DANE OSOBOWE PO NOWEMU

PRCH Legal Club

Warszawa, 10.10.2017

STRONG PARTNERS IN GDPR

KIM JESTEŚMY

MAGNUSSON

- Magnusson to międzynarodowa firma prawnicza o silnej pozycji lokalnej, obecna na polskim rynku od 2001 roku
- Kancelaria posiada wieloletnie doświadczenie w zakresie prawa własności intelektualnej, ochrony danych osobowych i nowych technologii

F-SECURE

- Założona w 1988 spółka pochodząca z Finlandii, notowana na giełdzie Helsinki Stock Exchange od 1999
- Eksperci F-Secure uczestniczyli w największej ilości dochodzeń związanych z cyberprzestępczością w Europie w porównaniu do jakiejkolwiek innej firmy na rynku

Łączymy siły na potrzeby RODO, przeprowadzamy wspólne audyty, wdrażamy nowe przepisy, zapewniamy utrzymanie odpowiedniego poziomu bezpieczeństwa prawnego i IT

DZIŚ DOWIESZ SIĘ...

1. Co to jest RODO i czy powinniśmy się bać nowych regulacji?
2. Jaki jest stan cyberbezpieczeństwa w Polsce i na świecie?
3. Strategia bezpieczeństwa i analiza ryzyka; reagowanie na incydenty
4. Wdrożenie nowych funkcjonalności systemu IT wymaganych przepisami RODO
5. Kluczowe zmiany ochrony danych osobowych dla branży retail i nieruchomości (sklepy online, aplikacje mobilne, marketing, monitoring wizyjny)
6. Przygotowanie planu wdrożenia RODO w firmie

RODO / GDPR

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

- Weszło w życie 24 maja 2016
- Stosuje się od 25 maja 2018

JUŻ JEST PÓŹNO

DANE OSOBOWE

Informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej

Osoba, którą można bezpośrednio lub pośrednio zidentyfikować,
w szczególności na podstawie identyfikatora:

- imię i nazwisko
- numer identyfikacyjny
- dane o lokalizacji
- identyfikator internetowy

DANE OSOBY FIZYCZNEJ

Osoby fizyczne i przykładowe zbiory danych

KONSUMENCI

- wszelkie operacje B2C, sklep online, reklamacje, telemarketing,
- marketing: newsletter, wizytówki, fanpage na facebooku

KONTRAHENCI, OSOBY KONTAKTOWE ZE STRONY KLIENTA

- operacje B2B, korespondencji, faktury, bazy marketingowe, CRM

OSOBY POSTRONNE PRZYPADKOWE

- monitoring wizyjny, książka korespondencyjna, rejestr gości obiektu

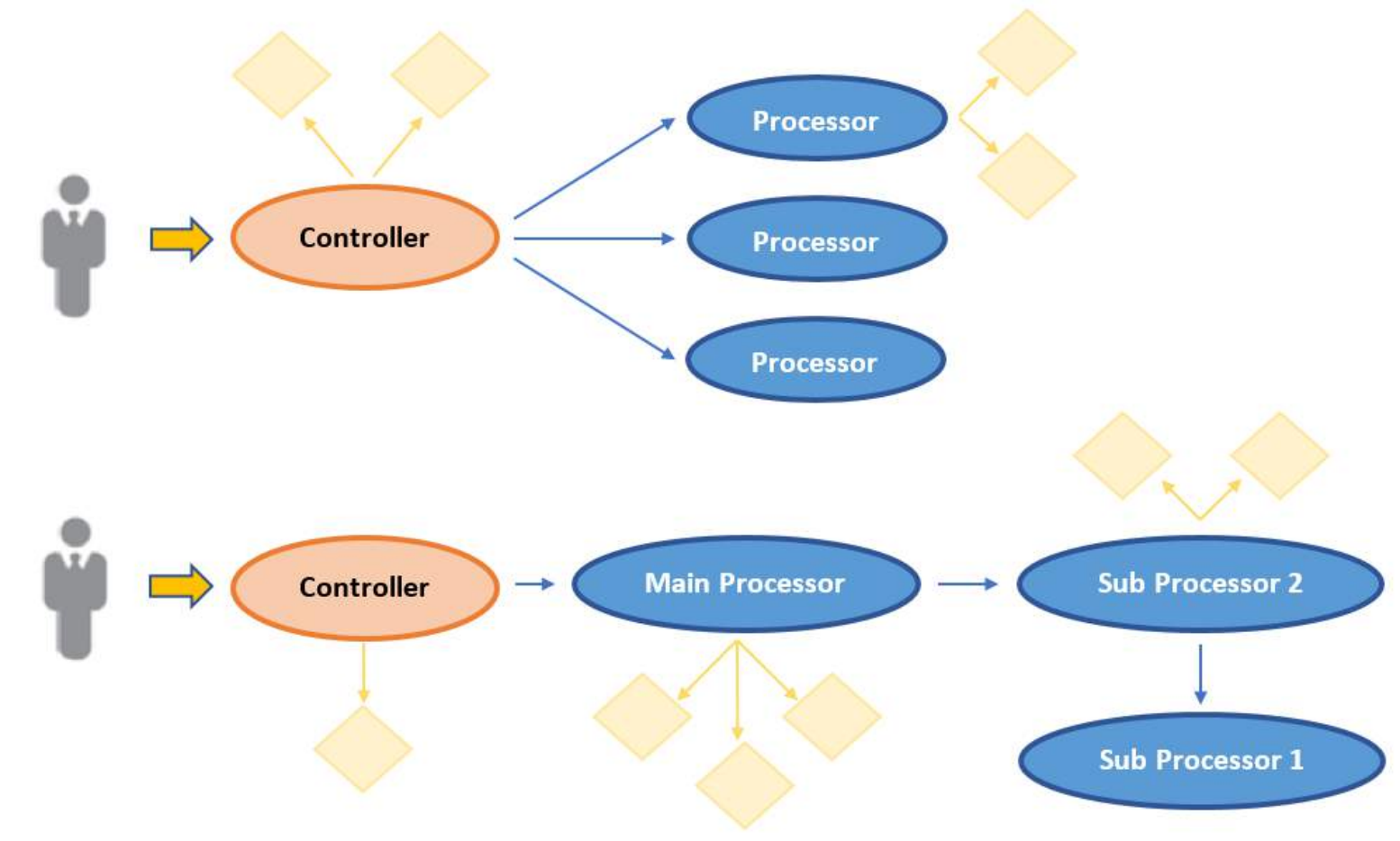
PRACOWNICY

KAŻDY PRZEDSIĘBIORCA PRZETWARZA DANE OSOBOWE

CZYM JEST PRZETWARZANIE?

Zbieranie	Przeglądanie	Łączenie
Utrwalanie	**Przechowywanie**	Ograniczenie
Porządkowanie	Pobieranie	Usuwanie
Modyfikowanie	Ujawnianie	Udostępnianie

CONTROLLER / PROCESSOR



SFERY ODDZIAŁYWANIA RODO

Prawo

- ✓ weryfikacja umów (klauzule powierzenia przetwarzania)
- ✓ weryfikacja zgodności z prawem (klauzule zgody)
- ✓ spełnianie obowiązku informacyjnego

Technologia

- ✓ bezpieczeństwo sieciowe
- ✓ infrastruktura IT
- ✓ funkcjonalności systemów IT

Struktura

- ✓ odpowiednie procedury i polityki (wdrożenie i rzeczywiste przestrzeganie)
- ✓ DPO
- ✓ wiedza personelu

CELE RODO

Prawo do prywatności
Prawo do ochrony danych osobowych

Zaufanie do e-usług

Bezpieczeństwo informacji

Cyberbezpieczeństwo

Swobodny przepływ danych osobowych w UE

(jednolity rynek cyfrowy)

SANKCJE

do 10 MLN EUR lub do 2% całkowitego rocznego światowego obrotu

- brak prawidłowego przetwarzania danych
- brak zastosowania odpowiednich środków technicznych i organizacyjnych w celu ochrony przetwarzania
- niezawiadomienie odpowiednich organów o naruszeniu bezpieczeństwa
- niewyznaczenie Inspektora Ochrony Danych w przypadku, gdy było to obowiązkowe
- brak podstawy do przetwarzania danych

do 20 MLN EUR lub do 4% całkowitego rocznego światowego obrotu

- naruszenie praw lub wolności podmiotów danych
- przekazywanie danych do podmiotów poza EOG w sposób niezapewniający odpowiedniego poziomu bezpieczeństwa
- nieprzestrzeganie nakazów lub zakazów nałożonych przez organ nadzorczy itp.

CZYNNIKI ŁAGODZĄCE I OBCIĄŻAJĄCE

- Charakter, waga, czas trwania naruszenia, kategorie danych
- Umyślność bądź nieumyślność
- Działania w celu minimalizacji szkody
- Stopień odpowiedzialności (przyczynienia się)
- „Recydywa”, wcześniej zastosowane środki
- Stopień współpracy z organem, czy była notyfikacja
- Stosowanie kodeksów postępowania lub mechanizmów certyfikacji

CYBERBEZPIECZEŃSTWO

Zestaw środków organizacyjnych, prawnych, technicznych, fizycznych i edukacyjnych w celu zapewnienia nieprzerwanego funkcjonowania cyberprzestrzeni

Cechy:

- ciągłość funkcjonowania
- brak nieautoryzowanego dostępu
- brak nieautoryzowanego wykorzystania
- brak nieautoryzowanej zmiany
- brak uszkodzenia bez względu na przyczynę

Cyberprzestrzeń – przestrzeń przetwarzania i wymiany informacji przez syste teleinformatyczne.

DYREKTYWA NIS

- operatorzy usług kluczowych: bankowość, rynki finansowe, energetyka, transport, ochrona zdrowia
- dostawcy usług cyfrowych: internetowe platformy handlowe, usługi przetwarzania w chmurze oraz wyszukiwarki internetowe

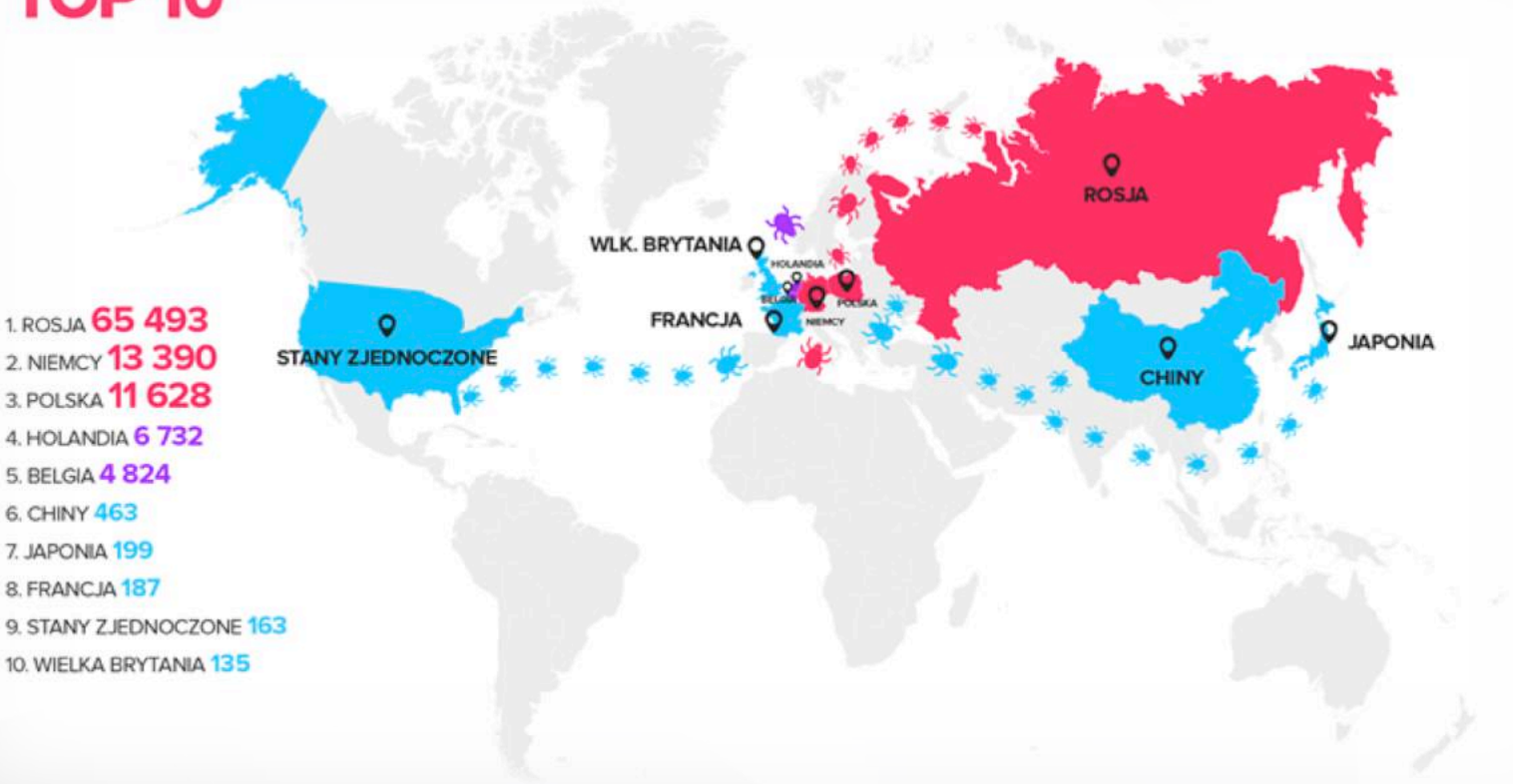
ustanowienie procedur i obowiązku zgłaszania incydentów

ustanowienie szczególnych wymogów dotyczących zapewniania bezpieczeństwa

przyjęcie na poziomie krajowym strategii w zakresie bezpieczeństwa sieci i systemów IT

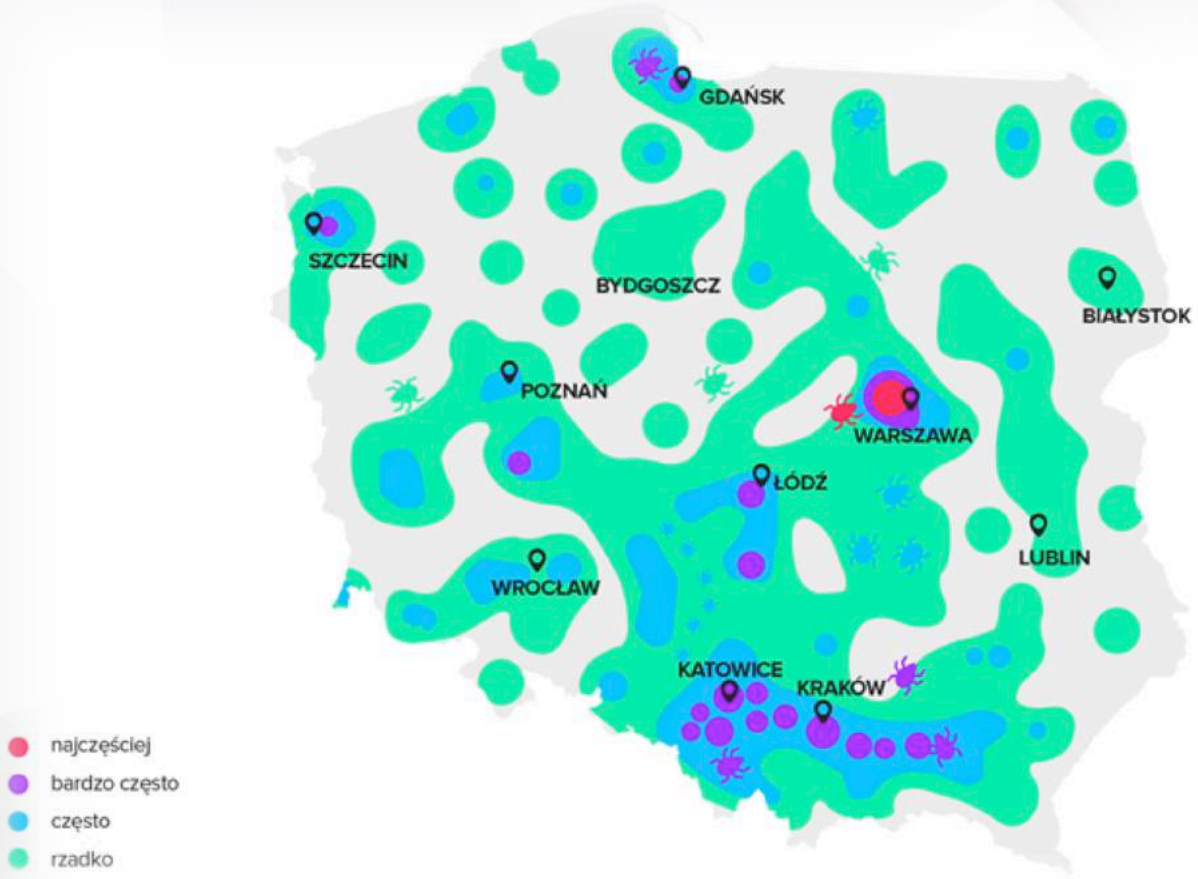
ATAKI NA POLSKĘ

TOP 10



1. ROSJA 65 493
2. NIEMCY 13 390
3. POLSKA 11 628
4. HOLANDIA 6 732
5. BELGIA 4 824
6. CHINY 463
7. JAPONIA 199
8. FRANCJA 187
9. STANY ZJEDNOCZONE 163
10. WIELKA BRYTANIA 135

ATAKOWANE MIEJSCA W POLSCE

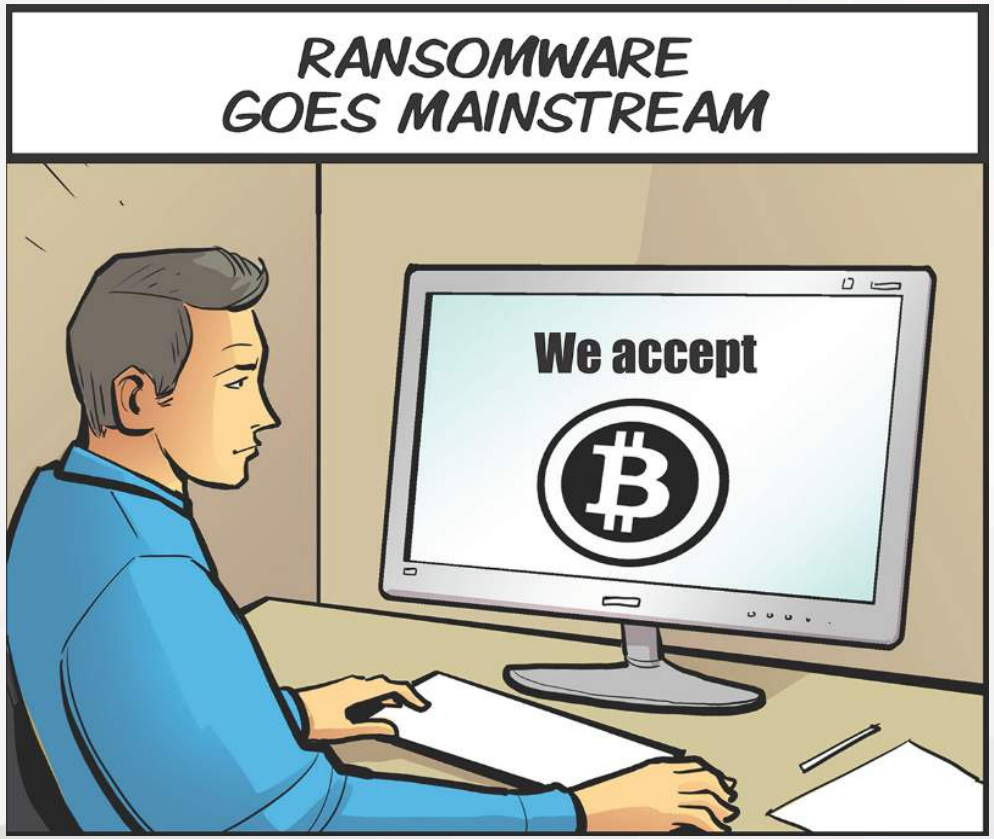


RANSOMWARE

Poczta Polska
Kurier nie dostarczył przesyłkę do numeru zgłoszenia RR6475929527PL na adres 7.20.2015, ponieważ nikt w tym czasie. Proszę zobaczyć informacje na temat wysyłki, drukowania i iść na pocztę, aby otrzymać pakiet.
Zobacz informacje
Uwaga
Jeżeli przesyłka nie dotrze w ciągu 7 dni roboczych Poczta Polska będzie miała prawo do ubiegania się koszty utrzymania przesyłka 50 zł za jeden dzień. Dziękujemy za korzystanie z naszych usług dostawy. Życząc miłego dnia Twoja Poczta Polska.
To jest generowany automatycznie e-mail, kliknij jeżeli chcesz się wypisać
Poczta Polska S.A. (c) 2015. Wszelkie prawa zastrzeżone.

Wana Decrypt0r 2.0
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/15/2017 16:32:52
Time Left
02:23:59:49
Your files will be lost on
5/19/2017 16:32:52
Time Left
06:23:59:49
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

RANSOMWARE: WANNACRY



H2 2016: NSA > ShadowBroker

03.2017: Microsoft SMB patch

05.2017: **WannaCry**

05.2017: Microsoft SMB patch WinXP

@MalwareTech

Killswitch: iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

RANSOMWARE: WANNACRY

Statystyki - 05.2017:

- ~200 000 zainfekowanych stacji
- 261 ofiar zapłaciło okup
- 40,5BTC
- ~70000 USD

RANSOMWARE: SWIFT

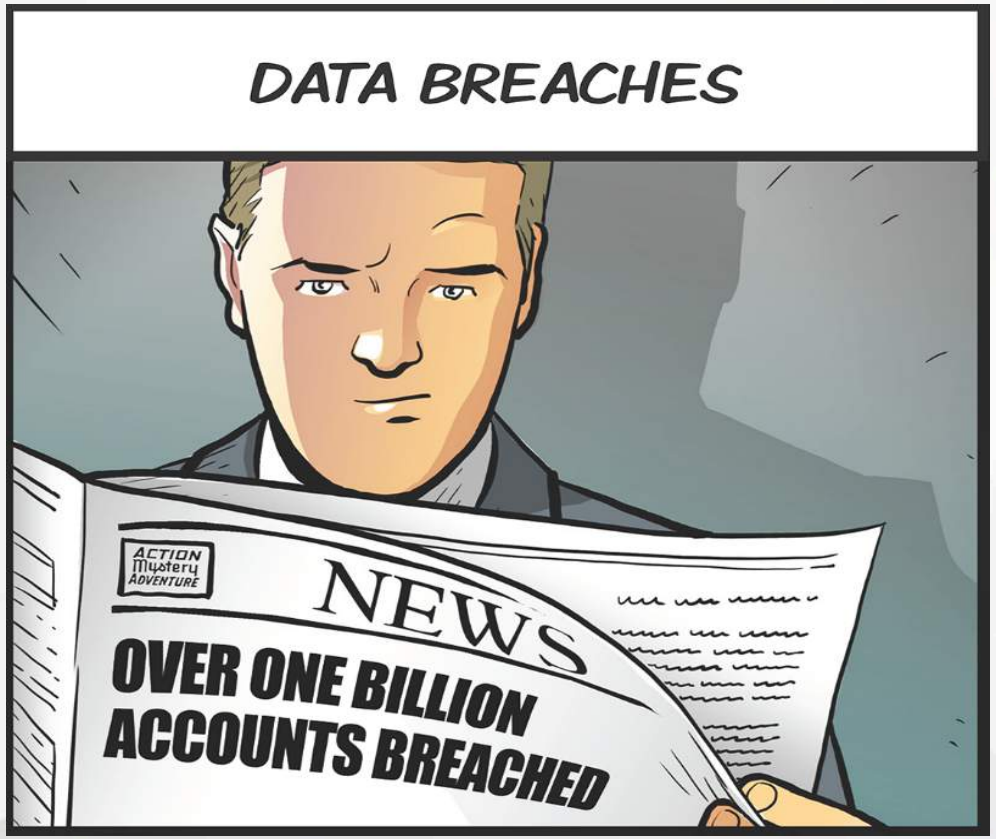
Bank Centralny – Bangladesz

81 milionów USD

Banco del Austro – Ekwador

12 milionów USD

WYCIEKI DANYCH



Kancelaria Mossack Fonseca:

- 11 milionów dokumentów w wycieku „Panama Papers”

Yahoo 2013/2014

- Największy wyciek danych użytkowników - 1miliarda użytkowników (500 milionów skrzynek webmail)

RANSOMWARE, A RODO?

```
victor@windowlicker:~$ mongo --host [redacted]
MongoDB shell version v3.4.1
connecting to: mongodb://[redacted]/
MongoDB server version: 2.2.0
WARNING: shell and server versions do not match
> show dbs
WARNING          0.203GB
[redacted]
> use WARNING
switched to db WARNING
> show collections
WARNING
system.indexes
> db.WARNING.find()
{ "_id" : ObjectId("5859a0370b8e49f123fcc7da"), "mail" : "harak1r1@sigaint.org"
, "note" : "SEND 0.2 BTC TO THIS ADDRESS 13zaxGVjj9MNc2jyvDRhLyYpkCh323MsMq AND
 CONTACT THIS EMAIL WITH YOUR IP OF YOUR SERVER TO RECOVER YOUR DATABASE !" }
> exit
bye
victor@windowlicker:~$ ^C
victor@windowlicker:~$
```

Harak1r1 group

- Atak na bazy danych MongoDB – ponad 8000 przejętych instancji
- Okup w wysokości 0.2 BTC (~3000 PLN)

0.2 BTC

vs

2% rocznego obrotu

KAŻDY JEST CELEM…

WYMAGANIA BEZPIECZEŃSTWA

ZMIANA PODEJŚCIA DO OCHRONY DANYCH - ***risk base approach***

- zapewnienie bezpieczeństwa oparte na analizie skutków i ryzyka
- proces ciągłego dostosowywania poziomu bezpieczeństwa w miejsce jednorazowej zmiany
- odpowiednie środki techniczne i organizacyjne

JAKIE HASŁO JEST BEZPIECZNE ?

„co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne” + „zmiana co 30 dni”

PSEUDONIMIZACJA I SZYFROWANIE

Anonimizacja – nieodwracalne uniemożliwienie identyfikacji danych

Żadna ze stron nie ma możliwości wyodrębnienia poszczególnych danych ze zbioru.

Proces jest nieodwracalny!

W przypadku anonimizacji nie mówimy o przetwarzaniu danych osobowych (w kontekście RODO)

Pseudonimizacja – zastąpienie jednego atrybutu w zapisie innym atrybutem

Przykłady:

- Szyfrowanie: posiadacz odpowiedniego klucza może bez problemu zidentyfikować dane
- Funkcja skrótu: Marcin Galeja > ‚MG’ lub ‚M*n G*a’

W dalszym ciągu przetwarzamy dane osobowe.

WŁAŚCIWOŚCI SYSTEMU

Poufność – przydzielenie odpowiednich ról dostępowych do danych

Integralność – kontrola nad edycją danych i możliwościami ich zmiany

Dostępność – zapewnienie dostępu do danych osobowych

Odporność – brak podatności na ataki zewnętrzne/wewnętrzne

Zdolność przywrócenia dostępności – odpowiednia polityka backupu danych

MONITORING I OCENA SKUTECZNOŚCI

Regularne audyty bezpieczeństwa oraz testy penetracyjne

Analiza podatności oraz bieżące ich usuwanie

Security Operation Center – zewnętrzna analiza zdarzeń

INCYDENTY

- Naruszenie ochrony danych osobowych

Naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych

- Rola Kodeksów Postepowania i mechanizmów certyfikacji

RODZAJE INCYDENTÓW

- Włamanie
- DoS / DDoS
- Defacement (strona www)
- Narzędzia sociotechniczne
- Insider attack
- Wyciek poufnych informacji
- Blackmailing (szantaż)
- Phishing (próby wyłudzenia)
- Malware

IR VS FORENSICS

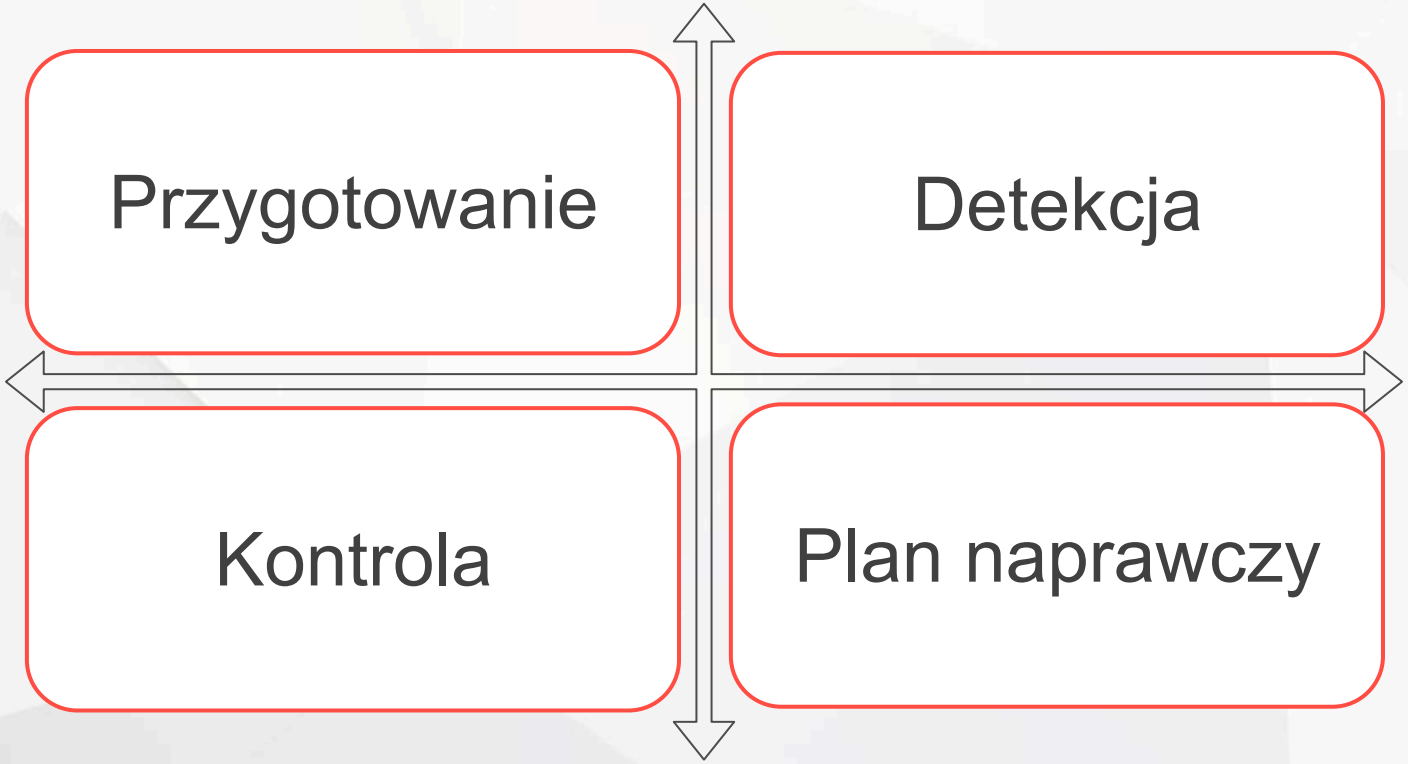
Incident Response

- Atak prawdopodobnie cały czas trwa
- Działające systemy
- Czynniki środowiskowe (komputer użytkownika vs. stacja kontrolująca linie produkcyjne)
- Inne (minimalizacja szkód, zachowanie dowodów)

Forensics

- Analiza prawna / informatyka śledcza
- Zbieranie dowodów
- Zazwyczaj analizowane są dane „offline” (obraz dysku / zrzut pamięci RAM)

INCYDENT – CO ROBIĆ?



PRZYGOTOWANIE

- Przydzielenie odpowiednich ról
- Przygotowanie planu IR
- Utrzymywanie dokumentacji
  - ✓ Diagramy sieciowe
  - ✓ Reguły na firewall
  - ✓ Serwery – historia aktualizacji
  - ✓ Serwery – dopuszczone role/ usługi
  - ✓ Kopia zapasowa
- Logowanie
  - ✓ Centralne zbieranie logów
  - ✓ Retencja logów
  - ✓ Poziom szczegółowości logów

DETEKCJA

- Użytkownicy (niestandardowe wydarzenia na stacjach roboczych)
  - ✓ wewnętrzne szkolenia – podnoszenie świadomości użytkowników!
- Administratorzy
- Alerty z systemów IPS/IDS/Firewall
- Alerty aplikacji antywirusowych

- Zewnętrzny monitoring – SOC / usługa IR

KONTROLA

- Oszacowanie sytuacji
  - **Do not panic!**
  - Współpraca z innymi administratorami
  - Geneza i rozpoznanie przyczyny incydentu
- Izolacja środowiska gdzie wystąpił incydent
- Zapobieganie rozprzestrzenianiu
- Zebranie i zabezpieczenie dowodów

PLAN NAPRAWCZY

- Usunięcie pozostałości po incydencie (malware / rootkits)
- Usunięcie dostępnych wektorów ataku (aktualizacja lub zmiana konfiguracji)
- Przywrócenie do działania wszystkich usług

NOTYFIKACJE INCYDENTÓW

OBOWIĄZEK

Zgłoszenie naruszenia w ciągu 72h organowi nadzoru – wyjątek małe ryzyko

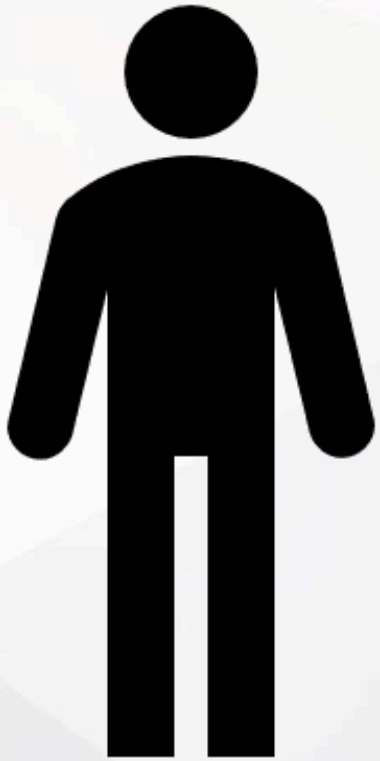
Zawiadomienie osoby, której dane dotyczą o naruszeniu – zasada duże ryzyko

PODSTAWY PRZETWARZANIA DANYCH

1.ZGODA

1.wypełnienia **obowiązku prawnego ADO**

1.zadania w interesie publicznym / **władzy publicznej**



1.wykonania umowy

ochrona żywotnych interesów osoby

1.PRAWNIE UZASADNIONY INTERES ADO

UPRAWNIENIA JEDNOSTEK

Prawo do informacji i dostępu do danych
Prawo do przenoszenia danych
Prawo do bycia zapomnianym
Zgoda na profilowania

Prawo do sprostowania
Prawo do uzupełnienia danych
Prawo do ograniczenia
Prawo do sprzeciwu

KLUCZOWE ZMIANY DLA BRANŻY

kontrola dostępu

monitoring wizyjny

aplikacje mobilne

KLUCZOWE ZMIANY DLA BRANŻY

klienci sklepu

sklep online

marketing

RYZYKO BRAKU WDROŻENIA

Ryzyko operacyjne

- „niekompatybilność” z innymi przedsiębiorcami z UE
- wyeliminowanie z rynku przez konkurencję (utrata rynku)
- problemy z transferem danych
- kontrole organów połączone z postanowieniem ograniczenia przetwarzania danych

Ryzyko finansowe

- kary administracyjne
- odszkodowania w drodze powództw cywilnych
- koszty procesowe
- utrata przychodów (także spodziewanego zysku)

Ryzyko wizerunkowe

- naruszenie prestiżu firmy, spadek renomy marki
- utrata zaufania klientów, odejścia klientów

PROPOZYCJE WDROŻENIA RODO

1.
Audyt
Oszacowanie ryzyka

2.
Przygotowanie
i wdrożenie strategii

3.
Bieżące zarządzanie
Monitoring i aktualizacja

PROPOZYCJE DZIAŁAŃ

- Inwentaryzacja danych
- Oznaczenie grup danych, badanie ich legalności, zbadanie spełnienia obowiązku informacyjnego
- Zbadanie dostępu do danych wewnątrz i z zewnątrz organizacji (*data flow mapping*)
- Inspektor Ochrony Danych – powołanie
- Wdrożenie polityk i procedur związanych z bezpieczeństwem w organizacji
- Audyt umów organizacji
- Szkolenia
- Ubezpieczenie

DZIĘKUJEMY ZA UWAGĘ

Wioletta Kulińska
Adwokat

wioletta.kulinska@magnussonlaw.com
M: +48 606 969 746

Marcin Galeja
Sales Engineer

marcin.galeja@f-secure.com
M: +48 665 223 227