

BEZPIECZEŃSTWO SYSTEMÓW KOMPUTEROWYCH

Adam Karczewski

CZY BEZPIECZEŃSTWO JEST WAŻNE?

- Wirus Sobig - straty na 38.5 mld USD (2003)
- Wirus Stuxnet - uszkodzenie wirówek do uranu (2010)
- Wpływ na wyniki wyborów USA, Francja (2016,2017)
- Handel danymi osobowymi

PODSTAWOWE ZAGROŻENIA

- Zamierzone (aktywne), związane z działaniami wykonywanymi z premedytacją, świadomie wykraczające poza obowiązki, szpiegostwo, wandalizm, terroryzm, itd.
- Losowe (pasywne) wewnętrzne, to niezamierzone błędy ludzi, zaniedbania użytkowników, defekty sprzętu i oprogramowania, zniekształcania lub zagubienie informacji, itd.
- Losowe (pasywne) zewnętrzne, to skutki działania temperatury, wilgotności, zanieczyszczenia powietrza, zakłócenia źródła zasilania, wyładowania atmosferyczne, klęski żywiołowe.

•

SKUTKI BIZNESOWE

- Bezpośrednie straty finansowe, np. dominującej technologii
- Pośrednie straty finansowe, np. koszty sądowe, sankcje prawne
- Utrata prestiżu, wiarygodności, klientów i kontrahentów.
- Przerwa w pracy, utrata sprzętu, dezorganizacja, załamanie działalności
- Konieczność wymiany oferowanych produktów
- Konieczność zmiany konfiguracji systemu komputerowego
- Wzrost składek ubezpieczeniowych
- Ucieczka kadry

.

POPULARNE ZAGROŻENIA

- Złośliwe oprogramowanie: wirusy, konie trojańskie, itp.
- Ataki blokady usług DoS (ang. Denial of Service) oraz DDoS (ang. Distributed DoS) realizowane często przez komputery zombie i sieci botnet
- SPAM – niechciana poczta elektroniczna i inne przekazy
- Phishing to oszukańcze pozyskanie poufnej informacji osobistej, np. hasła, przez udawanie osoby godnej zaufania, której te informacje są pilnie potrzebne
- Intruzi - nieupoważniona osoba próbująca włamać się do systemu informatycznego, może działać na poziomie personalnym, firm (szpiegostwo przemysłowe), globalnym (wojna informatyczna)

BEZPIECZEŃSTWO W INTERNECIE

BEZPIECZNE HASŁO

- Długość
- Złożoność
- Oryginalność

	Liczba			Liczba			Liczba	
	Liczba	Hasło		Liczba	Hasło		Liczba	Hasło
1	46818	123456	21	3563	agnieszka	41	2621	qazwsx
2	16682	qwerty	22	3450	bartek	42	2615	natalia
3	13093	123456789	23	3366	polska1	43	2589	0
4	10138	12345	24	3351	password	44	2583	lukasz
5	10113	zaq12wsx	25	3348	qwe123	45	2519	piotrek
6	6538	polska	26	3343	damian	46	2516	dupa
7	6220	111111	27	3266	1qaz2wsx	47	2489	daniel
8	5774	1234	28	3227	michal	48	2389	madzia
9	5182	misiek	29	3025	samsung	49	2383	1q2w3e
10	4776	monika	30	3024	qwerty123	50	2366	1q2w3e4r
11	4418	marcin	31	3020	zxcvbnm	51	2327	misiaczek
12	4369	12345678	32	3000	kacper	52	2323	patryk
13	4240	mateusz	33	2920	maciek	53	2241	komputer
14	4108	123qwe	34	2896	kasia	54	2236	dragon
15	4086	123	35	2885	kochanie	55	2217	haslo1
16	4073	1234567	36	2841	qwertyuiop	56	2213	adrian
17	3933	123123	37	2816	lol123	57	2208	abc123
18	3874	1.23E+09	38	2772	myszka	58	2177	matrix
19	3850	qwerty1	39	2696	kasia1	59	2173	mateusz1
20	3620	karolina	40	2683	666666	60	2147	kochamcie

CERTYFIKAT BEZPIECZEŃSTWA

- SSL
- Https
- Szyfrowanie

OCHRONA WPROWADZANYCH INFORMACJI



WIARYGODNOŚĆ ADRESU

Wiadomość dotycząca bezpieczeństwa. Twoje konto mBank zostało tymczasowo zablokowane. Odebrane x

 **mBank** przez s7.jupe.pl 14:15 (7 minut temu) ☆  
do mnie ▾

Szanowny kliencie,



Twój dostęp do serwisu transakcyjnego mBank Online został tymczasowo zablokowany ze względów bezpieczeństwa.

Wykryliśmy podejrzaną działalność związaną z Twoim kontem bankowym.

Aby uzyskać więcej informacji oraz odblokować dostęp online, należy przejść na stronę mBanku <https://online.mbank.pl/pl/odblokuj> i zweryfikować swoje dane.

Pozdrawiamy,
Zespół mBanku

From: Kundenservice DHL Logistik [mailto:stegnitz@silometal.sk]

Sent: Wednesday, May 20, 2015 9:56 AM

To:

Subject: Obecny stan przesyłki DHL

Sledzenie trasy przesyłki DHL

DHL Sendungsverfolgung

Numer przesyłki

49177414936436

Produkt / serwis

DHL RETOURE

Status od środa, 20.05.2015
07:55:19

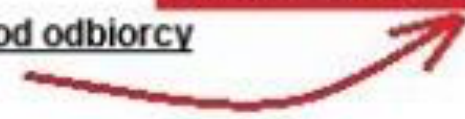
Przesyłka jest przygotowywana w początkowym centrum
pakowania.

Doreczono do

Przesyłka zwrotna do nadawcy

<http://www.cetil.com.uy/4if30oexj8y>
Kliknij, aby śledzić łącze

Sprawdź informacje od odbiorcy
(ZIP Format)





Twoje centrum e-płatności

Informacja o płatności:

Odbiorca: DotPay S.A.
Opis: Dopłata do przesyłki

Kwota: 1 PLN

Wybrany kanał płatności:

Karty płatnicze



Szybkie transfery



- Wylogowywanie się
- Ostrożnie z danymi osobowymi
- Aktualny antywirus
- Regularne kopie zapasowe
- Ostrożnie z załącznikami
- Unikanie publicznych WiFi
- Lepsze łącze kablowe niż WiFi
- Selekcja informacji w SM
- Uwaga na reklamy i AdWare
- Smartphone też jest komputerem

WARTOŚĆ INFORMACJI

- Koszty związane z czasową jej **niedostępnością**
- Koszty wynikające z **utraty informacji**
- Koszty wynikające z zafałszowania informacji lub wystąpienia ukrytych błędów
- Koszty ponownego pozyskania i wprowadzenia danych
- Koszty **korekty** błędnych danych

\$5,000 REWARD
Backpack with PhD Data
No Questions Asked

call +1 (315) 657-5266 or +1 (315) 546-6207

Google Voice: 352-561-8317


Whats app +90 543 493 97 30

cloismeg@gmail.com

When: Nov 25 (Saturday) around noon

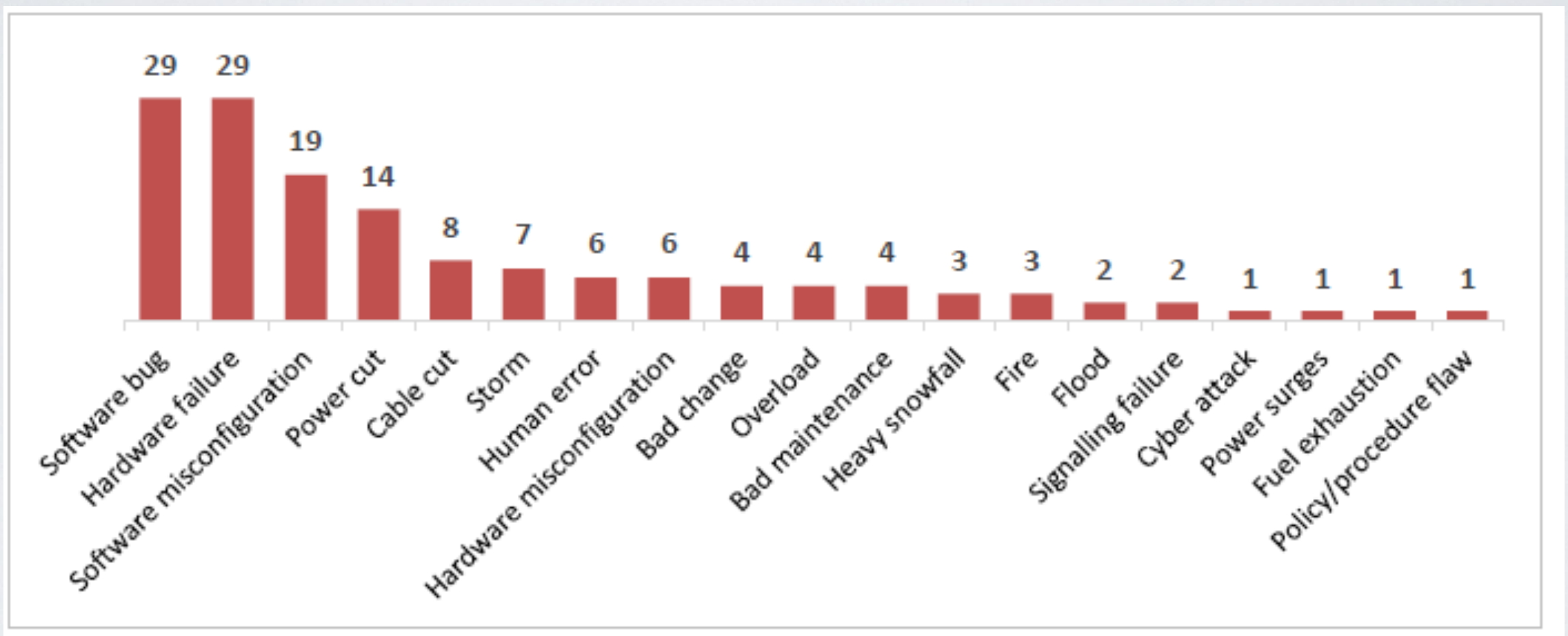
What: backpack with PhD data on thumb drives, Lenovo laptop, handwritten notebook, leather bag, Lenovo laptop

Where: My car at Drummond and Sherbrooke street parking

 **cotopaxi**



NAJCZĘSTSZE POWODY PROBLEMÓW



ARCHIWIZACJA DANYCH

CEL

- data archiving
- Przeniesienie danych w inne miejsce w pamięci masowej
- Archiwizacja != Kopia bezpieczeństwa
- Dane starsze, mniej używane przenoszone na tańszy nośnik

SPOSOBY PRZEPROWADZANIA

- Przeprowadzona w regularnych odstępach czasu
- Dane poddawane są kompresji i deduplikacji
- Często stosuje się archiwizację hierarchiczną

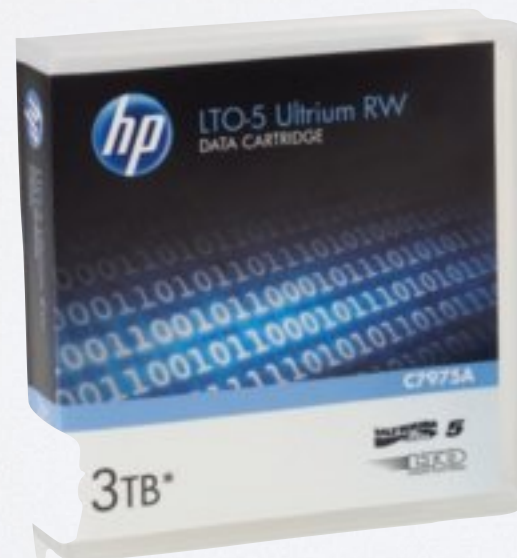
PODSTAWOWE PARAMETRY

- Okres podlegający archiwizacji
- Czas przechowywania (retencji) danych
- Możliwości modyfikacji archiwum

TECHNICZNE REALIZACJE

- Płyta DVD - słaby pomysł, ryzyko utlenienia warstwy refleksyjnej
- M-Disc: materiał podobny do kamienia, koszt około 15zł/25GB, trwałość 1000lat
- Specjalne pamięci FLASH np Memory Vault, gwarantowana trwałość 100 lat

- Taśmy magnetyczne: 30 lat, bardzo duże pojemności, tanie, system LTFS 5



KOMPRESJA

DEFINICJA

- data compression
- Zmiana sposobu zapisu informacji tak, aby zmniejszyć redundancję i tym samym objętość zbioru
- Wyrażenie tego samego zestawu informacji za pomocą mniejszej liczby bitów
- Kompresja bezstratna i stratna

ZIP

- Kompresja bezstratna + archiwizacja
- Głównie Windows
- Różne algorytmy kompresji

7Z

- Wysoki stopień kompresji
- Silne szyfrowanie
- Nazwy plików w Unicode
- Maksymalna wielkość archiwum jest określona na poziomie 16 000 000 000 GB
- Obsługiwany przez 7-Zip

RAR

- Kompresja bezstratna
- Szyfrowanie AES-128 (opcjonalne)
- Obsługuje WinRAR

TAR

- Stosowany w Linuxie
- Tylko archiwizacja
- `tar [opcje] źródło`
 - **-c** – tworzy plik w formacie tar
 - **-f** – określa nazwę pliku archiwum tar
 - **-v** – wypisuje nazwy wszystkich plików
 - **-x** – wyodrębnia wymienione pliki
 - **-t** – wyświetla zawartość archiwum
 - **-r** – włącza bezwarunkowe dołączanie plików do archiwum
 - **-u** – powoduje dołączenie do archiwum tylko tych plików, które są nowsze niż ich odpowiedniki w archiwum

KOMPRESJE LINUX

- GZIP + TAR = .tar.gz (tgz)
- BZIP2 + TAR = .tar.bz2
- COMPRESS + TAR = .tar.Z
- Opcje kompresji w tar:
 - **-z** – włącza kompresję programem `gzip`
 - **-j** – włącza kompresję programem `bzip2`
 - **-Z** – włącza kompresję programem `compress`
 - **-J** – włącza kompresję programem `xz`

KOPIA ZAPASOWA (BACKUP)

BACKUP

- dane, które mają służyć do odtworzenia oryginalnych danych w przypadku ich utraty lub uszkodzenia,
- ochrona przed awarią podzespołów,
- ochrona przed błędami użytkownika, np. nadpisanie

RODZAJE BACKUPU

- Backup pełny to kompletna kopia zapasowa wszystkich danych.
- Backup dyferencjalny, różnicowy lub kumulacyjny - tworzenie kopii zapasowej tylko tych danych, które zostały zmodyfikowane od ostatniego pełnego backupu.

- Backup przyrostowy lub inkrementalny - kopiowane są dane, które zostały zmienione od czasu ostatniego pełnego lub przyrostowego backupu. Chcąc dokonać przywrócenia danych potrzeba ostatniego pełnego backupu oraz wszystkich zrobionych po nich backupów inkrementalnych.
- Backup syntetyczny jest kopią zapasową wszystkich danych, ale tworzona nie na podstawie aktualnego stanu systemu, tylko na bazie wszystkich innych najbardziej aktualnych rodzajów backupu.

BACKUP OFFLINE (I NIE TYLKO)

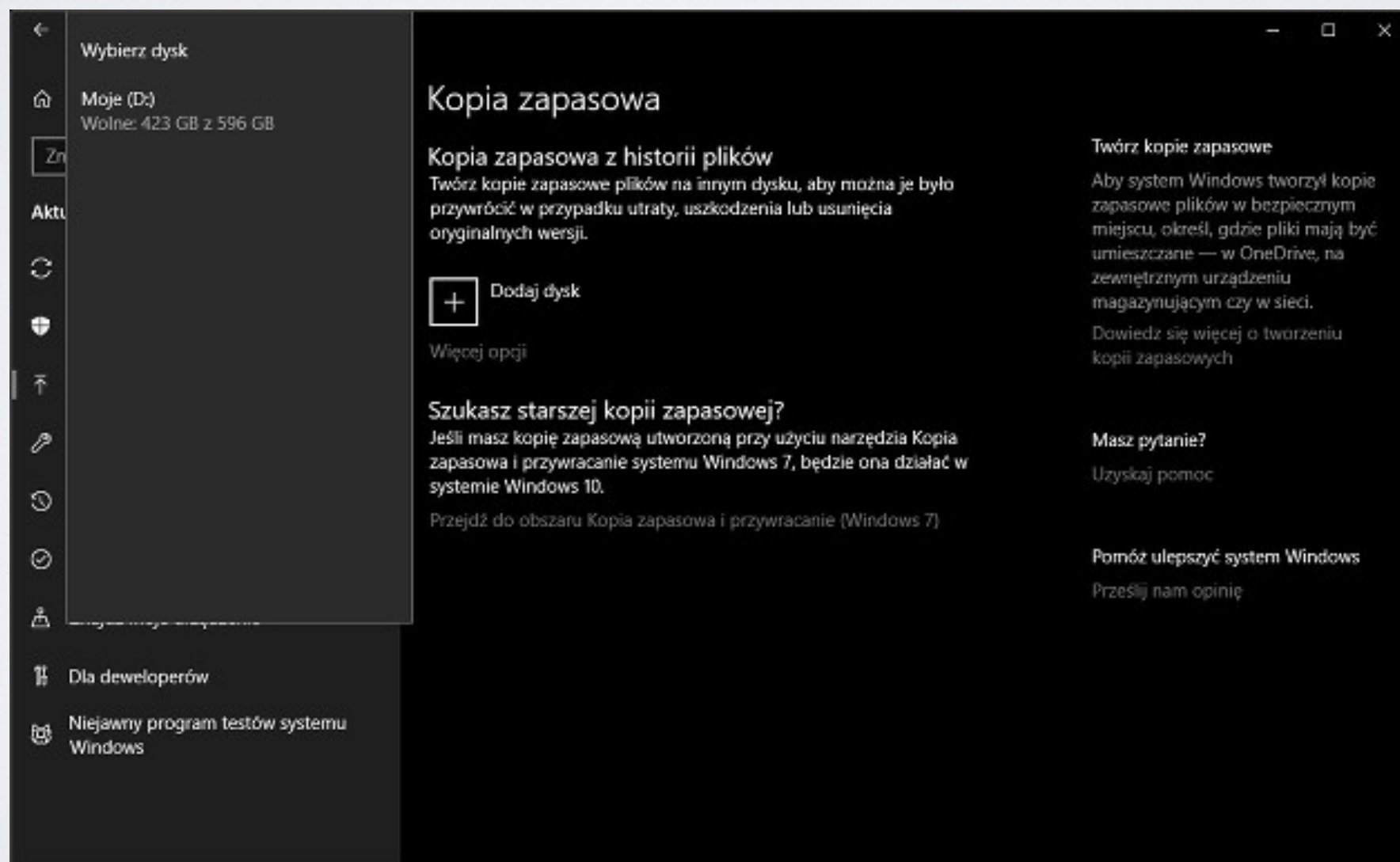
- SyncBack
- Acronis
- Bacula
- itd...

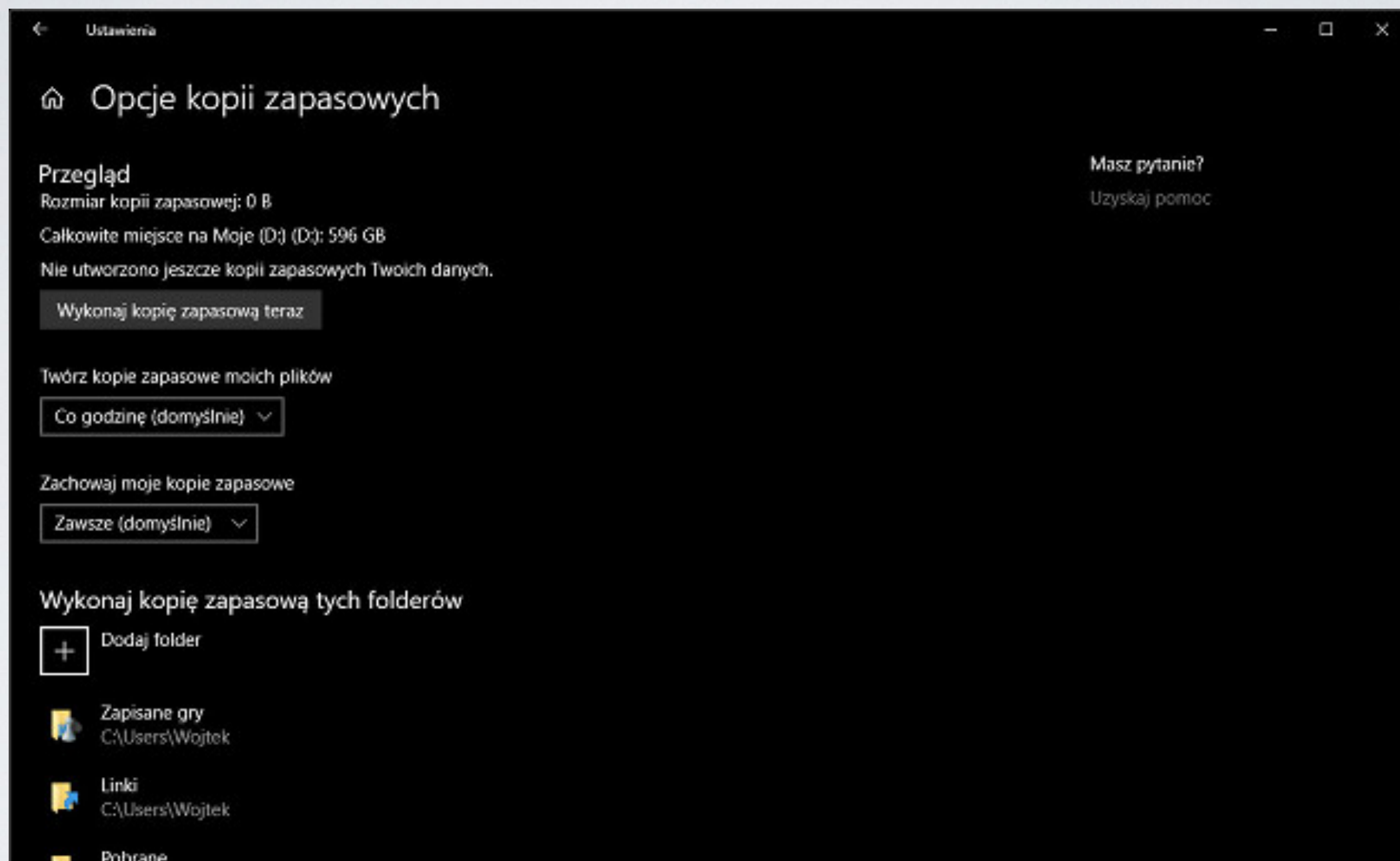
BACKUP ONLINE

- Dropbox
- OneDrive
- Google Drive
- Idrive
- Crashplan
- Mozy

NARZĘDZIE SYSTEMOWE WINDOWS 10

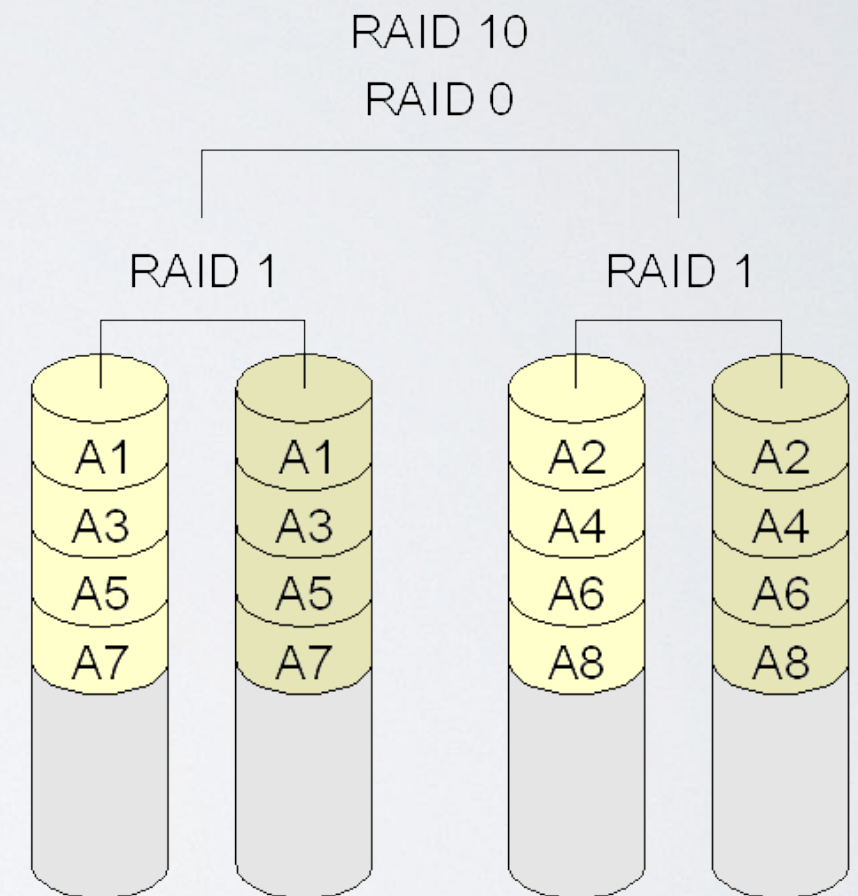
- Ustawienia - Aktualizacja i zabezpieczenia - Kopia zapasowa





RAID

- To nie kopia zapasowa!
- RAID 1 - dwa lustrzane dyski
- RAID 10
- RAID 0+1



SZYFROWANIE DYSKU

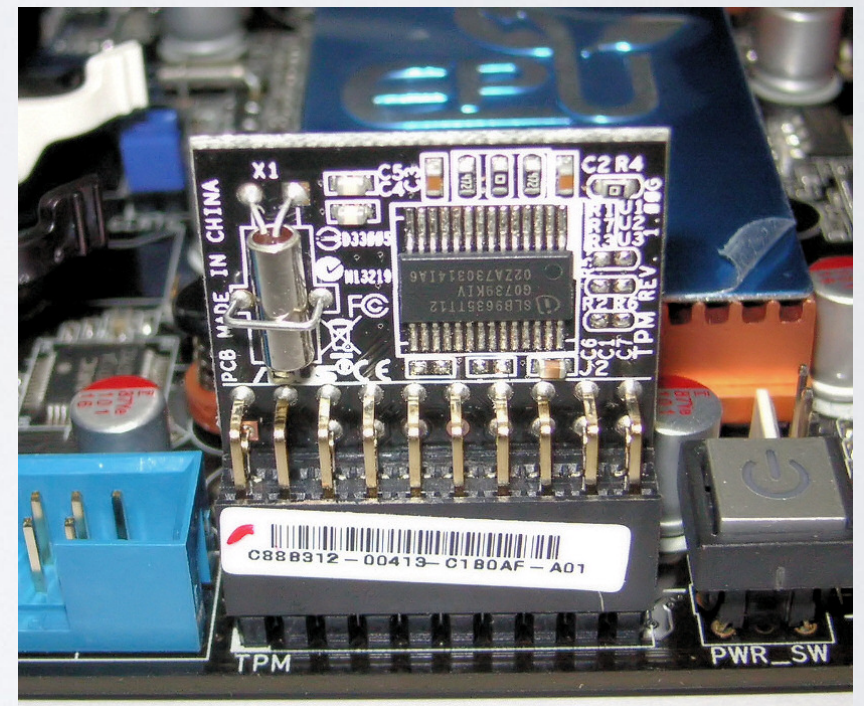
- Każdy bajt danych zostaje zaszyfrowany
- Niemożliwe jest odczytanie danych bez klucza
- Kradzież dysku bez klucza bezsensowna
- Np. Bitlocker, VeraCrypt, FileVault

BITLOCKER

- Wbudowany w Windows
- Klucz zapisany na innym dysku np. pamięć USB, wpisywany z klawiatury lub z użyciem modułu TPM
- Głównie szyfrowanie partycji systemowej
- Możliwe szyfrowanie innych partycji (ograniczone funkcje)

TPM

- Układ cyfrowy
- Może być wbudowany lub dołączany jako moduł do płyty głównej
- Funkcjonalności:
 - generowanie liczb pseudolosowych
 - generowanie podpisu cyfrowego dla ciągu bajtów
 - generowanie skrótów dla ciągu bajtów
 - szyfrowanie ciągu bajtów
 - generowanie skrótów dla sekwencji operacji wykonywanych przez procesor



ODZYSKIWANIE DANYCH

- Proces usuwania danych -> sektory w dysku oznaczane jako FREE, nie są zerowane (zbyt kosztowne)
- Możliwe odzyskanie danych, jeśli nie zostały nadpisane
- Im szybciej tym lepiej
- Specjalistyczne oprogramowanie np. Recuva

BIBLIOGRAFIA

- prof. dr hab. inż. Krzysztof Walkowiak, Bezpieczeństwo Sieci Komputerowych - slajdy do wykładu
- <https://sekurak.pl>
- <https://niebezpiecznik.pl>
- <https://www.chip.pl/2013/02/dane-na-wiecznosc-najtrwalsze-nosniki-na-swiecie/>
- <https://en.wikipedia.org/>
- <https://www.kei.pl/blog/cala-prawda-o-backupie/>
- <https://support.microsoft.com/pl-pl/>