

Hakerzy się nie włamują

Sebastian Jelinski

Senior Server Solutions Consultant
sebastian.jelinski@ibm.com

Rafał Owczarek

Infrastructure Platform Architect
rafal.owczarek@ibm.com

- Credentiale głównym paliwem ransomware
- 4,5 milarda wykradzionych credential w darknet
- Wzrost o 79% rok do roku

- + 389 % rok do roku – atakow ransomware
- 49 % ataków wykorzystuje dane do logowania

- Coraz mniej potrzebny malware



- Liczba grup atakujących wrozsla o ponad 50%
- AI przyspiesza ataki
- Hakerzy nie wymyslaja nowych metod



- Nowoczesne cyberataki coraz rzadziej zaczynają się od bezpośredniego ataku na firmę. Coraz częściej wykorzystują podatności, integracje i zaufane środowiska dostawców — a AI dramatycznie zwiększa szybkość całego procesu.

Polska stała się głównym celem cyberataków w Unii Europejskiej, a skala agresji może być największa na świecie. Gen. dyw. Karol Molenda, dowódca cyberwojsk, ujawnia porażające statystyki: 7 tysięcy obsłużonych incydentów rocznie i miliony prób phishingu.



Dowódca cyberwojsk: Liczba ataków na Polskę jedną z największych na świecie / East News



Polska stała się głównym celem cyberataków w Unii Europejskiej, a skala agresji może być największa na świecie. Gen. dyw. Karol Molenda, dowódca cyberwojsk, ujawnia porażające statystyki: 7 tysięcy obsłużonych incydentów rocznie i miliony prób phishingu.

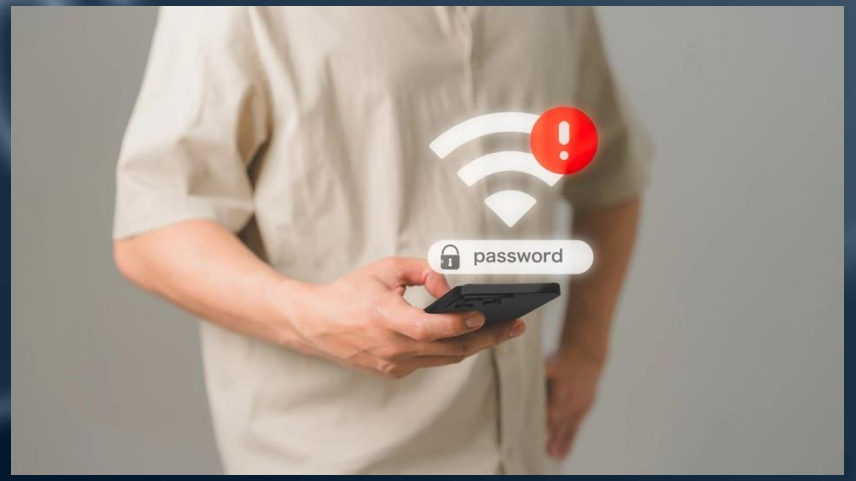


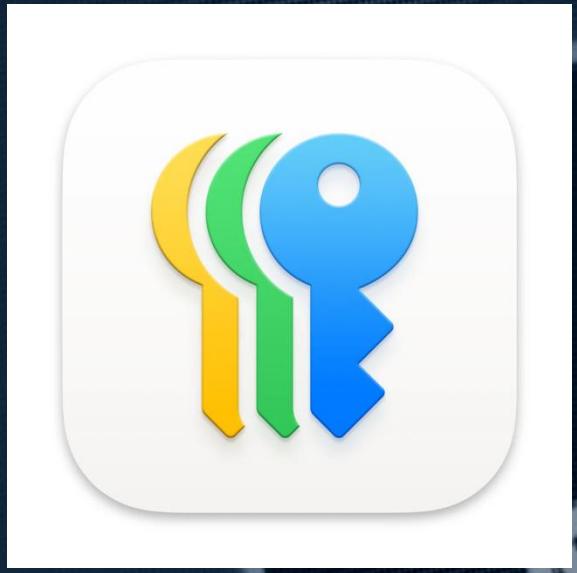
Dowódca cyberwojsk: Liczba atak[illegible] Polski jedną z największych na świecie / East News

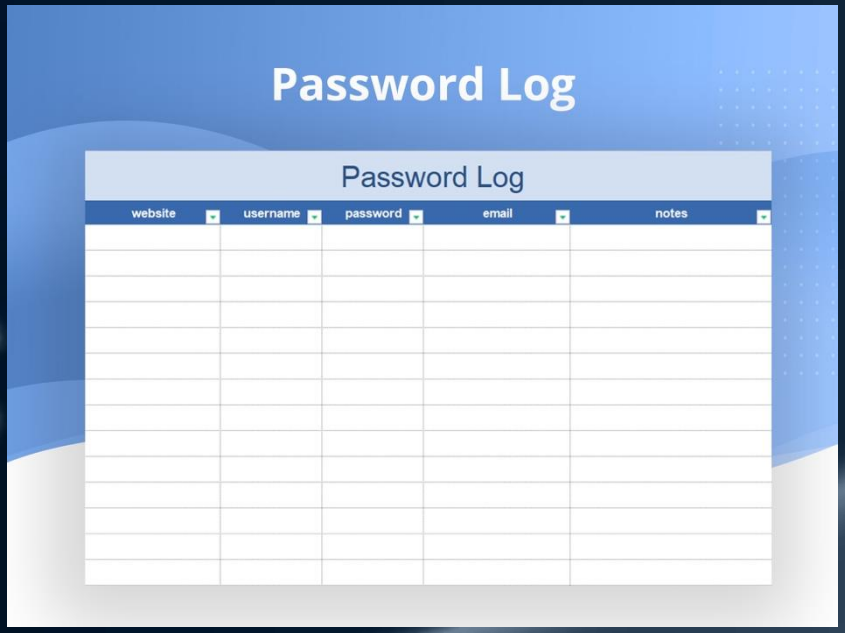


Polska najczęściej atakowanym krajem w UE


password
is
123456
shutterstock.com · 2644733931


password




Password Log
Password Log
website
username
password
email
notes

YOUR COMPANY IS LOSING PASSWORDS EVERY DAY

Weak habits. Human behavior. Massive risk.



HOW ATTACKERS GET IN



1. CREDENTIALS STOLEN

Through phishing, malware, breaches or dark web



2. SOLD & SHARED

Billions of stolen credentials traded on the dark web



3. USED TO ACCESS

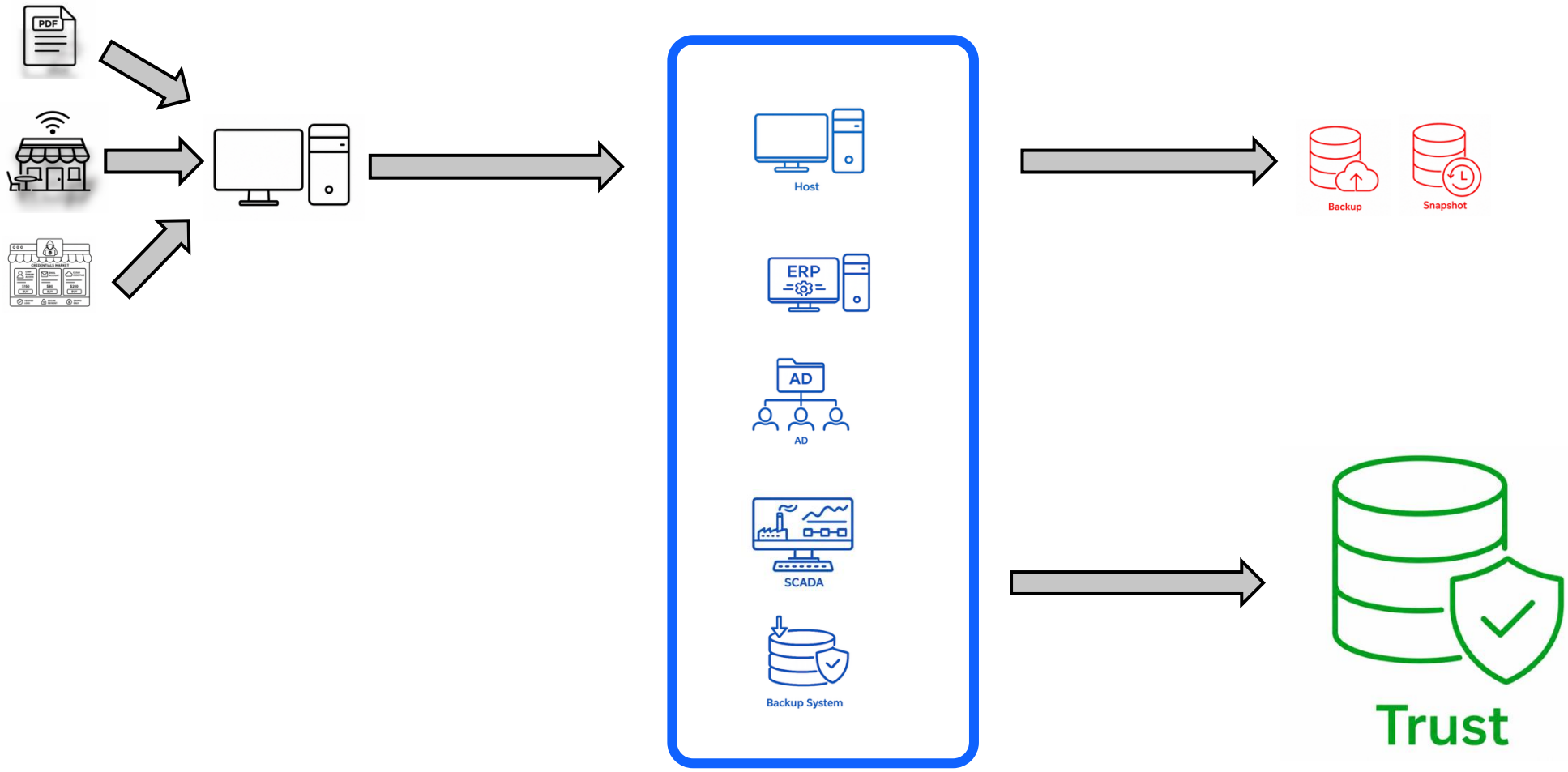
Attackers use valid credentials to log in as real users



4. DATA STOLEN

Access leads to data theft, ransomware, fraud and financial loss

Atak ransomware




FIRMA PO ATAKU
RANSOMWARE
BACKUP NIEDOSTĘPNY
SNAPSHOTY USUNIĘTE
DANE NIEDOSTĘPNE
CO SIĘ STAŁO?
DLACZEGO?
NIKT NIE WIE...
TWOJE DANE ZOSTAŁY SKRADZIONE
WSZYSTKIE TWOJE DANE ZOSTAŁY ZASZYFROWANE.
ABY JE ODZYSKAĆ ZAPŁAĆ OKUP:
10 000 000 USD
CZAS: 72:00:00
SYSTEM OFFLINE
NETWORK DOWN
NO DATA
ACCESS DENIED



The hack is likely to cost JLR hundreds of millions of pounds. Photograph: Simon Kirwan/Alamy

This article is r

Inside Rover factor cybersecurity and supply chain woes

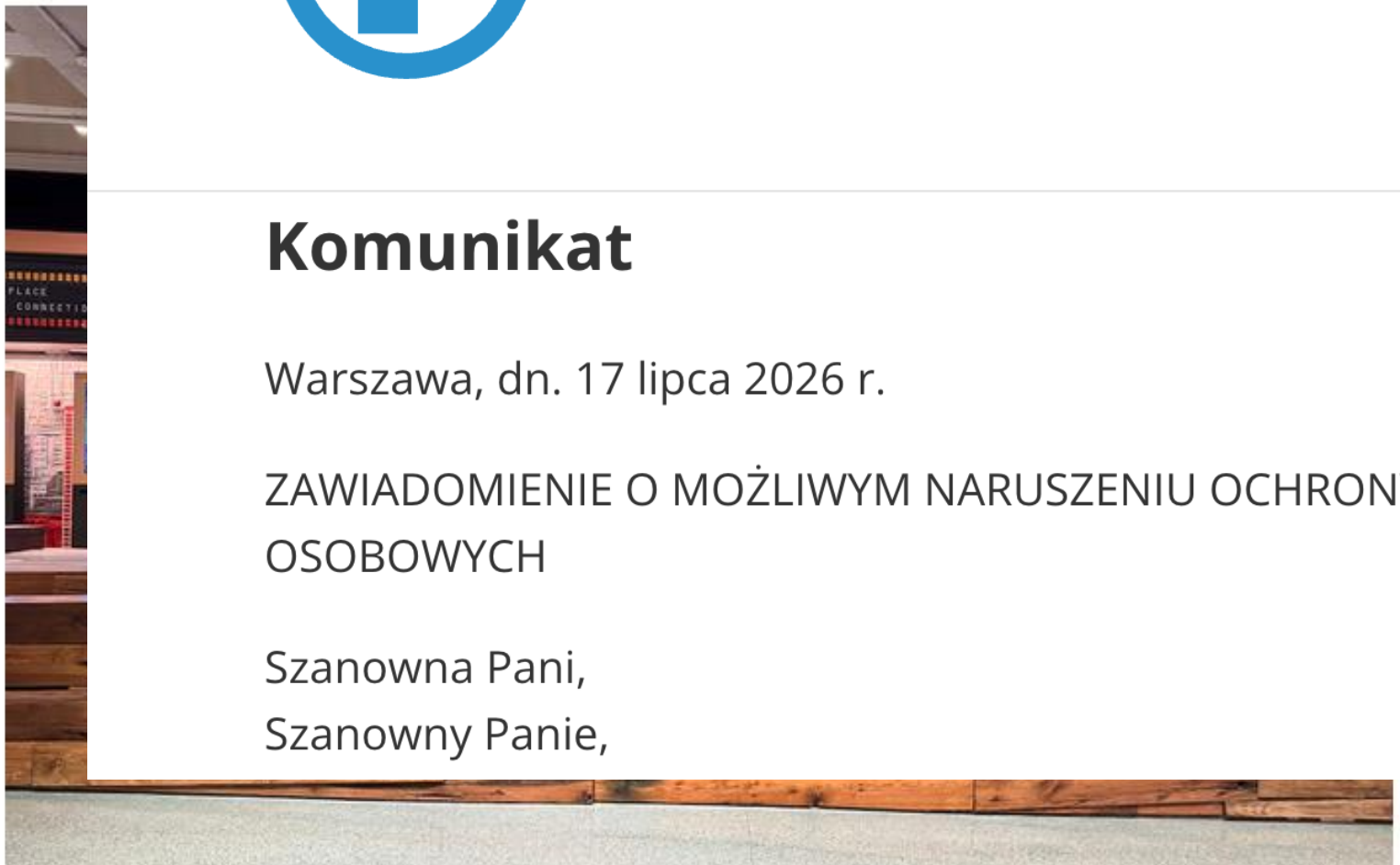
```
root@attacker:~# attack_chain

[10:24:15] Rozpoczynam analizę ścieżki ataku...

 [1] Jira
     [✓] Dostęp uzyskany (konto użytkownika)
     ↓
 [2] SSO
     [✓] Token SSO przejęty
     ↓
 [3] AD / IAM
     [✓] Dostęp do domeny / tożsamości
     ↓
 [4] VMware
     [✓] Dostęp do vCenter uzyskany
     ↓
 [5] Servers
     [✓] Serwery w sieci przejęte
     ↓
 [6] Backup
     [✓] Systemy backupu skompromitowane
     ↓
 [7] MES / ERP / OT
     [✓] Dostęp do systemów przemysłowych uzyskany

root@attacker:~#
```

NASK analizuje przypadki cyberataków z ostatnich tygodni na firmy

ShinyHunters hackers expanded attacks on

By Reu

Septem



Komunikat

Warszawa, dn. 17 lipca 2026 r.

ZAWIADOMIENIE O MOŻLIWYM NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Szanowna Pani,
Szanowny Panie,

01



Podmiana legalnego pliku wykonywalnego / instalacja backdoora

02



Uruchomienie nieautoryzowanego malware / ransomware

04



Reconnaissance / skanowanie hosta przed dalszym atakiem

03



Zmiana konfiguracji systemu po uzyskaniu dostępu

05



Modyfikacja krytycznych plików systemowych

Pełna izolacja:

- Wysokie mury
- Morskie pływy
- Ruchome piaski



LE MONT
SAINT MICHEL

POWER 11 is here



Cybersecurity with IBM Power: NIS-2 & DORA

Risk Management

- Full data encryption End-to End (RAM <->CPU)
- PowerVM: hardware virtualizator
- Automated isolation of resources
- Quantum-resistant cryptography



IBM Hardware
is certified by NATO

AIX

No ransomware detected

Business Continuity

- PowerHA for active/passive clusters
- VM Recovery Manager for active/inactive VMs
- Highest reliability on server market

Zero Trust Security

Encryption at every level

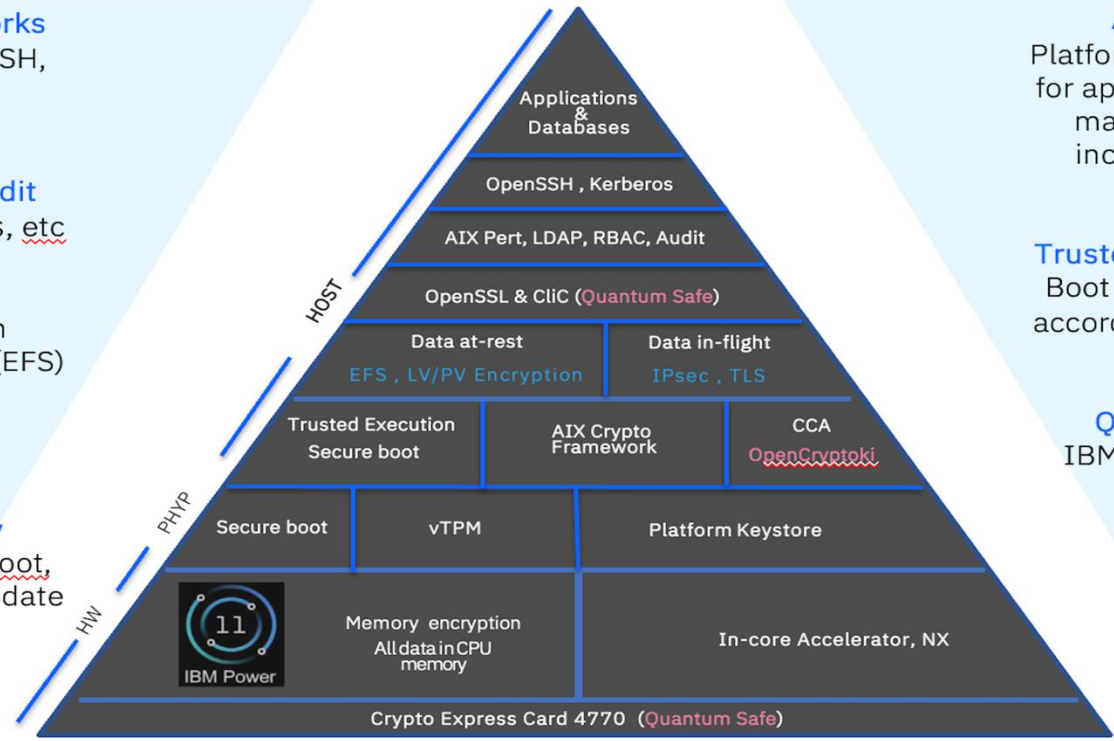
Application frameworks
OpenSSL/TLS, OpenSSH, Opencryptokey

Authentication, Authorizations & Audit
RBAC, LDAP, Kerberos, etc

Data at rest
PV & LV Encryption
Encrypted Filesystem (EFS)

Data in flight
IPsec, TLS

Platform Integrity
Secureboot, Trustedboot, trusted execution & update
Platform Keystore



Security with Power11

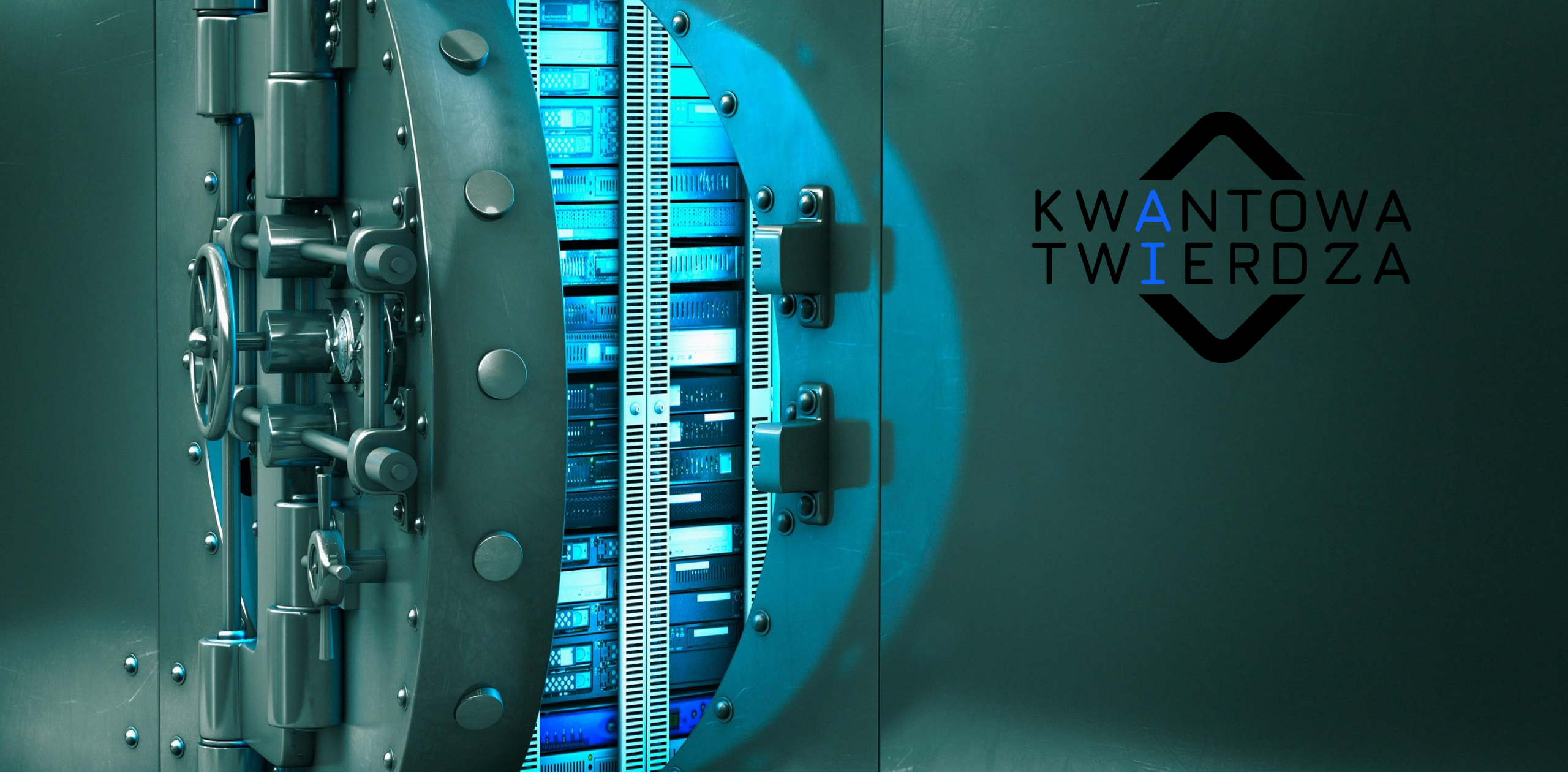
AIX Key Manager
Platform-level secure storage for application cryptographic materials such as keys, including key wrapping functionality.

Trusted Boot with vTPM 2.0
Boot integrity verification in accordance with the TPM 2.0 specification.

Quantum Safe HSM
IBM Crypto Express card (4770)

Cryptographic Acceleration

Unlock blazing fast cryptographic operations with built-in Power in-core accelerators.
Seamlessly optimized for OpenSSL to power your most demanding workloads with confidence
Deliver high throughput encryption for TLS, VPN (IPsec) and secure storage.



nie do zdobycia...

BADAŁEŚ SIĘ?

WKRÓTCE POZNACIE DIAGNOZĘ.

