URZĄD OCHRONY DANYCH OSOBOWYCH

ARCHITEKTURA ZAUFANIA W EPOCE AI:

OD CYBERHIGIENY DO ZERO TRUST

Urząd Ochrony Danych Osobowych
ul. Stanisława Moniuszki 1A, 00-014 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl

STAN OBECNY

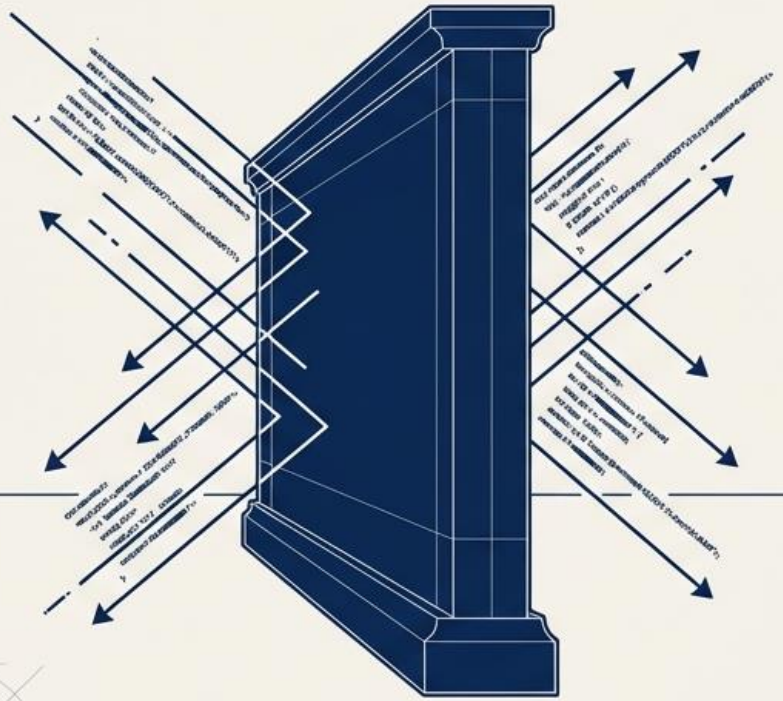
URZĄD OCHRONY DANYCH OSOBOWYCH

STAN OBECNY

URZĄD OCHRONY DANYCH OSOBOWYCH

Tradycyjne zapory sieciowe nie chronią już przed nowoczesnymi atakami

Stary paradygmat:
Atak na infrastrukturę IT

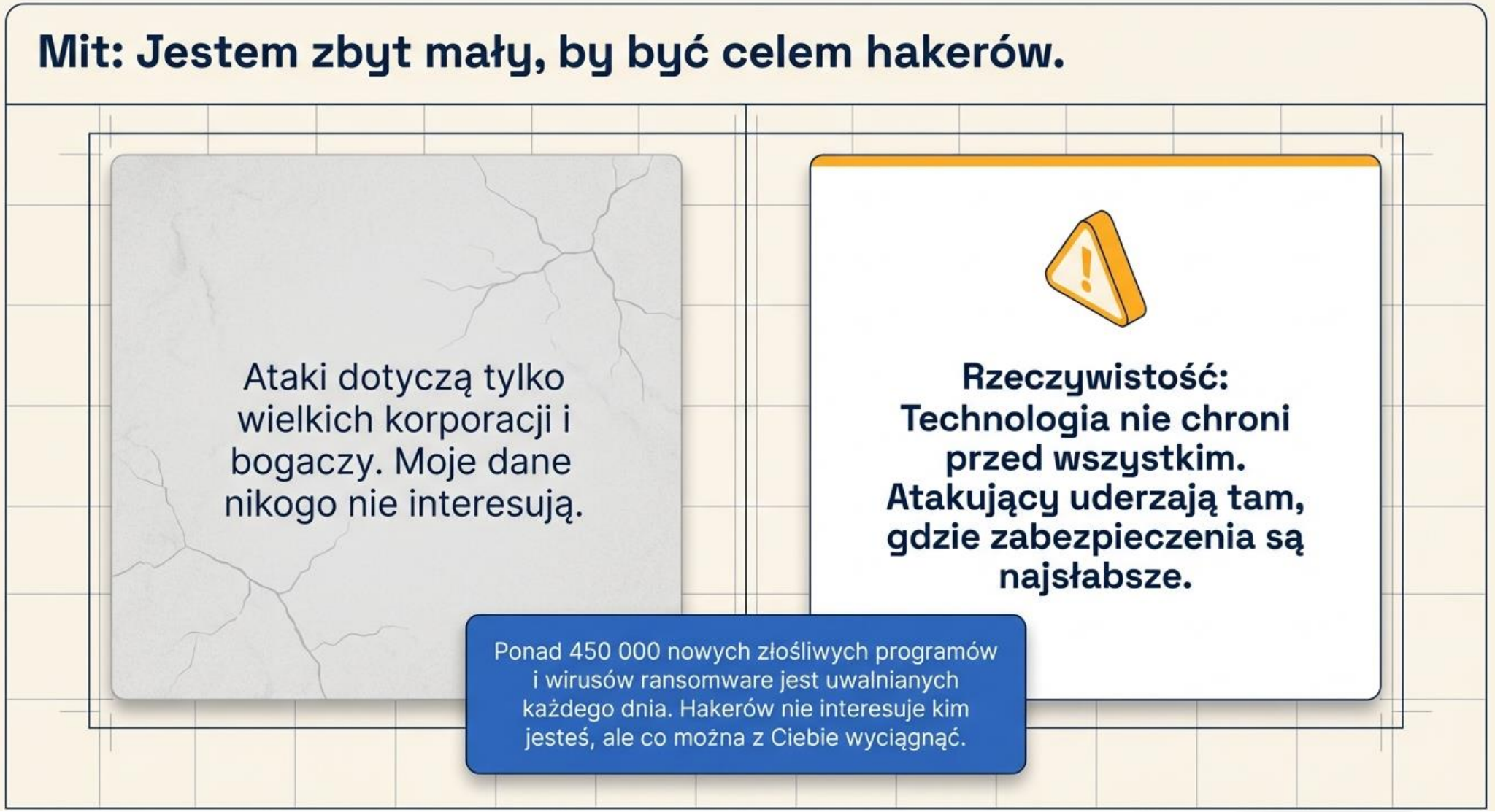


Nowa rzeczywistość:
Atak na ludzki umysł

Technologia to za mało, gdy cyberprzestępcy omijają zabezpieczenia, wykorzystując autorytet, strach i zaufanie. Złodzieje danych polują na dane finansowe, medyczne oraz dostęp do firmowych zasobów, traktując użytkownika jako punkt wejścia (Jump Point).

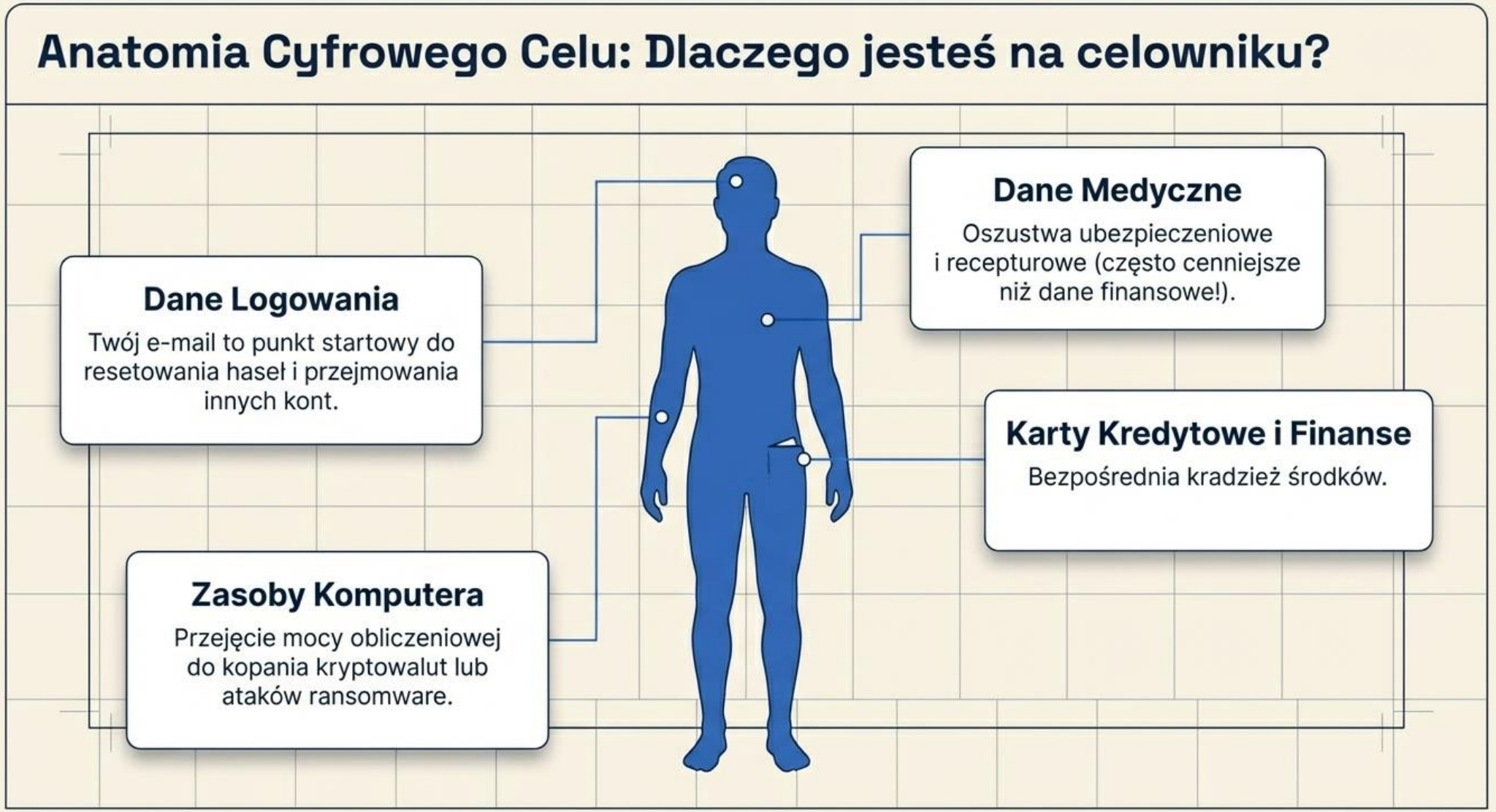
DLACZEGO NALEŻY ZASTANOWIĆ SIĘ, CO PUBLIKUJEMY W SIECI?

URZĄD OCHRONY DANYCH OSOBOWYCH



DLACZEGO NALEŻY ZASTANOWIĆ SIĘ, CO PUBLIKUJEMY W SIECI?

URZĄD OCHRONY DANYCH OSOBOWYCH



CZY BEZPŁATNE USŁUGI CYFROWE SĄ NA PEWNO DARMOWE?

URZĄD OCHRONY DANYCH OSOBOWYCH

4,025 mld PLN wyniosła wartość danych polskich użytkowników dla Google'a, a 2,196 mld PLN wartość danych z Polski dla Facebooka (dane z 2020 r.)

Miesięczny przychód z danych pojedynczego polskiego użytkownika dla Google wynosi 10,16 PLN

Miesięczny przychód z danych polskiego użytkownika dla Facebooka wynosi 8,52 PLN

Kluczowe liczby:

- 87% badanych twierdzi, że firmy technologiczne wiedzą o nas za dużo
- 84% badanych uważa, że działalność firm technologicznych powinna podlegać większej kontroli
- 81% badanych nie jest obojętne, co firmy technologiczne robią z ich danymi
- 14,10 PLN miesięcznie jesteśmy skłonni płacić za brak dostępu Google'a do naszych danych, w tym aktywności na innych portalach
- 17,07 PLN miesięcznie jest skłonny płacić przeciętny Polak za to, aby Facebook nie miał dostępu do danych agregowanych na platformie oraz pochodzących z innych źródeł

Źródło: *Ile warte są nasze dane?* Polski Instytut Ekonomiczny, Warszawa 2021, ISBN 978-83-66698-57-4

DLACZEGO NALEŻY ZASTANOWIĆ SIĘ, CO PUBLIKUJEMY W SIECI?

URZĄD OCHRONY DANYCH OSOBOWYCH

Źródło: https://picarta.pl/

Open Source Intelligence (OSINT) w celu kradzieży tożsamości

- OSINT to w najprostszym ujęciu pozyskiwanie i analizowanie rozmaitych informacji z legalnych źródeł otwartych lub półotwartych
- Każda udostępniona przez nas w mediach społecznościowych informacja może zostać pozyskana przez osoby, które poszukują informacji (infobrokerów)

DLACZEGO NALEŻY ZASTANOWIĆ SIĘ, CO PUBLIKUJEMY W SIECI?

URZĄD OCHRONY DANYCH OSOBOWYCH

Źródło: https://picarta.pl/

Open Source Intelligence (OSINT) w celu kradzieży tożsamości

- Każda udostępniona przez nas w mediach społecznościowych informacja może zostać poddana analizie
- Analizując te dane, można uzyskać kluczowe informacje, takie jak imię i nazwisko, data urodzenia, miejsce zamieszkania, a nawet szczegóły z życia prywatnego (imiona osób najbliższych, zwierzaka)

(RE)EWOLUCJA ZAGROŻEŃ

URZĄD OCHRONY DANYCH OSOBOWYCH

Inżynieria społeczna wspomagana przez AI zmienia ekonomię cyberprzestępczości

Faza 1: Tradycyjny Phishing

Masowe, tekstowe próby wyłudzenia haseł. Łatwe do wykrycia przez filtry i czujnych użytkowników.

Faza 2: Deepfake Audio/Wideo

Autonomiczne boty, polimorficzne złośliwe oprogramowanie i deepfake'i generowane w czasie rzeczywistym.

Anatomia ataku AI: Atakujący wykorzystują sieci GAN (Generative Adversarial Networks) do klonowania głosu, twarzy i stylu pisania. Celują bezpośrednio w psychologiczną podatność na autorytet.

(RE)EWOLUCJA ZAGROŻEŃ

URZĄD OCHRONY DANYCH OSOBOWYCH

Oszustwo na prezesa (CEO Fraud) z użyciem sklonowanego głosu

1. Cyberprzestępcy generują Deepfake Audio

2. Telefon do pracownika naśladujący głos CEO

3. Ominięcie procedur przez presję autorytetu

4. Natychmiastowy transfer środków

Wektor ataku: Użycie dźwięku wygenerowanego przez AI, aby z przerażającą dokładnością naśladować głos dyrektora.

Mechanizm psychologiczny: Pracownik bezwzględnie zaufał poleceniu przełożonego, omijając weryfikację.

Przypadek z życia: Brytyjska firma energetyczna straciła w ten sposób ponad 200 000 dolarów.

URZĄD OCHRONY DANYCH OSOBOWYCH

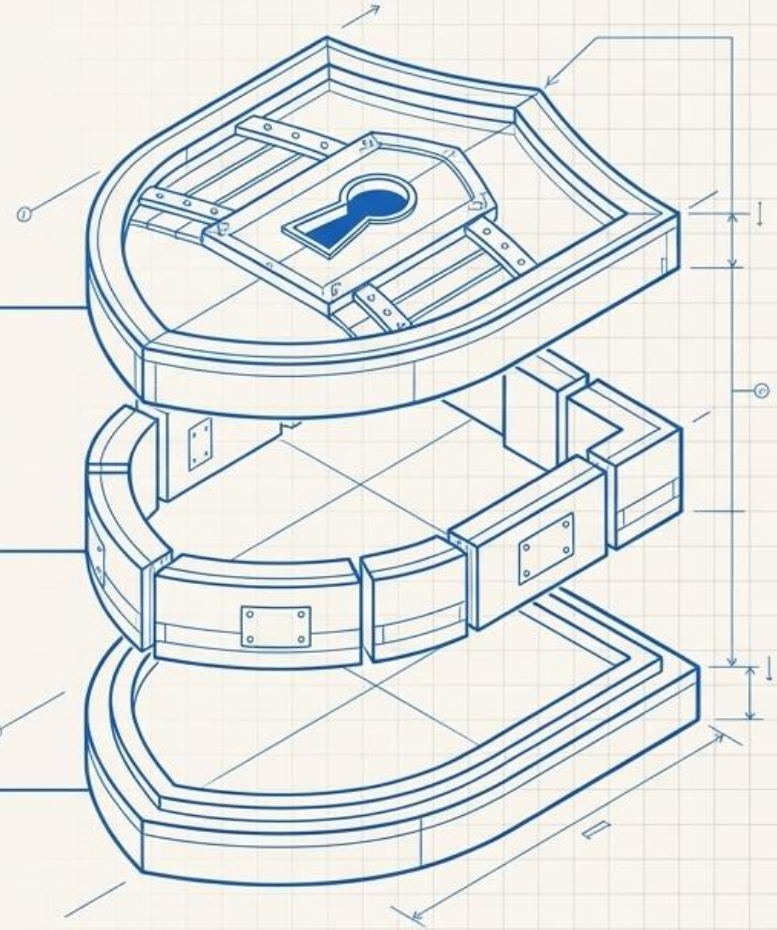
Architektura Twojej Obrony

Bezpieczeństwo to nie jeden magiczny program, to system warstwowy. **Zbudujemy Twoją ochronę krok po kroku.**

Bramy i Klucze: Hasła (Kontrola dostępu)

Mury: Aktualizacje (Łatanie podatności)

Fundament: Kopie Zapasowe (Ostatnia deska ratunku)



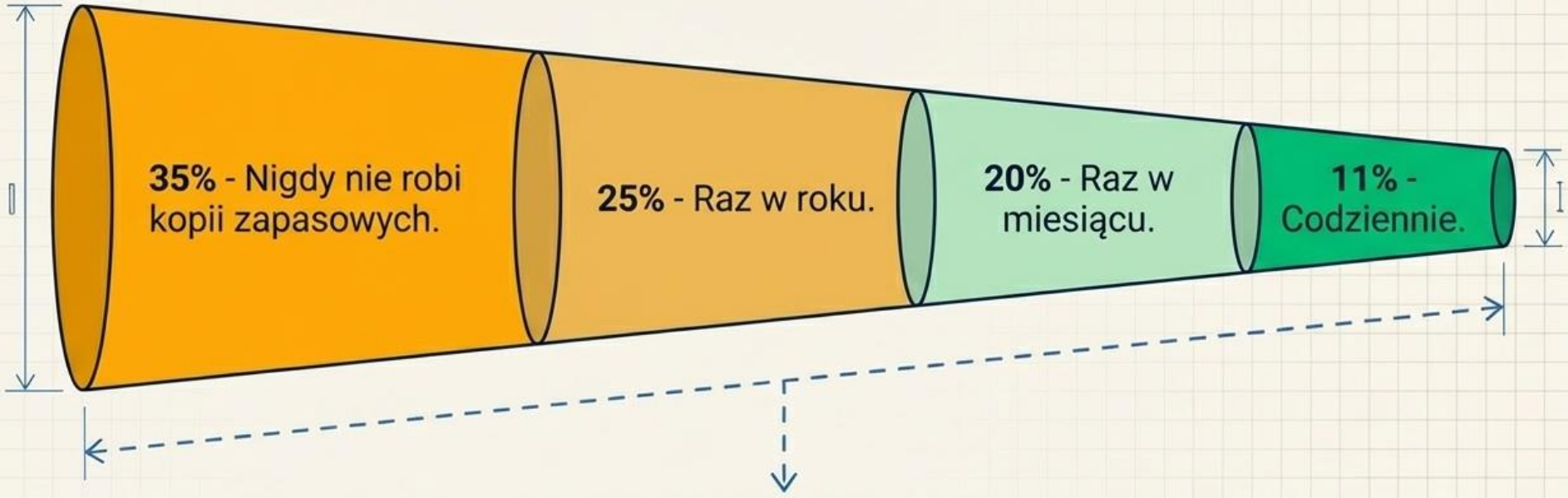
URZĄD OCHRONY DANYCH OSOBOWYCH

Warstwa 1: Fundament (Kopie Zapasowe)

- Kopie zapasowe chronią, gdy zawiedzie wszystko inne.
- To jedyna gwarantowana ochrona przed oprogramowaniem wymuszającym okup (Ransomware).
- **Złota zasada**: Nośniki kopii zapasowych nie powinny być podłączone do komputera przez cały czas.
- **Najważniejsze**: Testuj swoje kopie! Próbuj je odtworzyć, zanim wydarzy się awaria.

URZĄD OCHRONY DANYCH OSOBOWYCH

Lejek Ryzyka: Jak często robisz kopie zapasowe?



W której grupie jesteś? Twoje dane (zdjęcia, dokumenty, finanse) istnieją tylko do momentu **pierwszej awarii** dysku lub ataku hakerskiego.

URZĄD OCHRONY DANYCH OSOBOWYCH

Warstwa 2: Mury Obronne (Aktualizacje)

- To, co było bezpieczne wczoraj, może nie być bezpieczne dzisiaj.
- Każdego dnia odkrywane są nowe luki w oprogramowaniu.
- W cyfrowym świecie nie istnieje zasada Zainstaluj i zapomnij.
- Aktualizuj systemy i programy antywirusowe do najnowszych definicji, aby zapewnić ochronę przed najnowszymi zagrożeniami.

URZĄD OCHRONY DANYCH OSOBOWYCH

Ekosystem Podatności: Pamiętaj o wszystkim!

URZĄD OCHRONY DANYCH OSOBOWYCH

Warstwa 3: Bramy i Klucze (Hasła)

“Ktoś odgadł moje hasło, teraz muszę zmienić imię psa.”

Unikaj używania informacji, które można z Tobą powiązać: adresów, numerów telefonów czy imion zwierząt.

DLACZEGO NALEŻY STOSOWAĆ SILNE HASŁA I UWIERZYTELNIANIE MFA?

URZĄD OCHRONY DANYCH OSOBOWYCH

Długość > Skomplikowanie (Czas na złamanie hasła)

Złe Hasło (8 znaków)

P@ssw0rd

Czas złamania: Sekundy

Świetne Hasło (31 znaków)

Mojsynurodzilsiewlistopadzie1995!

Czas złamania: Stulecia

Używaj minimum 12 znaków, ale 15 i więcej to znacznie lepszy standard.

Unikaj najpopularniejszych haseł roku: 123456, password, qwerty, 111111.

DLACZEGO NALEŻY STOSOWAĆ SILNE HASŁA I UWIERZYTELNIANIE MFA?

URZĄD OCHRONY DANYCH OSOBOWYCH

Przydatne wskazówki:

- hasło nie powinno być takie samo jak nazwa użytkownika lub część tej nazwy
- hasło nie powinno być imieniem nikogo z naszego najbliższego otoczenia (członka rodziny, znajomego ani zwierzaka)
- hasło nie powinno zawierać danych osobowych Twoich lub Twojej rodziny. Mowa tu o informacjach, które łatwo zdobyć, takie jak data urodzenia, numer telefonu, numer rejestracyjny samochodu, nazwa ulicy, numer mieszkania/domu itd.
- nie używaj sekwencji kolejnych liter, liczb lub innych znaków. Na przykład: abcd, 1234, QWERTY
- nie używaj pojedynczego wyrazu dowolnego języka pisanego normalnie lub wspak, ani tego wyrazu poprzedzonego lub zakończonego znakiem specjalnym lub cyfrą
- nie używaj więcej niż 3 kolejnych znaków na klawiaturze (takie jak abc lub 123)
- nie używaj więcej niż dwóch kolejno powtarzających się ciągów znaków (bbbb2bbb)

* możesz sprawdzić czy Twoje hasło nie zostało ujawnione (https://haveibeenpwned.com/Passwords)

DLACZEGO NALEŻY STOSOWAĆ SILNE HASŁA I UWIERZYTELNIANIE MFA?

URZĄD OCHRONY DANYCH OSOBOWYCH

Time It Takes Using AI to Crack Your Password [2023]

# OF CHARACTER	Numbers Only	Lowercase Letters	Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	4 Seconds
7	Instantly	Instantly	22 Seconds	42 Seconds	6 Minutes
8	Instantly	3 Seconds	19 Minutes	48 Minutes	7 Hours
9	Instantly	1 Minutes	11 Hours	2 Days	2 Weeks
10	Instantly	1 Hours	4 Weeks	6 Months	5 Years
11	Instantly	23 Hours	4 Years	38 Years	356 Years
12	25 Seconds	3 Weeks	289 Years	2K Years	30K Years
13	3 Minutes	11 Months	16K Years	91K Years	2M Years
14	36 Minutes	49 Years	827K Years	9M Years	187M Years
15	5 Hours	890 Years	47M Years	613M Years	14Bn Years
16	2 Days	23K Years	2Bn Years	26Bn Years	1Tn Years
17	3 Weeks	812K Years	539.72M Years	2Tn Years	95Tn Years
18	10 Months	22M Years	7.23Bn Years	96Tn Years	6Qn Years

DLACZEGO NALEŻY STOSOWAĆ SILNE HASŁA I UWIERZYTELNIANIE MFA?

URZĄD OCHRONY DANYCH OSOBOWYCH

Macierz Strategii Haseł

Wygoda

Bezpieczeństwo

Karteczki samoprzylepne.

Ostrzeżenie: Nie przechowuj haseł otwartym tekstem!

Menedżer Haseł (Twój Cyfrowy Sejf)

To samo hasło wszędzie.

Używane przez 52% osób. Jeden wyciek niszczy całe Twoje życie.

Wiele skomplikowanych haseł z pamięci.

Niemożliwe do utrzymania w dłuższej perspektywie.

DLACZEGO NALEŻY STOSOWAĆ SILNE HASŁA I UWIERZYTELNIANIE MFA?

URZĄD OCHRONY DANYCH OSOBOWYCH

Uwierzytelnianie wieloskładnikowe (MFA) jako fundament weryfikacji tożsamości

Dlaczego hasła to za mało?

Nawet najbardziej skomplikowane hasło może zostać wykradzione, wyłudzone (phishing) lub odgadnięte.

Definicja MFA

Bezpieczny proces logowania wymagający co najmniej dwóch niezależnych dodowodów tożsamości z różnych kategorii.

Rola w architekturze

MFA jest krytycznym elementem modelu Zero Trust oraz podstawowym wymogiem zgodności z nowoczesnymi regulacjami (w tym z NIS2 i RODO).

DLACZEGO NALEŻY STOSOWAĆ SILNE HASŁA I UWIERZYTELNIANIE MFA?

URZĄD OCHRONY DANYCH OSOBOWYCH

Trzy kategorie składników uwierzytelniania

Coś, co znasz (Wiedza)

Haslo lub kod PIN. Najslabsze ogniwo, jeśli stosowane samodzielnie.

Coś, co posiadasz (Posiadanie)

Fizyczny token (np. klucz YubiKey), aplikacja w telefonie, Smart Card.

Coś, czym jesteś (Cechy fizyczne)

Dane biometryczne: odcisk palca, skan twarzy. Najtrudniejsze do podrobienia.

DLACZEGO NALEŻY STOSOWAĆ SILNE HASŁA I UWIERZYTELNIANIE MFA?

URZĄD OCHRONY DANYCH OSOBOWYCH

Różnica między logowaniem dwuetapowym a prawdziwym MFA

Tylko hasło	Składnik wiedzy.	Ochrona bardzo słaba ❌
Hasło + Pytanie pomocnicze	Składnik wiedzy + Składnik wiedzy.	To uwierzytelnianie 2-etapowe, ale NIE 2-składnikowe. Ochrona słaba ❌
Hasło + Kod SMS	Składnik wiedzy + Składnik posiadania.	Prawdziwe 2FA, ale podatne na zaawansowany phishing i przechwycenie SMS ⚠️
Hasło + Klucz sprzętowy/Biometria	Składnik wiedzy + Składnik posiadania/Cechy fizyczne.	Silne, oporne na phishing uwierzytelnianie wieloskładnikowe ☑️

URZĄD OCHRONY DANYCH OSOBOWYCH

Cyberhigiena: Człowiek jako ostatnia linia obrony

Zasada ograniczonego zaufania

Twoja wiedza i nawyki to najlepsza ochrona przed oszustwami, których nie wyłapią systemy IT.

Oddzielenie sfer (Church & State)

Rygorystyczny podział. Prywatne konta i urządzenia służą wyłącznie celom prywatnym. Sprzęt służbowy wyłącznie do pracy.

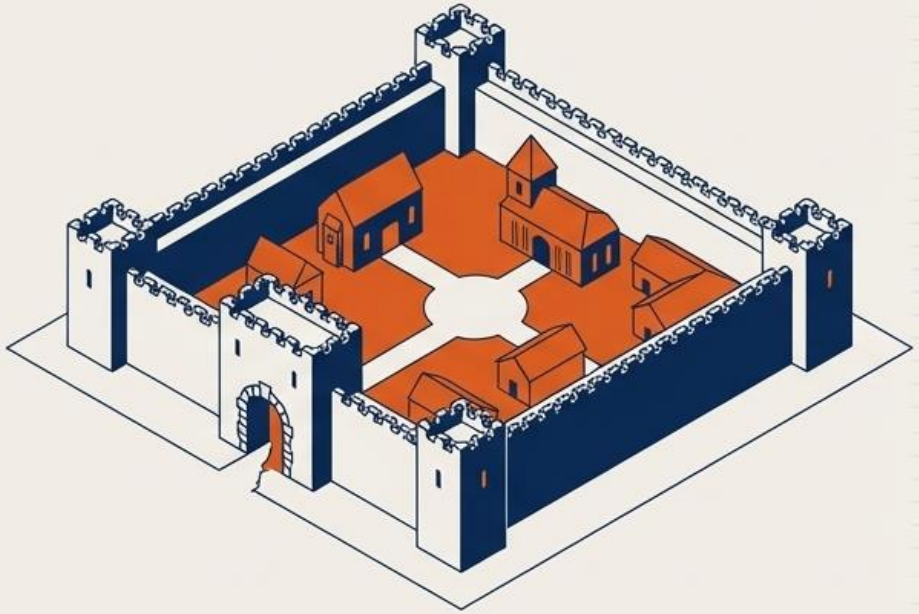
Bezwzględne Aktualizacje

Nie odkładaj instalacji łat bezpieczeństwa. Systemy takie jak Windows, macOS, czy oprogramowanie antywirusowe muszą być natychmiast aktualizowane.

URZĄD OCHRONY DANYCH OSOBOWYCH

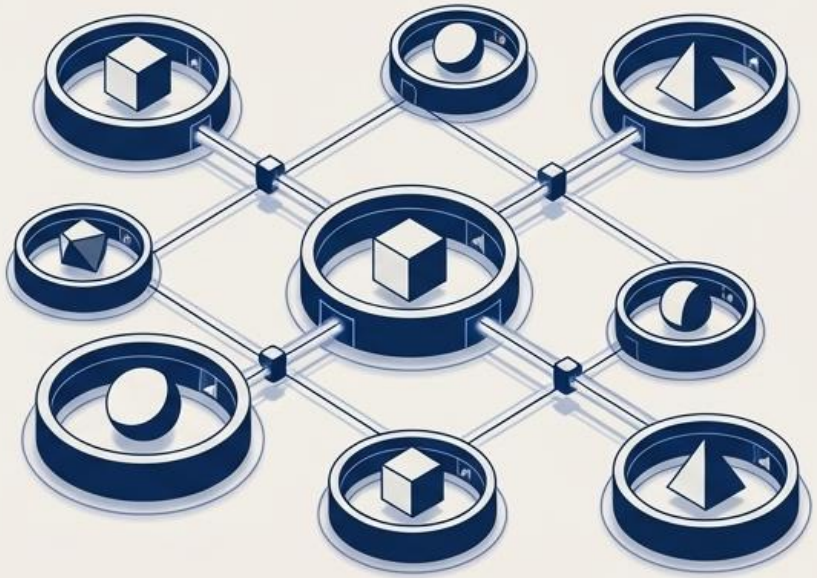
Zmiana paradygmatu: Koniec modelu Zamek i Fosa

Stary Model (Zaufanie domyślne)



Zakłada, że każdemu i wszystkiemu wewnątrz sieci firmowej można ufać. Przełamanie jednego hasła daje dostęp do wszystkiego.

Nowy Model (Architektura Zero Trust)

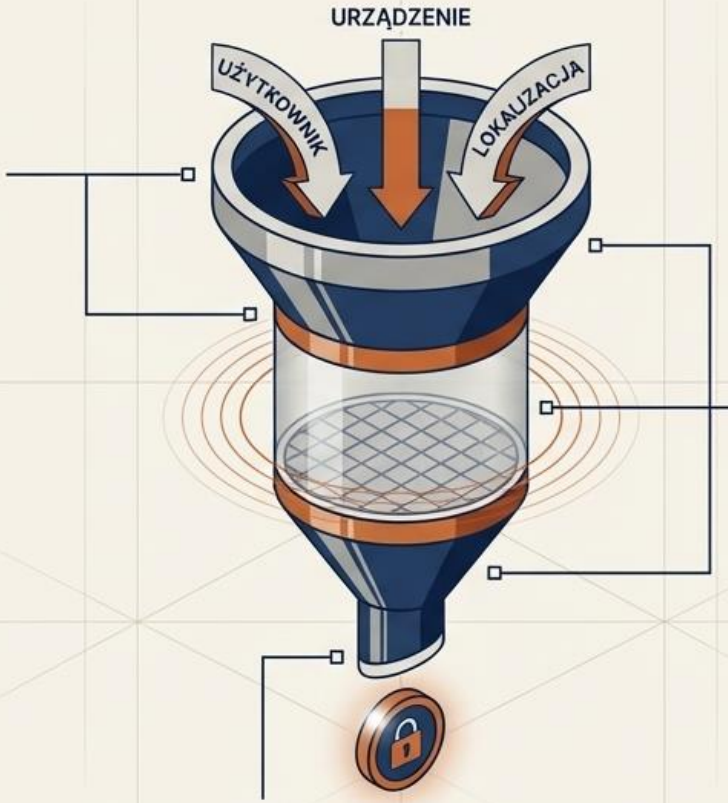


Nigdy nie ufaj, zawsze weryfikuj. Traktuje każdą próbę dostępu tak, jakby pochodziła z otwartej, niezabezpieczonej sieci. Zaufanie musi być nieustannie weryfikowane.

URZĄD OCHRONY DANYCH OSOBOWYCH

Dynamiczna weryfikacja w czasie rzeczywistym

Wejście (Analiza Kontekstu):
Kim jest użytkownik?
Z jakiego urządzenia się łączy?
Jaka jest jego lokalizacja?



Filtracja (Weryfikacja Ciągła):
Szyfrowanie end-to-end, analiza anomalii w zachowaniu sieciowym.

Wyjście (Mikrodostęp):
Selektywny dostęp wyłącznie do autoryzowanych danych i aplikacji, zabezpieczający pracę zdalną i modele BYOD.

URZĄD OCHRONY DANYCH OSOBOWYCH

Udostępnianie informacji

Ogranicz widoczność swoich kont i zastanów się co publikujesz:

- aby jak najlepiej chronić swoją prywatność, warto ograniczyć widoczność informacji powiązanych z kontem
- ważne jest, aby grono odbiorców Twojego konta składało się tylko z osób, które znasz
- przed zaakceptowaniem zaproszenia w social mediach, dokładnie zweryfikuj profil osoby, która je wysłała. Zwróć uwagę na datę założenia konta oraz publikowane treści. Dzięki temu informacje, którymi dzielisz się na swoim profilu, będą dostępne wyłącznie dla zaufanej grupy osób

CZŁOWIEK W ŚWIECIE WSPÓŁCZESNYCH CYBERZAGROŻEŃ - DOBRE PRAKTYKI I WSKAZÓWKI

URZĄD OCHRONY DANYCH OSOBOWYCH

Zadbaj o swoją infrastrukturę sieciową

- Włącz segmentację sieci (VLAN)
- Nie podłączaj do sieci (zwłaszcza Wi-Fi) nieznanych urządzeń
- Włącz zaporę sieciową (Firewall)
- Używaj wieloskładnikowego uwierzytelniania (MFA)
- Wykonuj inwentaryzację zasobów sieciowych

CZŁOWIEK W ŚWIECIE WSPÓŁCZESNYCH CYBERZAGROŻEŃ - DOBRE PRAKTYKI I WSKAZÓWKI

URZĄD OCHRONY DANYCH OSOBOWYCH

Zadbaj o swoją infrastrukturę sieciową

- Stosuj polityki haseł oparte na aktualnych standardach
- Zmień standardowe hasło administratora, wyłącz konto gościa (guest)
- Wyłącz dostęp ssh i telnet, jeżeli z nich nie korzystasz
- Uczestnicz w symulowanych atakach phishingowych
- Wykonuj testy penetracyjne przynajmniej raz w roku

CZŁOWIEK W ŚWIECIE WSPÓŁCZESNYCH CYBERZAGROŻEŃ - DOBRE PRAKTYKI I WSKAZÓWKI

URZĄD OCHRONY DANYCH OSOBOWYCH

Ogólne zasady bezpieczeństwa w sieci

- Używaj aktualnego oprogramowania antywirusowego
- Wykonuj kopie zapasowe danych (i cyklicznie sprawdzaj, czy da się z nich odtworzyć dane!). Co najmniej jedna kopia powinna być przechowywana offline
- Aktualizuj aplikacje (po uprzednim wykonaniu kopii zapasowej danych i zapoznaniu się z rejestrem zmian - przeanalizuj ewentualne ujawnione błędy, jakie mogą wystąpić nowej wersji)
- Unikaj otwierania w poczcie elektronicznej załączników z nieznanych źródeł

URZĄD OCHRONY DANYCH OSOBOWYCH

Synteza: Twój Ekosystem Przetrwania

URZĄD OCHRONY DANYCH OSOBOWYCH

Przejmij Kontrolę: Twoje 3 Zadania na Dziś

ON

Ustaw Automatyczną Kopię Zapasową

W chmurze lub na dysku zewnętrznym - i odłącz go po użyciu!

ON

Włącz Automatyczne Aktualizacje

Na telefonie, komputerze i domowym routerze.

ON

Zainstaluj Menedżera Haseł

I przestań wymyślać hasła samodzielnie.

URZĄD OCHRONY DANYCH OSOBOWYCH

DZIĘKUJĘ ZA UWAGĘ!

Urząd Ochrony Danych Osobowych
ul. Stanisława Moniuszki 1A, 00-014 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl