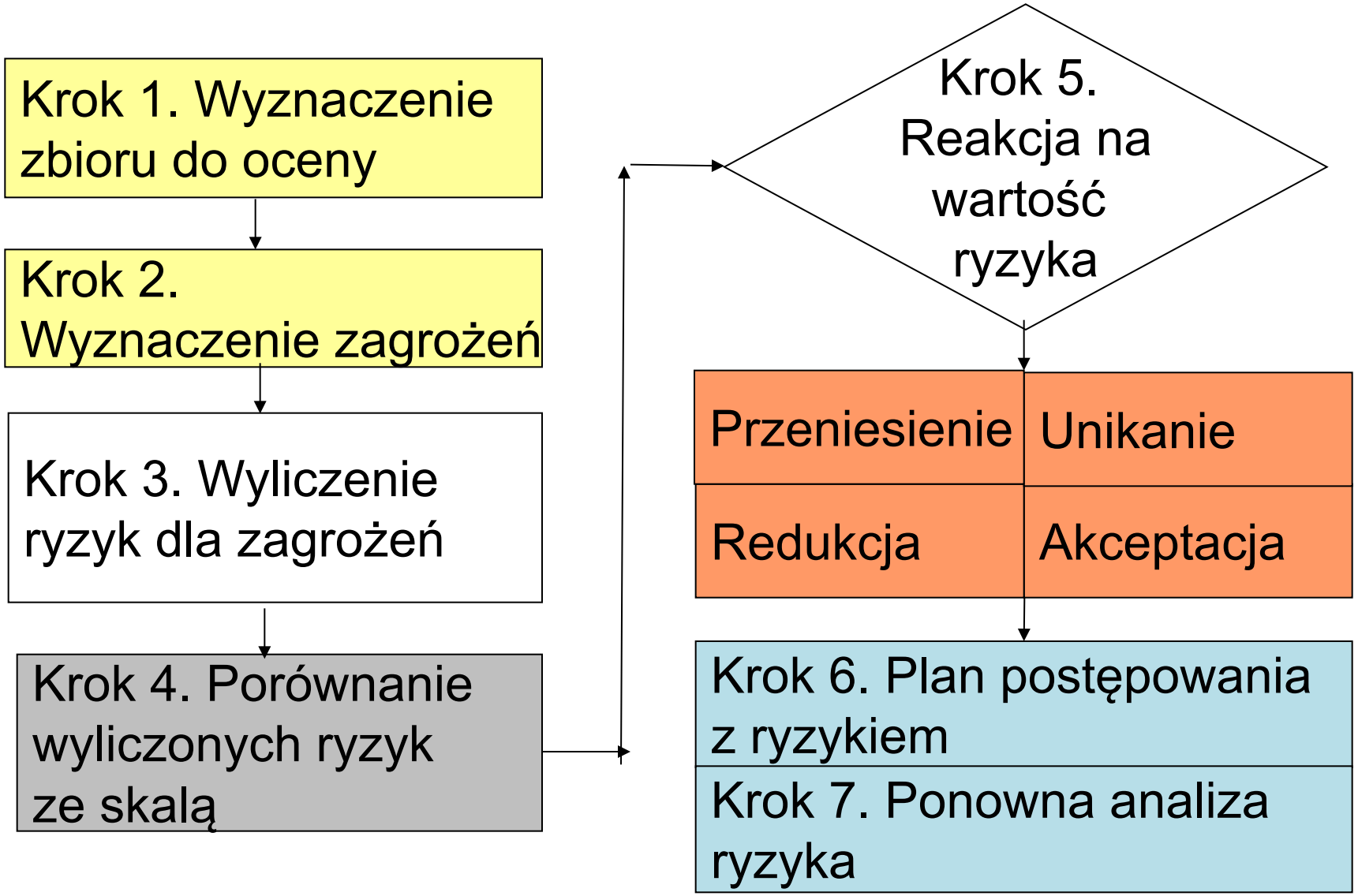
[….] każda osoba działająca z upoważnienia administratora [….] i mająca dostęp do danych osobowych przetwarza je wyłącznie na polecenie administratora [….]

Rozporządzenie UE - upoważnienia

[….] każda osoba działająca **z upoważnienia** administratora [….] i mająca dostęp do danych osobowych przetwarza je wyłącznie **na polecenie** administratora [….]

[….] any person acting **under the authority of** the controller or of the processor, who has access to personal data, shall not process those data except **on instructions** from the controller [….].

Proponowana metoda analizy ryzyka



Procesy zarządzania ryzykiem

- **Centralny element systemu**
- Proces ciągły (cykliczny)
- Potrzebny do dokonania obowiązkowej oceny skutków przetwarzania danych osobowych, ale wcześniej: do upewnienia się, czy taka ocena jest w naszym przypadku obowiązkowa
- Potrzebny do spełnienia wymagania ***zabezpieczenia adekwatne do ryzyka***

Procesy zarządzania ryzykiem

- Mowa nie o każdym o ryzyku, a o tym związanym z naruszeniem praw i wolności osób których dane dotyczą, w szczególności prawa do prywatności.

- Ryzyko rozpatrujemy z punktu widzenia tych osób

- Ryzyko może wystąpić w aspektach: **dostępności**, **integralności i poufności**

Wyliczenie ryzyka dla aktywów

POUFNOŚĆ - Zapewnienie, że informacja jest dostępna wyłącznie dla osób uprawnionych

INTEGRALNOŚĆ - Zapewnienie, że dane nie zostały zmienione, dodane lub usunięte w nieautoryzowany sposób (zaufanie do danych)

DOSTĘPNOŚĆ - Zapewnienie, że upoważnione osoby mogą z niej skorzystać w danym miejscu i czasie.

BEZPIECZEŃSTWO

- **(C)onfidentality - poufność**
- **(I)ntegrity - integralność**
- **(A)vailability - dostępność**

Inwentaryzacja (Klasyfikacja i kontrola aktywów)

Aktywa:

- Procedury, kodeksy, polityki, zasady
- Media (zasilanie, łączność)
- Outsourcing
- Oprogramowanie (własne/zakupione) do przetwarzania danych
- Infrastruktura IT (sieć wraz z elementami, poczta, Internet)
- Infrastruktura (obiekty, biura, transport)
- Pracownicy i współpracownicy

Wyznaczenie zagrożeń i podatności

ZAGROŻENIE - Potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu lub instytucji.

PODATNOŚĆ - Słabość systemu, która może być wykorzystana przez zagrożenie

Zagrożenia środowiskowe (naturalne), losowe

a. Pożar obiektu/pomieszczeń

b. Zalanie wodą dokumentów/serwera/komputerów

c. Braki zasilania

d. Utrata łączności telefonicznej / internetowej

e. Zamieszki gospodarcze / społeczne / polityczne

Zagrożenia losowe, wynikające z przypadku (nie z działań zamierzonych)

a. Awarie serwera / komputerów / oprogramowania systemowego / aplikacji biznesowych

b. Pomyłki informatyków, użytkowników

c. Utrata nośników przenośnych

d. Zagubienie / porzucenie danych poza organizacją

e. Utrata kluczowych pracowników

Zagrożenia wynikające z działań zamierzonych (umyślnych)

a. Włamanie do systemu informatycznego

b. Włamanie do obiektu/pomieszczeń

c. Kradzież danych / komputerów

d. Nieautoryzowany dostęp do systemu

e. Ujawnienie tajemnicy przedsiębiorstwa lub Danych Osobowych osobom nieupoważnionym

f. Szpiegostwo / podsłuchiwanie danych

g. Świadome zniszczenie lub sfałszowanie dokumentów/danych

Wyliczenie ryzyka

RYZYKO –Wskaźnik informujący jednocześnie o:

*- **prawdopodobieństwie** wystąpienia **zagrożenia**, które wykorzysta **podatność** zasobu lub grupy zasobów, powodując utratę poufności, integralności lub dostępności danych osobowych w takim stopniu, że naruszy prawa i wolności osób, których dane są przetwarzane.*

*- **stopniu** (wadze) naruszenia tych praw*

RODO (Art.32) Bezpieczeństwo przetwarzania

Krok 4. Porównanie wyliczonego ryzyka ze skalą

Ryzyko (**R**) wyliczone z formuły R= P*S

1-2, to ryzyko pomijalne i akceptowalne (akceptujemy)
3-6, to ryzyko jest opcjonalne (akceptujemy albo obniżamy)
9, to ryzyko jest nieakceptowalne (musimy obniżyć)

Krok 5. Reakcja na wartość wyliczonego ryzyka

Przeniesienie

Unikanie

Redukcja

Krok 6. Plan postepowanie z ryzykiem
Krok 7. Ponowna analiza ryzyka

Procesy zarządzania ryzykiem

Wybór wariantów postępowania z ryzykiem

Akceptacja –akceptacja ryzyka dla poziomu

Przeniesienie –przerzucenie ryzyka (outsourcing, ubezpieczenie)

Unikanie –eliminacja działań powodujących ryzyko *(np. zakaz wynoszenia komputerów przenośnych poza biuro)*

Redukcja –zastosowanie zabezpieczeń w celu obniżenia ryzyka

Plan postępowania z ryzykiem (przykład)

Analiza ryzyka stwierdza: Zagrożenie (kradzież) może wykorzystać podatność (niechronione przechowywanie danych) z prawdopodobieństwem średnim (2). Skutki (straty) wysokie (3). Ryzyko: 6. Decyzja: redukcja -

Plan (podstępowanie) : Opracować i wdrożyć politykę kluczy do dnia … Osoba odpowiedzialna: ... Dokonać ponownego oszacowania ryzyka do dnia ...

Dokumentacja procesu zarządzania ryzykiem

Procedura zarządzania ryzykiem

Opis czynności podejmowanych w ramach analizy ryzyka (inwentaryzacja aktywów, szacowanie ryzyka, decyzje itp.); przypisanie odpowiedzialności

Wyniki poszczególnych etapów – inwentaryzacja, arkusze analizy ryzyka, podejmowane decyzje wraz z uzasadnieniem

Plany postępowania z ryzykiem

Lista bieżących i zakończonych planów (kto, co, na kiedy, jak mierzyć), dokumentacja przebiegu każdego planu (co zrobiono, co zaplanowano)

GRUPY ZAGROŻEŃ

- **Ataki socjotechniczne**
- **Ataki na infrastrukturę**
- **Złośliwe oprogramowanie**
- **Zagrożenia dla sprzętu**
- **Zagrożenia dla danych**
- **Błędy ludzkie**
- **Zagrożenia dla ciągłości biznesowej**

ATAKI SOCJOTECHNICZNE

- **Inżynieria społeczna:**
  Metody wprowadzania w błąd rozmówcy lub odbiorcy komunikatu w celu wyłudzenia lub nakłonienia do działań

- **Przykłady socjotechnik:**
  Wyłudzenia metodą „na wnuczka”, kradzieże samochodów „na stłuczkę”

- **Przykłady ataków socjotechnicznych:**
  phishing, clickjacking, scam, ataki telefoniczne, podrzucanie nośników

ATAKI SOCJOTECHNICZNE

- **SCAM – oszustwo polegające na wzbudzeniu u kogoś zaufania, a następnie wykorzystanie tego zaufania do wyłudzenia pieniędzy lub innych składników majątku.**

- **Osoba wzbudzająca fałszywe zaufanie zwykle działa na jedną z ludzkich cech charakteru, zarówno negatywnych, jak i pozytywnych, takich jak: pycha i chciwość, ale też empatia i altruizm.**

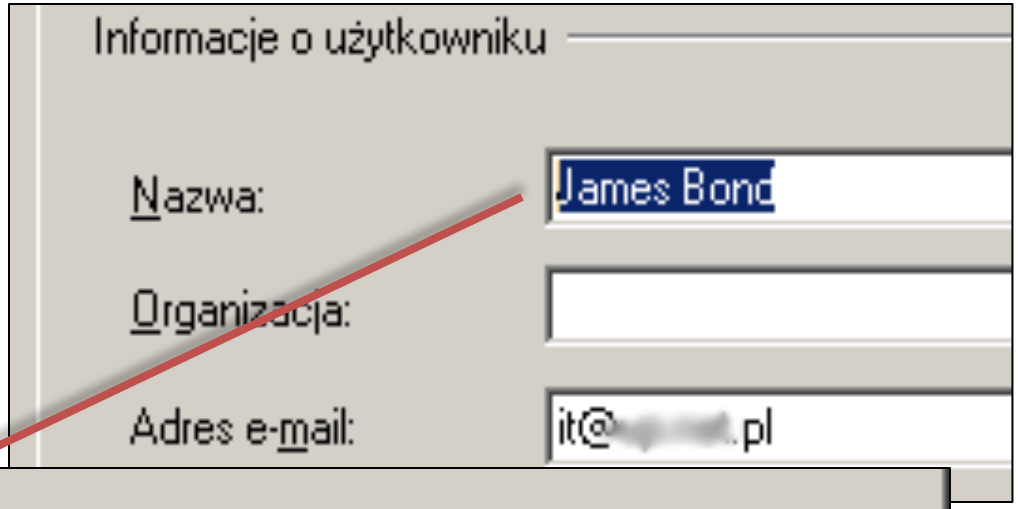

Drogi Użytkowniku!
Ktoś próbował przejąć Twoje konto w serwisie **Facebook**.
Aby temu zapobiec wygenerowaliśmy nowe hasło do Twojego konta.
Udaj się pod Adres http://www.[redacted]tk/
Aby w pełni bezpiecznie odzyskać swoje konto
Postępuj zgodnie z instrukcjami zawartymi na stronie.
Z Poważaniem Facebook Group

PODSZYWANIE SIĘ

- **Maile, w których intruz podaje się za kogoś kogo znamy**
- **Rozmowy telefoniczne, w których intruz podaje się za kogoś, kim nie jest (np. pracownika znanej instytucji)**
- **Sieci społecznościowe, w których intruz zakłada konto wykorzystując czyjeś imię i nazwisko**
- **SMSy, w których intruz fałszuje numer nadawcy**

ATAKI SOCJOTECHNICZNE

PHISHING
Mail z prośbą o zalogowanie. Informacja wyglądająca na wiarygodną, pochodząca od znanej osoby.



Od: [redacted]
Data: Thursday, May 28, 2015 10:23 AM
Temat: logowanie do portalu

Szanowni Państwo,

w związku z przygotowaniami do uruchomienia nowego portalu intranetowego proszę o próbę logowania pod poniższym adresem.
Proszę wybrać opcję "komputer służbowy" i podać własną nazwę użytkownika oraz hasło (te same, które używane są do logowania w systemie windows).

http://intranet [redacted] .pl

ATAKI SOCJOTECHNICZNE

Uruchamianie lustrzanych serwisów będących kopiami prawdziwych portali w celu przechwycenia danych logowania, numerów kart kredytowych itp.

http://www.allegro.home.ro/spol/enter_login.html

CYBERSQUATTING (domainsquatting, typosquatting) – rejestrowanie domen internetowych w celu przekierowania ruchu, podszywania się lub odsprzedaży

PRZYKŁADY:

- **www.rnbank.pl** **zamiast** **www.mbank.pl**
- **WWW.PK0.pl** **zamiast** **www.PKO.pl**
- **wvvw.onet.pl** **zamiast** **www.onet.pl**
- **wwwallegro.pl** **zamiast** **www.allegro.pl**
- **www.allegro.pl** **zamiast** **www.allegro.pl**
  użyto 2 duże „i”

CLICKJACKING – przechwytywanie interakcji użytkownika ze stroną WWW poprzez nałożenie na nią niewidocznej warstwy

NAKŁANIANIE DO WYKONANIA NIEBEZPIECZNYCH CZYNNOŚCI

- Uruchamianie załączników
- Wpisywanie komend
- Instalowanie i uruchamianie nieznanych narzędzi
- Odwiedzanie nieznanych stron
- Działania w sieciach społecznościowych
- Łańcuszki

NIEZNANE NOŚNIKI DANYCH

- **Brak ostrożności użytkowników w postępowaniu ze „znalezionymi” nośnikami danych**
- **Brak mechanizmów weryfikacji i zwiększone zaufanie dla przesyłek otrzymanych pocztą (np. karta z uszkodzonego aparatu firmowego lub pendrive z danymi odzyskanymi z laptopa)**

ATAKI TELEFONICZNE

Przykładowe scenariusze:

- **Intruz przedstawia się jako pracownik dostawcy łącza naprawiający usterkę. W celu weryfikacji skuteczności swoich działań prosi o sprawdzenie łączności z Internetem. Aby upewnić się, że prędkość połączenia jest zgodna z umową prosi o uruchomienie określonej strony internetowej.**
- **Intruz przedstawia się jako inżynier Microsoftu lub programista dostawcy oprogramowania. Podsyła „aktualizację” lub prosi o udostępnienie pulpitu**

ŁAMANIE I POZYSKIWANIE HASEŁ

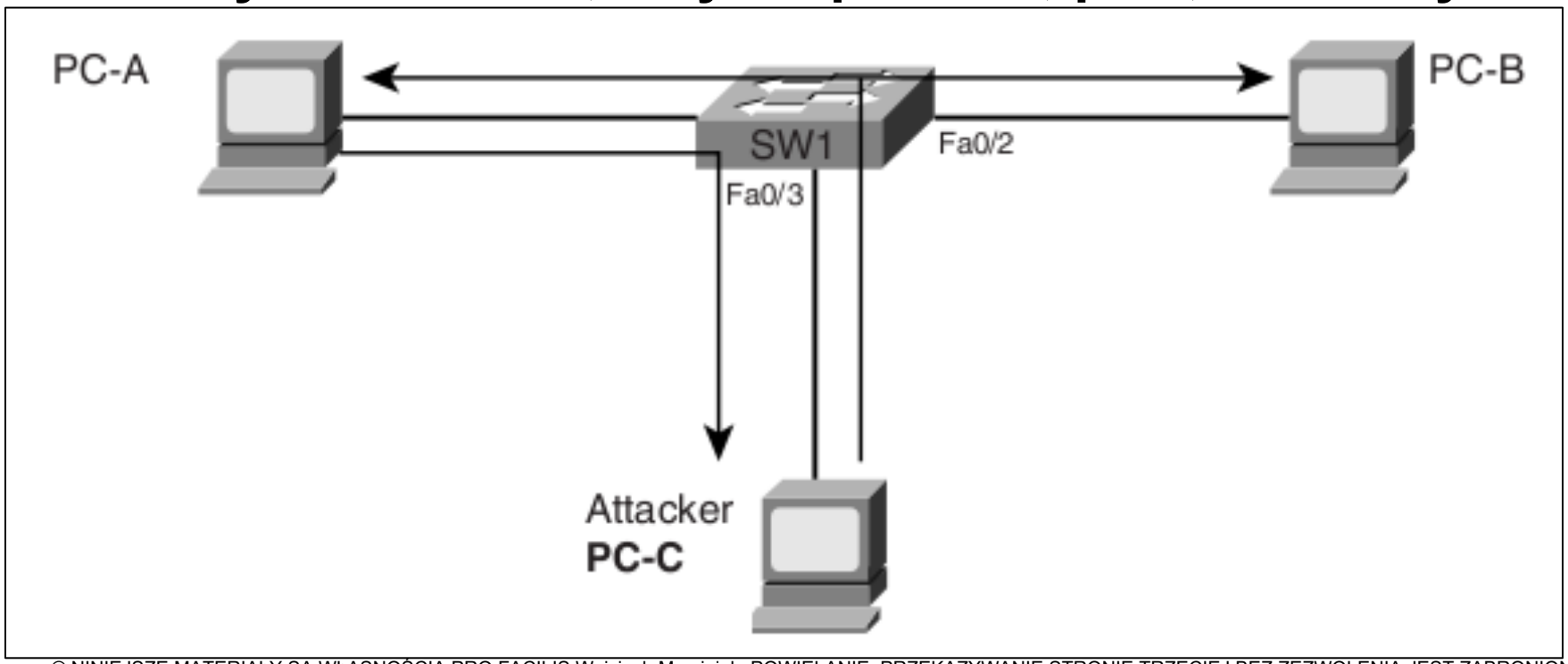
- **Łamanie metodami słownikowymi i siłowymi**
- **Ujawnianie haseł**
- **Nieprawidłowe przechowywanie (karteczki, pliki)**
- **Odgadywanie zbyt słabych, najpopularniejszych haseł**
- **Stosowanie domyślnych haseł producenta**
- **Stosowanie domyślnych, często niewystarczających polityk (np. 8 znaków z 3 grup: „Grażynka1”)**
- **Stosowanie jednego hasła do wielu (często wszystkich) systemów**

ATAKI MAN-IN-THE-MIDDLE

- **Wykonanie „podsłuchu” dla ruchu sieciowego poprzez przejęcie komputera lub dostęp do lokalnej sieci**

- **Wykonanie „podsłuchu” ruchu w otwartej sieci WIFI**

- **Przechwycenie ruchu, w tym np. hasła, pliki, rozmowy tel.**

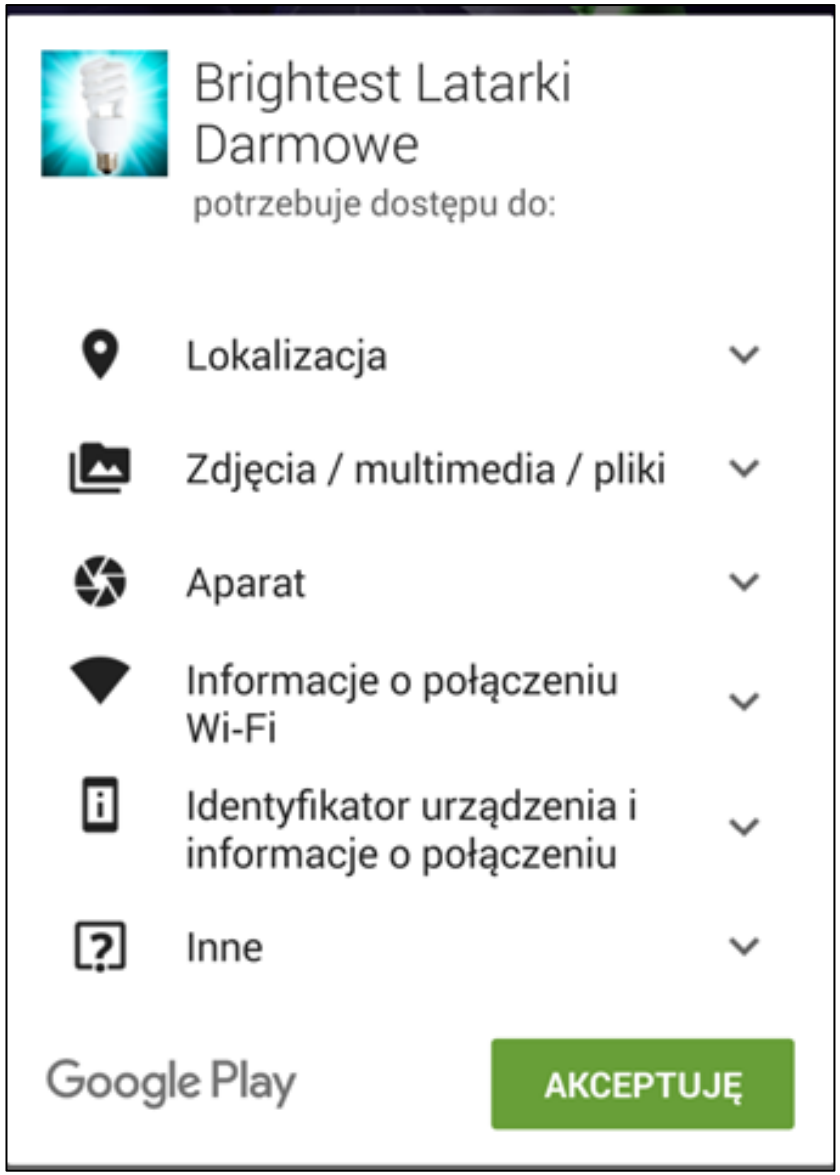


ZŁOŚLIWE OPROGRAMOWANIE

WIRUSY I TROJANY

- **Wirusy – samokopiujące poprzez doklejanie do kodu plików wykonywalnych. Infekcja przez pamięci przenośne lub sieć (robaki sieciowe).**

- **Trojany – złośliwe aplikacje udające oprogramowanie użytkowe. Zawierają ukrytą funkcjonalność, działają na szkodę użytkownika.**



BACKDORY

- **„Tylne furtki” pozostawione w systemie przez intruza w wyniku udanego ataku / włamania lub przez nieostrożne działania użytkownika**
- **Uruchamiane automatycznie razem z systemem umożliwiają intruzowi ponowny dostęp i stałą kontrolę nad systemem**
- **Systemy z aktywnymi backdoorami (tzw. boty) stanowią część botnetów kontrolowanych przez intruza za pomocą jednego serwera przekazującego rozkazy (CC – Command and Control)**

KEYLOGGERY

- **Oprogramowanie lub urządzenia służące do przechwytywania treści wpisywanych z klawiatury**
- **W formie urządzenia muszą być podpięte bezpośrednio do komputera ofiary, wymagają zatem fizycznego dostępu ale są trudne do wykrycia bez inspekcji sprzętu**
- **W formie oprogramowania mogą być uruchamiane zdalnie jako składnik backdoora, trojana lub niezależne aplikacje**
- **Zbierane treści wysyłają za pomocą sieci do intruza lub zapisują w pliku zlokalizowanym lokalnie lub np. na serwerze FTP**

RANSOMEWARE

- **Oprogramowanie blokujące dostęp do plików lub systemu i żądające opłaty w zamian za jego przywrócenie**

- **Rozpowszechniane w formie załączników do poczty lub zainfekowanych witryn www z użyciem socjotechnik**

- **Bardzo szybko rozwijające się i trudne do wykrycia przez typowe oprogramowanie antywirusowe**

EXPLOITY

- **Oprogramowanie służące do przełamywania zabezpieczeń wykorzystujące znane luki w systemach**
- **Może być aktywowane zdalnie przez intruza, nie wymaga interakcji ze strony ofiary**
- **Wynikiem jego działania jest najczęściej uzyskanie dostępu do zdalnego systemu, zwiększenie posiadanych uprawnień lub zdalne wykonanie kodu na systemie / urządzeniu (RCE)**
- **Może być zintegrowane w tzw. exploitpacki, które zawierają całą gamę exploitów i aktywują odpowiednie z nich po rozpoznaniu wersji systemu lub np. przeglądarki www**

ZAGROŻENIA DLA SPRZĘTU

- **Kradzież / zniszczenie** – *kradzież komputerów w organizacji i laptopów poza nią, uszkodzenie sprzętu na skutek przepięcia, czy upadku*

- **Pożar / eksplozja** – *pożar serwerowni, wybuch gazów technicznych*

- **Zalanie** – *np. powódź, pęknięta rura kanalizacyjna, zalanie kawą*
- **Przegrzanie –** *wysoka temperatura w serwerowni*

- **Awaria zasilania –** *skoki napięcia / przerwy w dostawie*

- **Awaria sprzętu –** *awaria dysków, modułów, płyty głównej, sterowników, routerów*

ZAGROŻENIA DLA DANYCH

- **Nieuprawniony dostęp –** *nadane zbyt wysokie uprawnienia użytkownikom lub brak kontroli nad dostępem do plików*
- **Nieuprawniona modyfikacja / usunięcie –** *może mieć również charakter niezamierzony lub być efektem pomyłki*
- **Nieuprawnione kopiowanie danych** – *technicznie trudne do zabezpieczenia*
- **Kradzież danych lub nośników**
- **Utrata danych dostępowych (hasła, klucze, certyfikaty)**
- **Błąd / awaria oprogramowania** – *uszkodzenie bazy danych*

ZAGROŻENIA DLA DANYCH

- **Brak / błędy w wykonywaniu kopii bezpieczeństwa –** *doraźne lub za rzadkie wykonywanie kopii, błędy podczas procesu wykonywania kopii, kopie dostępne bez zabezpieczeń*

- **Udostępnianie danych osobom nieupoważnionym –** *upublicznienie danych w przestrzeni publicznej, dostęp przez internet, przesłanie informacji do osoby nieupoważnionej*

- **Nieprawidłowe / brak procedur niszczenia nośników z danymi –** *wyrzucenie uszkodzonych nośników bez ich zniszczenia, wyrzucenie niezniszczonych pendrive, DVD*

- **Nieprawidłowe / brak procedur napraw w serwisach zewnętrznych** – *naprawa sprzętu z nośnikami w serwisie bez standardu bezpiecznej naprawy i bez umowy bezpieczeństwa*

BŁĘDY LUDZKIE

- **Nieprzestrzeganie procedur i zasad –** *świadome naruszenie procedur, np. niewylogowywanie się z systemu, przekazywanie haseł koledze*
- **Pomyłki –** *błąd ludzki wynikający z pośpiechu lub nieuwagi*
- **Brak świadomości**
- **Brak wiedzy** – *nieprzeszkolony personel*
- **Błędy projektowe / konfiguracyjne –** *błędy programistów*

ZAGROŻENIA DLA CIĄGŁOŚCI DZIAŁANIA

- **Brak aktualnej dokumentacji** – *utrudnia przywracanie środowiska i zarządzanie nim gdy np. odejdzie informatyk*
- **Nieprawidłowe / brak umowy o współpracy** – *brak odpowiedzialności stwarza ryzyko braku staranności*
- **Nieprawidłowe / brak umowy gwarancyjnej lub wsparcia serwisowego –** *umowy wymagają przedłużania*
- **Upadek firmy outsourcingowej lub dostawczej –** *ryzyko braku zastępstw, np. dla hostingodawcy poczty, dla wsparcia do zakupionej aplikacji*
- **Awaria łączy telekomunikacyjnych**

SYSTEMY ANTYWIRUSOWE I ANTYSPAMOWE

- Działają na bazie sygnatur i badania zachowania programu po jego uruchomieniu
- Wciąż niezbędne ale nie stanowią już wystarczającej ochrony
- Występowanie: urządzenia końcowe (komputery, telefony, tablety), serwery, składnik innych urządzeń sieciowych
- Przybierają też bardziej zaawansowaną postać np. systemów typu sandbox

SZYFROWANIE

- **Pozwala zabezpieczyć treści przed nieuprawnionym dostępem nawet w przypadku ich przechwycenia**
- **Szyfrowanie na poziomie ruchu sieciowego (np. HTTPS, poczta)**
- **Szyfrowanie na poziomie dysku twardego BitLocker dla systemu Windows (nie używamy TrueCrypta!)**
- **Szyfrowanie na poziomie plików (np. 7zip)**
- **Szyfrowanie na poziomie całej bazy danych lub wybranych pól w bazie**

HARDENING

- **Tzw. „utwardzanie” systemów polega na podnoszeniu domyślnego poziomu bezpieczeństwa**
- **Zmiana domyślnej konfiguracji**
- **Włączenie szyfrowania**
- **Zmiana domyślnych haseł**
- **Wyłączenie niepotrzebnych funkcji i usług**
- **Bazuje na dobrych praktykach lub standardach**
- **Przykłady: dodatki noscript i adblocker do przeglądarek**

ZARZĄDZANIE AKTUALIZACJAMI

- **Wymuszanie automatycznych aktualizacji**
- **Co najmniej aktualizacje krytyczne i z kategorii security**

SYSTEMY BACKUPU I ARCHIWIZACJI

- **Nie tylko dane i programy: konfiguracje, licencje, hasła**
- **Uwzględniamy ryzyka związane z nośnikami, np. trwałość**

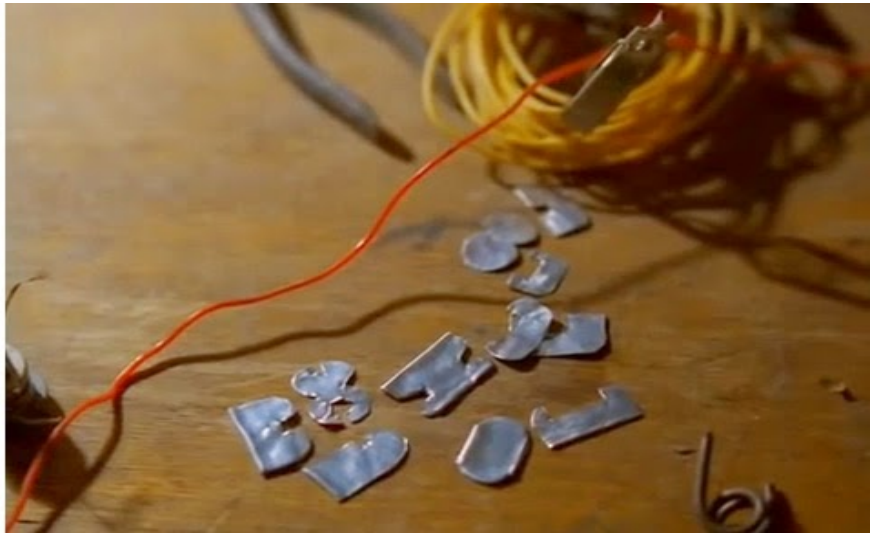
ZASILACZE AWARYJNE (UPS) / AGREGATY PRĄDOTWÓRCZE

- **Moc i czas pracy dostosowane do mocy urządzeń podtrzymywanych i czasu ich wyłączania**
- **Podtrzymanie do 30 min pozwoli na bezpieczny zapis danych i wyłączenie urządzeń**
- **Bypass – możliwość pracy w przypadku awarii UPS-a**
- **UPS – sprawdzamy regularnie czy nie ma spadków mocy – to jest akumulator, przeglądy serwisowe**
- **Agregat – regularny przegląd i odpalanie, wymieniamy i uzupełniamy paliwo**

ŚRODKI OCHRONY - TECHNICZNE

SYSTEMY ALARMOWE / ZABEZPIECZENIA ANTYWŁAMANIOWE

- **Drzwi, zamki, kraty – utrudniają fizyczny dostęp**
- **System alarmowy – informuje o próbie albo przełamaniu zabezpieczenia i dostępie do chronionego miejsca**
- **Te zabezpieczenia działają na zasadzie „i” nie „albo”**



SYSTEMY P. POŻ i AUTOMATYCZNEGO GASZENIA

ŚRODKI OCHRONY - ORGANIZACYJNE

PROCEDURY NISZCZENIA NOŚNIKÓW

- **Wbrew pozorom fizyczne uszkodzenie nośnika jest często niewystarczające**
- **Młotek lub wiertaka uszkadzają nośnik (urządzenie) ale nie 100% zawartych na nim danych**
- **Złamaną płytę CD/DVD da się odczytać**
- **Usuwanie, formatowanie, nadpisywanie również nie są wystarczająco skuteczne**
- **Korzystamy z dedykowanych narzędzi (np. DiskWipe) lub usług firm zewnętrznych**
- **Nie używamy zwykłych niszczarek do danych szczególnie chronionych**

PROCEDURY NAPRAW W SERWISACH ZEWNĘTRZNYCH

- **Komputery wysyłamy bez dysków, urządzenia mobilne bez kart pamięci**
- **Może być konieczne zawarcie specjalnej klauzuli w umowie gwarancyjnej, należy na to zwrócić uwagę przy zakupach**
- **Gdy nie ma takiej możliwości korzystamy z szyfrowania dysku / karty pamięci i wysyłamy sprzęt nie podając hasła**
- **Gdy nie ma innych możliwości, poszukajmy serwisu, który przyjedzie do nas (umowy gwarancyjne on-site)**

ZALECENIA DOTYCZĄCE HASEŁ

- **Stosuj raczej długie niż bardzo skomplikowane hasła**
- **Stosuj znaki z różnych grup (litery, cyfry, znaki specjalne)**
- **1 konto - 1 unikalny login - 1 unikalne hasło**
- **Regularnie zmieniaj hasła i obowiązkowo po incydencie**
- **Nie udostępniaj maila, którym resetujesz hasło**
- **Nie stosuj oczywistych pytań / odpowiedzi w procesie odzyskiwania hasła**
- **Używaj menedżerów haseł**

ZALECENIA DOTYCZĄCE HASEŁ

Przykłady niepoprawnych haseł:

- madzia321, Madzia77, Madzia2015 – hasło zawiera imię
- imiona dzieci, małżonków, numer rejestracyjny samochodu
- data urodzenia, data bitwy pod Grunwaldem
- bazujące na słowach, nazwach, nazwiskach
- Klawiaturowe: qwerty, 1qazxsw2, 123456

Przykłady dobrych haseł

- **S33$#Ddis$@12”?** (zbyt trudne do zapamiętania)
- **PieknyParostatkiemRejsik**
- **Polska-Niemcy4:0**
- **jujotjitdm@)!$** = Ja Uwielbiam Ją Ona Tu Jest I Tanczy Dla Mnie + 2014(z shiftem)

ŚRODKI OCHRONY - ZEWNĘTRZNE

ISP, HOSTING, CLOUD

- **Możliwość korzystania z doświadczenia i infrastruktury dużych i sprawdzonych dostawców.**
- **Nie ufamy jednak bezgranicznie, błędy popełniali nawet najlepsi**
- **Korzystanie z usług zewnętrznych może być efektywniejsze i pozwala na przeniesienie niektórych ryzyk**
- **Usługi specyficzne, wymagające dużego zaangażowania i eksperckiej wiedzy mogą być tańsze w utrzymaniu u dostawców (np. serwery poczty, www, DNS)**

UMOWY SERWISOWE

- **Umowy SLA (Service Level Agreement) powinny zawierać zapisy gwarantujące określony poziom dostępności (np. 99.9% w skali roku)**
- **W przypadku niedotrzymania gwarantowanego poziomu możliwość dochodzenia odszkodowania**
- **Warto wyliczyć jakie odszkodowanie nam przysługuje na podstawie umowy, zwrot 1/90 abonamentu może nie wystarczyć do pokrycia strat**
- **W przypadku dużych umów istnieje często możliwość negocjowania warunków**