Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

fundacja instytut
CYBERBEZPIECZEŃSTWA

Bezpieczny backup: jak uniknąć szantażu i sabotażu danych?

fundacja instytut
CYBERBEZPIECZEŃSTWA

Łukasz Nowatkowski

```
r02id@Foockin-Klingon ~ % Łukasz Nowatkowski, r02id, cybersecurity advocate, golfer
zsh: command not found: Łukasz
r02id@Foockin-Klingon ~ %
```

Tomasz Wiertelak

Fan chmury

Pasjonat cyberbezpieczeństwa

Audytor wiodący ISO 27001

Wykładowca akademicki

ISSA POLSKA

AGENDA

- LICZBY MÓWIĄ SAME ZA SIEBIE! 60 / 50 / 30
- ARCHIWIZACJA, BACKUP CZY TO TO SAMO?
- A CO Z CHMURĄ
- CZY BACKUP ZAWSZE NAS OCHRONI?

LICZBY 60 / 50 / 30

- 60% małych i średnich firm dotkniętych atakiem nie istnieje
- 50% ataków to ransomware
- 30% “backupujących” nie testuje kopii

C I A

Confidentiality

- Zapewnienie, że dane są dostępne tylko dla autoryzowanych osób lub systemów
- Ochrona przed nieuprawnionym dostępem i ujawnieniem informacji

Integrity

- Gwarancja, że dane pozostają **dokładne, kompletne i niezmienione** podczas przechowywania i transmisji
- **Zapobieganie nieautoryzowanym modyfikacjom danych**

Availability

- Zapewnienie, że dane i systemy są **dostępne** dla uprawnionych użytkowników, gdy są **potrzebne**
- Ochrona przed przerwami w **dostępie do danych** i systemów

CO NA TO PRAWO?

GDPR

- Art. 5 ust. 1 lit. f: „Dane osobowe muszą być przetwarzane w sposób zawierający 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”)
- Art. 32. ust. 1 lit. b: ”zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania”

CO NA TO PRAWO?

Ustawa o Krajowym Systemie Cyberbezpieczeństwa

- Art. 2 ust. 4: „cyberbezpieczeństwo – odporność systemów informacyjnych na działania naruszające poufność, **integralność, dostępność** i autentyczność przetwarzania danych lub związanych z nimi usług oferowanych przez te systemy.”
- Art. 8 ust. 4 lit. d: „wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, **integralność, dostępność** i autentyczność informacji;”

ARCHIWIZACJA CZY BACKUP?

ARCHIWIZACJA

- Długoterminowe przechowywanie danych, które nie są aktywnie używane, ale mogą być potrzebne w przyszłości
- Jednorazowa lub rzadka operacja
- Rzadki dostęp
- Długi okres przechowywania, często lata lub dekady
- Optymalizacja skupia się na kosztach i oszczędności miejsca

BACKUP

- Kopie aktywnych danych w celu ich ochrony przed utratą lub uszkodzeniem
- Operacja regularna, najczęściej codzienna
- Szybki dostęp w razie potrzeby natychmiastowego odtworzenia danych
- Krótki okres przechowywania danych
- Optymalizacja skupia się na szybkości tworzenia kopii zapasowych i odtwarzania danych

A CO Z CHMURĄ?

Responsibility	SaaS	PaaS	IaaS	On-prem
Information and Data	Customer	Customer	Customer	Customer
Devices (Mobile and PCs)	Customer	Customer	Customer	Customer
Accounts and Identities	Customer	Customer	Customer	Customer
Identity and directory infrastructure	Vendor / Customer	Vendor / Customer	Customer	Customer
Applications	Vendor	Vendor / Customer	Customer	Customer
Network Controls	Vendor	Vendor / Customer	Customer	Customer
Operating system	Vendor	Vendor	Customer	Customer
Physical hosts	Vendor	Vendor	Vendor	Customer
Physical network	Vendor	Vendor	Vendor	Customer
Physical datacenter	Vendor	Vendor	Vendor	Customer

Vendor Customer

Model współdzielenia odpowiedzialności

- dostawca chmury odpowiada za usługę przetwarzającą Twoje dane.
- właścicielem danych jest korzystający z usługi.

cloud mail, cloud storage

źródło: ochk

NAJLEPSZE PRAKTYKI

- Strategia 3-2-1 + rozszerzone strategie
- Automatyzacja i plany kopii zapasowych
- Szyfrowanie i bezpieczeństwo
- Kategoryzacja i priorytetyzacja danych
- Testowanie kopii
- Monitorowanie i zarządzanie
- Zgodność i audyty
- Rozwiązania hybrydowe

Obszary przetwarzania danych

- **Data recovery / Dane i przywracania**
- **Storage and Access / Magazyn danych i dostęp**
- **Transmission / Transmisja**
- **Isolation / Izolacja**

Bezpieczeństwo sferyczne

nowa doktryna w cyberbezpieczeństwie

Bezpieczeństwo sferyczne

- **Wielowarstwowość**
- **Centralna rola danych**
- **Dynamiczna ochrona**
- **Zaawansowane technologie**
- **Adaptacyjność**

Jakie dane chronić? / Data Protection Trends

- 70% bazy danych
- 58% konfiguracje systemowe
- 54% pliki aplikacyjne

- dane w pamięci ulotnej
- logi systemowe - to one pomagają w analizie powłamaniowej

fundacja instytut

CYBERBEZPIECZEŃSTWA