Cyber Women Community

Trendy technologiczne i ich wpływ na cyberbezpieczeństwo, czyli co nas czeka w najbliższym czasie

Mariola Więckowska

Head of Privacy Innovative Technologies

LexDigital Sp. z o. o.

LexDigital

Message in a bottle

Gartner: Trendy technologiczne w 2022

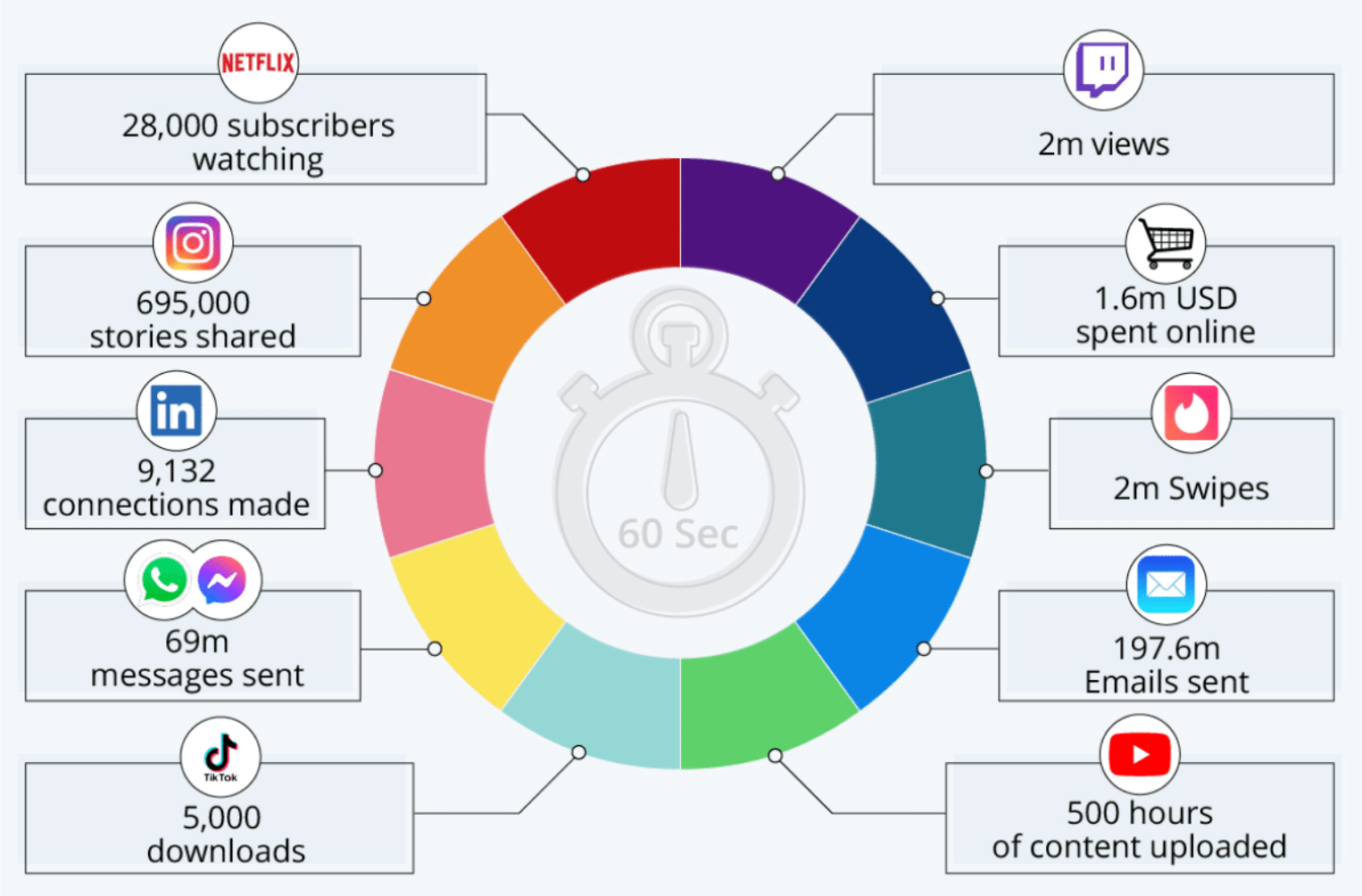
i 2023 vs. nowe trendy w cyberbezpieczeństwie

Privacy Enhancing Technologies (PETs) i ich wpływ na bezpieczeństwo przetrwania danych

Rejestry rozproszone oraz blockchain w kontekście bezpieczeństwa i cyberzagrożeń

1 minuta w internecie w 2021 roku

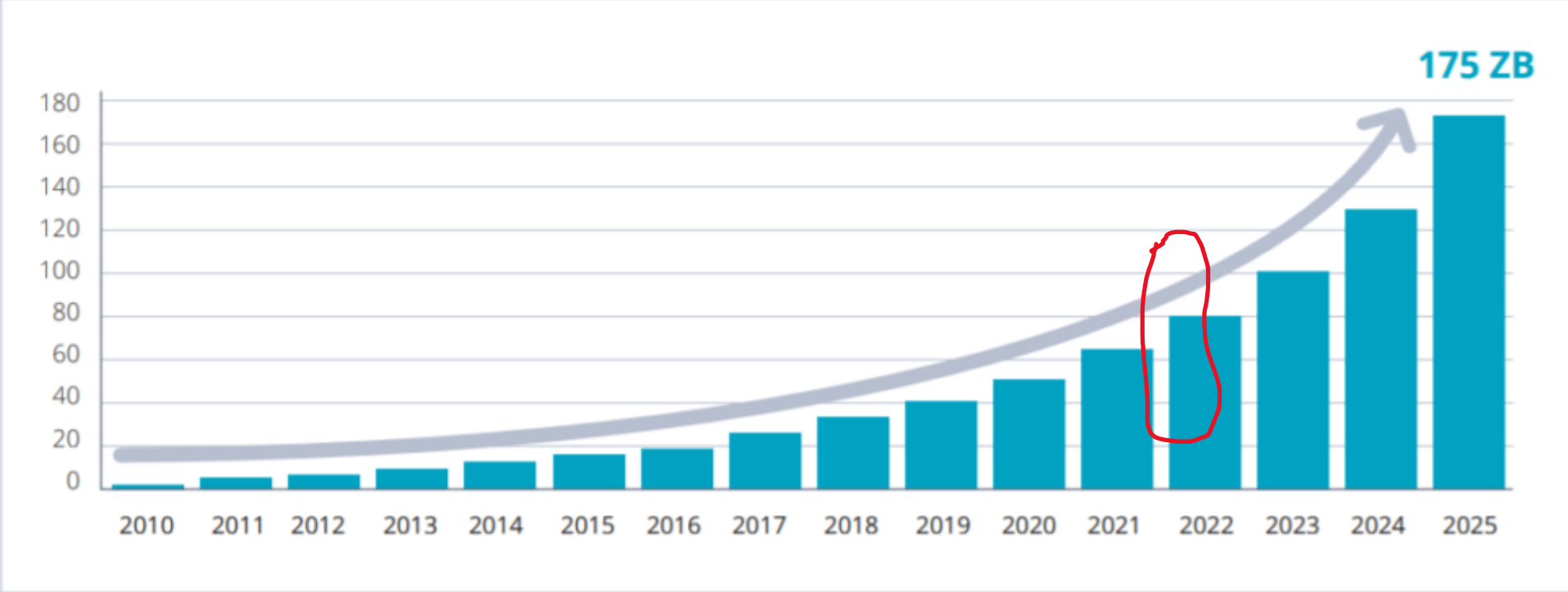
Szacowe dane dotyczące 60 sekund w internecie w 2021 roku



źródło: Lori Lewis | Statista
tłumaczenie: mobiRANK.pl

mobiRANK statista

WZROST WOLUMENU DANYCH NA ŚWIECIE



RYSUNEK 2.1.

Roczny wolumen danych na świecie w zettabajtach (bilionach gigabajtów)

Źródło: opracowanie własne na podstawie D. Reisel i in., *The Digitization of the World. From Edge to Core*, IDC White Paper #US44413318 2018, s. 6, https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.

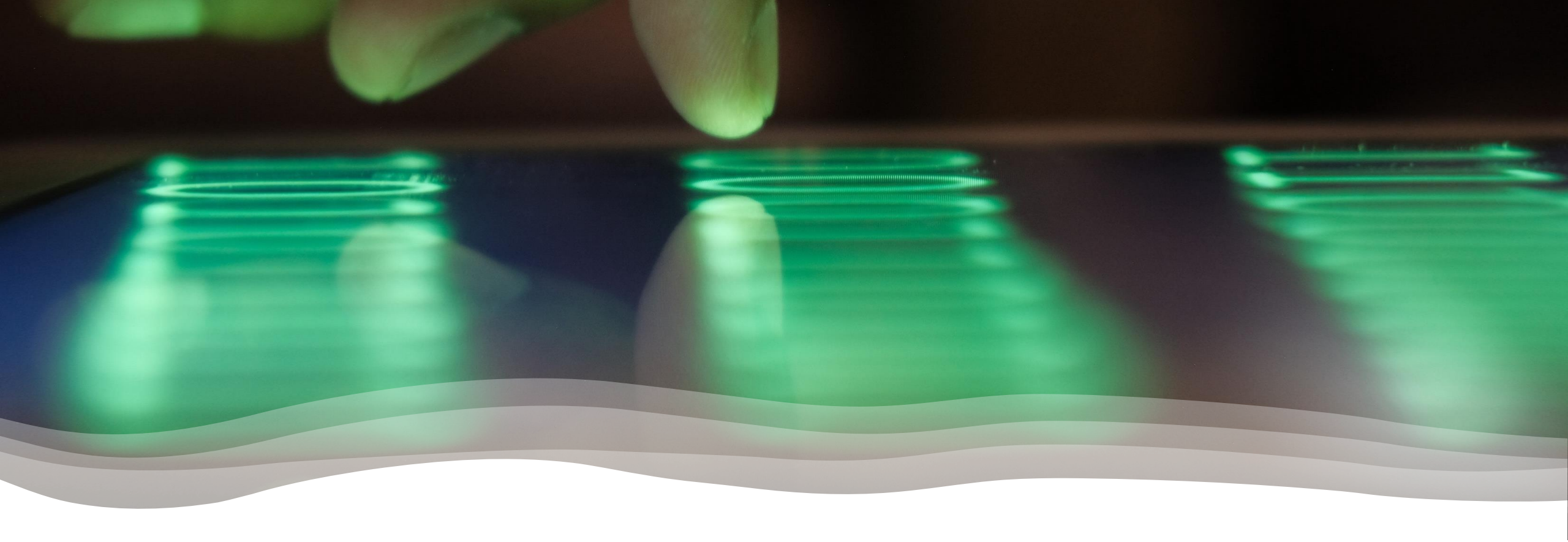
Źródło: https://przemyslprzyszlosci.gov.pl/wielki-wybuch-danych/

Cyberzagrożenia

Zasada Zero Zaufania stała się koniecznością

- Raport firmy Zscaler ukazuje 314% wzrostu ataków na zaszyfrowane kanały (HTTPS) względem 2020
- Na celowniku – znaczny wzrost ataków rok do roku:
  - Branża technologiczna: +2344%
  - Sprzedaż detaliczna i hurtowa: +841%
- Chwile na wytchnienie dla usług krytycznych – gwałtowny spadek liczby ataków – uwaga organów ścigania znacznie zmniejszyła ich atrakcyjność:
  - Opieka zdrowotna była największym celem w 2020 r.
  - Organizacje rządowe i infrastruktury krytycznej (np. Colonial Pipeline).
- Najbardziej atakowane kraje to: Wielka Brytania, USA, Indie, Australia i Francja.
- Taktyka się zmienia – ransomware zyskuje na popularności:
  - Malware: +212%
  - Phishing: +90%
  - Cryptomining malware: -20%.
- Zasada Zero Zaufania najlepszym sposobem ochrony zagrożeniami na szyfrowane kanały - architektury zerowego zaufania w oparciu o serwer proxy w chmurze zmniejsza powierzchnię ataku i umożliwia inspekcję całego ruchu przychodzącego i wychodzącego w trybie bezpośrednim i na dużą skalę.

https://www.zscaler.com/blogs/security-research/cybersecurity-lessons-carry-2022



Trendy technologiczne & Cyberbezpieczeństwo

PbD & Trendy technologiczne

PbD

obliguje administratorów i podmioty przetwarzające do ciągłego monitorowania trendów technologicznych i ich wykorzystania w nowoczesnych technologiach - art. 25 i 32 RODO

Trendy technologiczne

wskazane co roku przez Gartnera i ich wpływ na ochronę danych oraz cyberbezpieczeństwo

Gartner: strategicznych trendów technologicznych 2022 roku

Trzy motywy przewodnie w 2022

Budowanie zaufania (Engineering Trust)	**Kształtowanie zmian** (Sculpting Change)	**Przyspieszanie wzrostu** (Accelerating Growth)
Tworzenie bardziej odpornych i wydajnych podstaw IT poprzez zapewnienie integracji i bezpieczniejszego przetwarzania danych w środowiskach chmurowych i innych niż chmura w celu zapewnienia **ekonomicznego skalowania podstaw IT**	Kreatywne rozwiązania z zakresu nowych technologii w tym obszarze, pomoże skalować i przyspieszać cyfryzację organizacji. Nowe trendy technologiczne pozwalają **reagować na rosnące tempo zmian**, szybciej tworząc aplikacje automatyzujące działania biznesowe, optymalizujące sztuczną inteligencję (AI) i **umożliwiające szybsze podejmowanie dobrych decyzji**	Wykorzystanie strategicznych trendów technologicznych zwiększa siły IT, które pozwolą zdobyć biznes i udział w rynku. Razem te trendy umożliwiają **maksymalizację tworzenia nowych rozwiązać oraz zwiększyć możliwości cyfrowe**

Trendy technologiczne 2022 r.

Trend 1: **Siatka danych (Data Fabric) -** elastyczna i wytrzymała integracja danych pomiędzy różnymi platformami a użytkownikami biznesowymi – pozwala uprościć infrastrukturę wymiany informacji w organizacji i stworzyć skalowalną architekturę. Data Fabric oferuje zestaw usług związanych z danymi, które zapewniają spójne możliwości dla różnych punktów końcowych w hybrydowych środowiskach wielochmurowych.
Wartością Data Fabric, dzięki wbudowanej analityce, jest jej zdolność do dynamicznej poprawy **wykorzystania danych i łatwiejsze zarządzanie danymi nawet o 70%.**

Trend 2: Architektura siatki bezpieczeństwa cybernetycznego
(CyberSecurity Mesh Architecture – CSMA) - dane i użytkownicy mogą znajdować się gdziekolwiek, a to oznacza, że tradycyjna granica bezpieczeństwa odchodzi w niepamięć. Wymaga to architektury siatki bezpieczeństwa cybernetycznego, która pomoże zapewnić zintegrowaną strukturę bezpieczeństwa w celu zabezpieczenia wszystkich aktywów, niezależnie od lokalizacji, jednocześnie **przesuwając punkty kontrolne bliżej zasobów**, które mają chronić. Może szybko i niezawodnie weryfikować tożsamość, kontekst i zgodność z zasadami w środowiskach chmurowych i innych niż chmura. **Do roku 2024 organizacje przyjmujące architekturę CSMA w celu zintegrowania narzędzi bezpieczeństwa, by działały jako współpracujący ekosystem, odczują średnio o 90% mniejsze skutki finansowe pojedynczych incydentów bezpieczeństwa.**

Trendy technologiczne 2022 roku

Trend 3: Obliczenia zwiększające prywatność – oprócz radzenia sobie ze zmieniającym się międzynarodowym prawem dotyczącym prywatności i ochrony danych organizacje muszą unikać utraty zaufania klientów z powodu incydentów związanych z ich poufnością. Gartner przewiduje, że **do 2025 roku 60% dużych organizacji będzie stosować jedną lub więcej technik obliczeniowych zwiększających ich ochronę**.
Techniki obliczeniowe – które chronią dane osobowe i **wrażliwe informacje na poziomie danych, oprogramowania lub sprzętu** – bezpiecznie udostępniają, gromadzą i analizują dane bez naruszania poufności lub prywatności. Powszechne są przypadki użycia zarówno w wielu branżach, jak i infrastrukturach chmury publicznej, np. **zaufane środowiska wykonawcze.**

Trend 4: **Platformy natywne dla chmury (Cloud-Native Platforms (CNP)) -** odejście od metody typu *lift and shift* i zwrócić się w pełni w stronę platform chmurowych. Platformy CN wykorzystują podstawowe możliwości chmury obliczeniowej, zapewniając oczekiwane **skalę i elastyczność** dla twórców technologii dostarczających swoje usługi w modelu **SaaS**, co przyspiesza szybszy zwrot z inwestycji i redukuje koszty.
Analitycy Gartnera przewidują, że **do 2025 r. platformy chmurowe będą stanowić podstawę ponad 95% nowych inicjatyw cyfrowych – w 2021 r. było ich niecałe 40%**

Trend 5: **Aplikacje komponowalne -** umiejętność adaptacyjna organizacji w stronę architektury technologicznej, która umożliwi **szybką, bezpieczną i wydajną zmianę aplikacji.** To idea, zgodnie z którą bloki funkcjonalne aplikacji można oddzielić od kompletnej aplikacji lub procesu. Oznacza to, że można tworzyć nowe aplikacje, które są lepiej dopasowane, efektywniejsze, mają lepszą funkcjonalność. Komponowalna architektura aplikacji wspiera taką adaptację, a firmy, które przyjęły to podejście, **wyprzedzą konkurencję o 80% pod względem szybkości wdrażania nowych funkcji.**

Trend 6: Inteligencja decyzji - praktyczne podejście do usprawnienia podejmowania decyzji organizacyjnych. Modeluje każdą decyzję jako zestaw procesów, wykorzystując inteligencję i analizy do informowania, uczenia się na podstawie i udoskonalania decyzji. Inteligencja decyzyjna może wspierać i usprawniać podejmowanie decyzji przez ludzi, Gartner przewiduje, że w **ciągu najbliższych dwóch lat jedna trzecia dużych organizacji będzie wykorzystywać inteligencję decyzyjną do podejmowania ustrukturyzowanych decyzji w celu zwiększenia przewagi konkurencyjnej.**

Trendy technologiczne 2022 roku

Trend 7: **Hiperautomatyzacja -** przyspiesza wzrost i zwiększa elastyczność biznesu poprzez **szybką identyfikację, weryfikację i automatyzację jak największej liczby procesów biznesowych i informatycznych**. Hiperautomatyzacja umożliwia skalowalność, zdalną obsługę i zmianę modelu biznesowego.

Trend 8: **Inżynieria AI** - przedstawia zintegrowane podejście do wykorzystania modeli AI w praktyce poprzez **automatyczną aktualizację danych, modeli i aplikacji** w celu usprawnienia dostarczania AI dla wartości biznesowej.

– W przypadku połączonych zespołów zajmujących się sztuczną inteligencją, prawdziwym wyróżnikiem ich organizacji będzie ich zdolność do ciągłego zwiększania wartości poprzez szybkie zmiany AI. ***Do 2025 roku 10% przedsiębiorstw, które ustanowią najlepsze praktyki w zakresie inżynierii AI, wygeneruje co najmniej trzykrotnie większą wartość z włożonych wysiłków niż 90% przedsiębiorstw, które tego nie zrobią*** *(*powiedział D. Groombridge wiceprezes ds. badań w firmie Gartner).

Trend 9: Przedsiębiorstwa rozproszone - zdalnych i hybrydowych modeli pracy przekształcają się w przedsiębiorstwa rozproszone, realizujące zadania z różnych lokalizacji, co wymaga wprowadzenia zmian technicznych i usługowych zapewniających bezproblemowe wykonywanie pracy. To powoduje konieczność przekonfigurowania modelu dostarczania usług o usługi rozproszone, np. ubrania przymierzać w cyfrowej przymierzalni.
Analitycy Gartnera uważają, że **do 2023 roku 75% organizacji korzystających z zalet przedsiębiorstwa rozproszonego osiągnie wzrost dochodów o 25% szybciej niż konkurenci**.

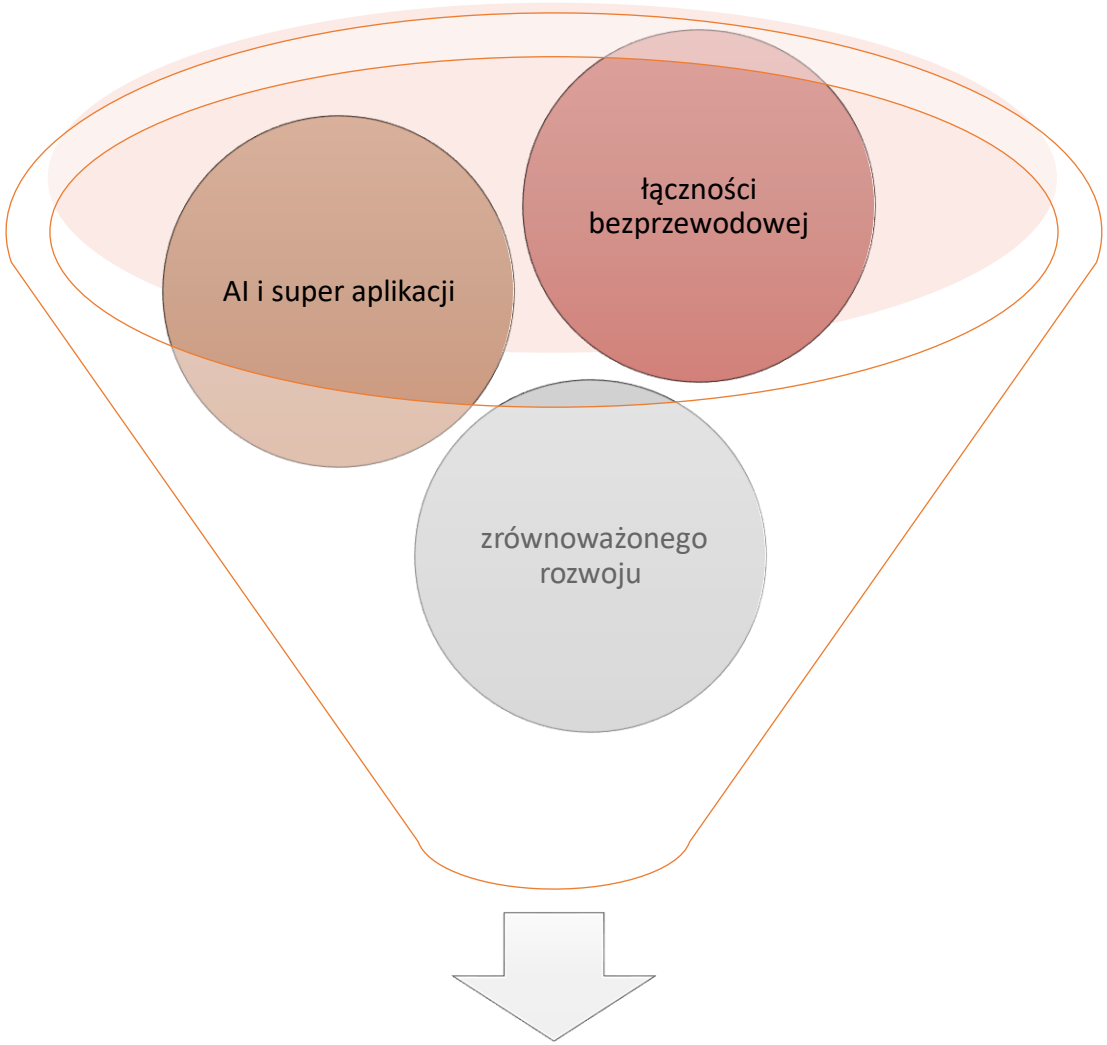
Trendy technologiczne 2022 roku

Trend 10: **Całkowite doświadczenie (Total Experience – TX) -** to strategia biznesowa łącząca dyscypliny **customer experience (CX), employee experience (EX), user experience (UX) oraz multiexperience (MX)**. Celem TX jest **zwiększenie zaufania klientów i pracowników, ich satysfakcji, lojalności i poparcia**. Organizacje zwiększą przychody i zyski dzięki osiąganiu adaptacyjnych i elastycznych wyników biznesowych w ramach modelu TX.

Trend 11: **Systemy autonomiczne** - samodzielnie zarządzane systemy fizyczne lub programowe, które uczą się od swoich środowisk i **dynamicznie modyfikują własne algorytmy w czasie rzeczywistym**, aby zoptymalizować swoje zachowanie w złożonych ekosystemach. Systemy autonomiczne tworzą zwinny zestaw możliwości technologicznych, które są w stanie obsługiwać nowe wymagania i sytuacje, optymalizować wydajność i bronić się przed atakami bez interwencji człowieka.
– Zachowanie autonomiczne można już obserwować w złożonych systemach zabezpieczeń, w dłuższej perspektywie upowszechni się ono w takich zastosowaniach, jak roboty, drony, maszyny produkcyjne czy inteligentne miasta.

Trend 12: Generatywna sztuczna inteligencja (Generative AI, GAI) - metody uczenia maszynowego polegające na uczeniu się treści lub obiektów na podstawie danych szkoleniowych i wykorzystujące je do **generowania zupełnie nowych produktów**, czyli na podstawie dostępnego tekstu, plików audio, obrazów i filmów tworzy zupełnie nowy zestaw danych.
Wykorzystanie m.in. do **tworzenia kodu oprogramowania, opracowywania receptur leków czy marketingu ukierunkowanego,** ale również do oszustw, wyłudzeń, dezinformacji politycznej czy fałszowania tożsamości.
Gartner spodziewa się, że **do 2025 r. Generatywna AI będzie odpowiadać za 10% wszystkich generowanych danych w porównaniu z mniej niż 1% obecnie.**

Trendy technologiczne 2023 roku



Trendy technologiczne 2023 roku

1. Technologie bezprzewodowe - Gartner przewiduje, iż do 2025 roku 60% przedsiębiorstw będzie korzystać z pięciu lub więcej technologii bezprzewodowych jednocześnie w tym m.in. 4G, 5G, LTE, WIFI 5, 6, 7. Integracja technologii bezprzewodowych zapewni bardziej opłacalną, niezawodną i skalowalną podstawę technologiczną, będącą źródłem danych i wartości biznesowej.

2. Superaplikacje - stosowanie nowego rodzaju platform łączących w sobie różne aplikacje i usługi w jeden ekosystem zwane jest superaplikacją (superapp). Udostępniona innym podmiotom platforma pozwala im na tworzenie i publikowanie mini aplikacji stron trzecich.

Analitycy przewidują, że do 2027 roku ponad 50% globalnej populacji będzie codziennie korzystać z wielu superaplikacji.

Przykład: Azjatyckie platformy: WeChat, AliPay i Gojek oraz japoński dostawca usług płatniczych PayPay, z prawie 50 milionami użytkowników, integruje w ramach jednej superaplikacji zakupy produktów i usług stron trzecich, np. kupowania biletów kinowych, zamawiania żywności czy wypożyczania rowerów.

3. Branżowe platformy chmurowe - duże platformy chmurowe oferujące połączenie SaaS, PaaS oraz IaaS zapewniające wsparcie dla konkretnych branż. Wykorzystanie pakietowych funkcjonalności branżowych platform chmurowych pozwoli organizacjom wdrażać innowacyjne rozwiązania sprawniej oraz w krótszym czasie wprowadzać produkty lub usługi na rynek. Wg Gartnera: do 2027 r. ponad 50% organizacji będzie korzystać z platform chmur branżowych.

Trendy technologiczne 2023 roku

4. Inżynieria platformowa - inżynieria platformowa tworzy i wykorzystuje samoobsługowe wewnętrzne platformy programistyczne w celu dostarczania oprogramowania i zarządzania cyklem jego życia. Benefitem użycia inżynierii platformowej jest optymalizacja doświadczeń programistów i przyspieszenie dostarczania produktów dla klientów przez zespoły deweloperskie.

Gartner przewiduje, że do 2026 r. 80% organizacji zajmujących się inżynierią oprogramowania utworzy zespoły platformowe, a 75% zbuduje portale samoobsługowe dla programistów.

5. Adaptacyjna Sztuczna Inteligencja - adaptacyjne systemy AI mogą stale, w oparciu o wciąż nowe dane, zmieniające się okoliczności i cele uczyć się w środowiskach wykonawczych i programistycznych oraz przekwalifikowywać w czasie rzeczywistym modele swojej inteligencji.

6. Zarządzanie zaufaniem, ryzykiem i bezpieczeństwem AI - według Gartnera 41% organizacji doświadczyło naruszenia prywatności lub incydentu związanego z bezpieczeństwem AI. Pokazuje to, że organizacje nie są wystarczająco dobrze przygotowane do zarządzania ryzykiem AI, które wymaga nowych, niezapewnianych przez konwencjonalne mechanizmy kontrolne form zarządzania zaufaniem, ryzykiem i bezpieczeństwem **(ang. AI Trust, Risk and Security Management (AI TRiSM)**. Takie podejście pozwoli zapewnić organizacjom stosowanie niezawodnych modeli, wiarygodność, bezpieczeństwo i ochronę danych oraz realizować projekty AI przechodząc z etapu proof-of-concept do etapu produkcyjnego.

Przykład: Duński startup Abzu stworzył oparty na AI produkt, który generuje matematycznie wyjaśnialne modele, identyfikujące związki przyczynowo-skutkowe, pozwalające na łatwiejszą walidację wyników. Przykładowo, doprowadziły do opracowania skuteczniejszych leków na raka piersi.

Trendy technologiczne 2023 roku

7. Obserwowalność stosowana (Applied observability) - obserwowalne dane to wszelkie działania osób w sieci w postaci zdigitalizowanych artefaktów zebranych z infrastruktury, aplikacji i operacji przedsiębiorstwa, czyli logi, ślady, wywołania API, czasy przebywania (ang. dwell time), pobrania i transfery plików. Tak pozyskane dane dają organizacjom potężne narzędzie, obserwowalność stosowaną, do uzyskania przewagi konkurencyjnej, poprzez podejmowanie szybkich działań opartych danych i na potwierdzonych działaniach osób, a nie ich intencjach.

Przykład: Tesla wykorzystuje elementy obserwowalności stosowanej w ofertach ubezpieczenia pojazdu w kilku stanach USA wyłącznie na podstawie „obserwowalnego" stylu jazdy danego kierowcy mierzonego przez pojazd w czasie rzeczywistym. Kierowcy mogą zaoszczędzić nawet do 60% na składce.

8. Inżynieria platformy - platformy deweloperskie dostarczające oprogramowania w oparciu o budowanie i obsługę samoobsługowych wewnętrznych platform. Wg Gartnera: 80% organizacji zajmujących się inżynierią oprogramowania utworzy do 2026 r. zespoły ds. platform, a 75% z nich będzie obejmować samoobsługowe portale deweloperskie, które mogą zawierać różne komponenty wielokrotnego użytku oraz biblioteki narzędzi i innych modułów.

9. Cyfrowy system odpornościowy - cyfrowy system odpornościowy łączy wiele praktyk i technologii od obserwowalności, przez testy wspomagane sztuczną inteligencją, inżynierię chaosu, autonaprawę, koncepcję inżynierii niezawodności (ang. Site Reliability Engineering, w skrócie SRE), aż po bezpieczeństwo łańcucha dostaw oprogramowania – pozwala to zwiększyć odporność produktów, usług i systemów. Organizacje, które do 2025 r. zainwestują w budowanie odporności cyfrowej, zmniejszą przestoje systemów nawet o 80%, co powinno przełożyć się na wyższe przychody.

Przykład: American Airlines wykorzystują koncepcję inżynierii niezawodności (SRE), praktyki inżynierii chaosu oraz podejście „po pierwsze testy", aby lepiej radzić sobie ze złożonością systemów i usuwać nieznane luki oraz słabości.

Trendy technologiczne 2023 roku

10. Metaverse

Metaverse definiuje się jako zbiorową, wirtualną, trójwymiarową przestrzeń współdzieloną 3D, stworzoną poprzez konwergencję wirtualnie rozszerzonej rzeczywistości fizycznej i cyfrowej. Metaverse ma być trwały, zapewniając najlepsze możliwe wrażenia wielowymiarowe i zmysłowe. Wg Gartnera: metaverse będzie niezależny od urządzeń konkretnych marek i nie będzie własnością jednego dostawcy. Powstanie własna wirtualna gospodarka stworzona w oparciu o waluty cyfrowe i niezbywalne/ niewymienne tokeny (NFT). Do 2027 r. ponad 40 proc. dużych organizacji na świecie będzie korzystać z kombinacji Web3, chmury rozszerzonej rzeczywistości (AR) i cyfrowych bliźniaków w opartych na metaverse projektach przyczyniając się do zwiększenia przychodów.

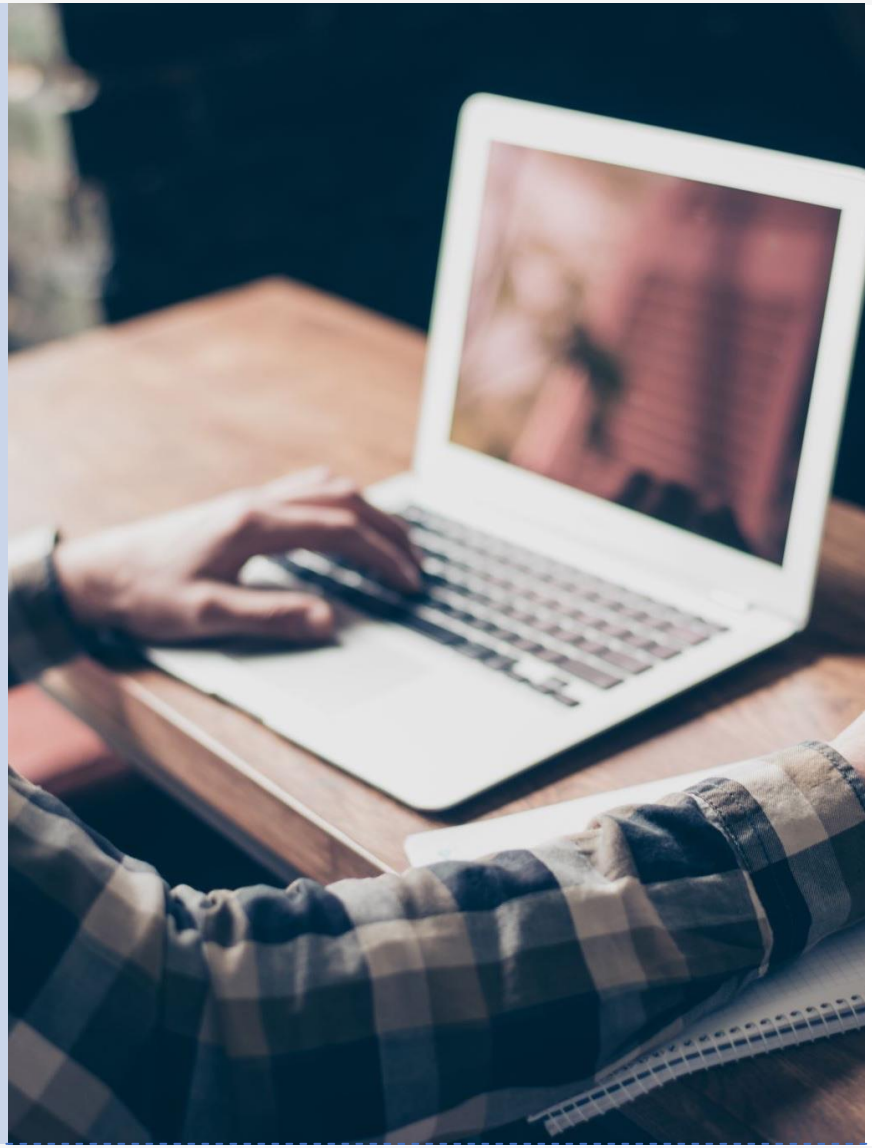
5 trendów technologicznych napędzających zmianę vs. Biznes & Bezpieczeństwo

- **Technologie zwiększające prywatność**
- **Architektura siatki bezpieczeństwa cybernetycznego**
- **Superaplikacje**
- **Cyfrowy system odpornościowy**
- **Generatywna sztuczna inteligencja**

Nowe trendy w cyberbezpieczeństwie na co dzień

Joanna Wziątek-Ładosz
Senior Security Engineer
Tenable

Trendy cyberzagrożeń



Skuteczność cyberataków

Socjotechnika - 80% do 90%

Brak aktualizacji oprogramowania - 20% do 40%

Źródło:

Roger Grimes, a former security specialist at Microsoft and now a data driven defense evangelist at KnowBe4

https://www.csoonline.com/article/3536696/us-secret-service-warns-of-malicious-emails-offering-covid-19-information.html

Na co zwracać uwagę w 2023?

- Praca zdalna i hybrydowa - miliony pracowników uzyskują obecnie dostęp do sieci korporacyjnych lub zasobów opartych na chmurze za pośrednictwem sieci prywatnego Wi-Fi.
- Działy IT zarządzają zdalnie systemami o znaczeniu krytycznym.
- Łańcuchy dostaw są obciążone

- **7 trendów cyberbezpieczeństwa:**
  1. Ransomware
  2. Cryptomining/Cryptojacking
  3. Deepfakes
  4. ataki wideokonferencyjne
  5. Ataki IoT i OT
  6. Ataki na łańcuch dostaw
  7. XDR

Źródło: https://www.csoonline.com/article/3262972/7-hot-cybersecurity-trends-and-2-going-cold.html

Trendy cyberbezpieczeństwa

1. **Ransomware** – praca zdalna i hybrydowa obliguje organizacje do dbania o pracowników i środowisku, w którym pracują.
   - Wdrażanie **cyberhigieny**, w tym szkoleń i edukacji dla całej organizacji, aby pomóc w łagodzeniu ataków phishingowych. Dodaje, że organizacje powinny być proaktywne w zabezpieczaniu danych i powinny rozważyć wdrożenie modelu bezpieczeństwa zero-trust.
2. **Cryptomining/Cryptojacking** - oprogramowania ransomware, występuje, gdy atakujący wykorzystują ataki phishingowe w stylu ransomware, aby włamać się do organizacji w celu wydobycia kryptowaluty przy użyciu zasobów obliczeniowych organizacji. Jedną z zalet atakującego jest to, że mogą pozostać niewykryci przez długi czas. Ponieważ nie żądano okupu i nie skradziono żadnych danych osobowych, firmy nie muszą ujawniać, że zostały zhakowane. Utrudnia to oszacowanie kosztów włamania, ponieważ szkody to takie rzeczy, jak utracone możliwości obliczeniowe, wolniejsza wydajność i wyższe rachunki za energię elektryczną. Jednakże, ponieważ kryptowaluty zyskują na wartości, istnieje większa zachęta dla atakujących do popełniania cryptojackingu. Ostateczna wypłata składa się z nagrody (w kryptowalucie) za bycie pierwszym, który zatwierdzi nowy blok transakcji.
3. **Deepfakes** – dezinformacja głównie w sferze rozrywki, politykami sfałszowanymi na wideo, mówiącymi rzeczy, których najwyraźniej nigdy nie powiedzieli, łamanie biometrycznej kontroli dostępu poprzez fałszowanie czyjejś twarzy, wykorzystanie sztucznej inteligencji np., w którym oszuści podszywają się pod głos prezesa i oszukali podwładnego, aby przelał dużą kwotę pieniędzy na fałszywe konto, do celów szantażu.
4. **Ataki na oprogramowanie wideokonferencyjne** - organizacje muszą przyjąć formalne zasady i procedury, których pracownicy będą przestrzegać, aby zwalczać cyberprzestępców próbujących podsłuchiwać rozmowy i przeglądać prezentacje, które mogą zawierać poufne informacje, np. czyszczenie list zaproszeń, zabezpieczanie wideokonferencji hasłem, wysyłanie haseł w oddzielnej komunikacji, ręczne przyjmowanie uczestników przez moderatora i blokowanie spotkania po jego rozpoczęciu.

Trendy cyberbezpieczeństwa

5. **Ataki IoT i OT** - ataki na infrastrukturę Internetu rzeczy (IoT), przemysłowego internetu rzeczy (IIoT) i technologii operacyjnych (OT) w tym na infrastrukturę krytyczną, zakładach produkcyjnych, a nawet w użyciu domowym. Atakujący będą atakować czujniki przemysłowe, aby spowodować fizyczne uszkodzenia, które mogą spowodować wyłączenie linii montażowych lub przerwanie usług.
   - Statystyki: Według jednego z eksperymentów, w którym testerzy konfigurowali sieć domową i monitorowali ją pod kątem ataków, w ciągu jednego tygodnia miało miejsce ponad 12 000 prób włamań.
6. **Ataki na łańcuch dostaw** - łańcuch dostaw jest tak silny, jak jego najsłabsze ogniwo i to wykorzystują hakerzy, np. atak SolarWinds, atak na łańcuch dostaw, w którym hakerzy wykorzystali lukę w oprogramowaniu do monitorowania sieci firmy SolarWinds, aby włamać się do setek firm. Zaleca się weryfikacje/kontrole stron trzeciech, partnerów, kontrahentów, dostawców usług zarządzanych i dostawców usług w chmurze.
   - Statystyki: dane firmy Forrester pokazują, że 55% specjalistów ds. bezpieczeństwa zgłosiło, że w ciągu ostatnich 12 miesięcy ich organizacja doświadczyła incydentu lub naruszenia z udziałem dostawców zewnętrznych lub łańcucha dostaw.
7. **Extended detection and response (XDR)** - zaawansowane narzędzie pozwalające na wykrywanie nietypowych zachowań i ataków, przeprowadzanie ocen ryzyka, reagowania na zdarzenia, prowadzenia dochodzeń oraz naprawy skutków ataków. Usługa oparta na chmurze, która obejmuje wiele strumieni danych związanych z bezpieczeństwem. XDR wykorzystuje moc analizy dużych zbiorów danych w chmurze, aby nadać sens danym z agentów ochrony punktów końcowych, bezpieczeństwa poczty e-mail, zarządzania tożsamością i dostępem, zarządzania siecią, bezpieczeństwa w chmurze, analizy zagrożeń i ich detekcję. Narzędzie, które może integrować możliwości wielu narzędzi bezpieczeństwa w celu wykrycia potencjalnego zagrożenia.
   - Statystyki: według Gartnera do końca 2027 roku aż 40% organizacji użytkowników końcowych będzie korzystać z CDR.

9 najpoważniejszych zagrożeń zidentyfikowanych w raporcie ENISA

Figure 1: ENISA Threat Landscape 2021 - Prime threats

- Ransomware (ataki z użyciem złośliwego oprogramowania na sieci i blokowanie danych z żądaniem okupu);
- Złośliwe oprogramowanie (malware);
- Kradzież kryptowalut (cryptojacking - przestępca wykorzystuje komputer ofiary do generowania kryptowalut);
- Zagrożenia związane z pocztą elektroniczną;
- Ataki na dane (naruszenie danych, wyciek danych);
- Zagrożenia dla dostępności i integralności danych (np. ataki typu DDoS – czyli blokowanie dostępu do usług poprzez sztuczne generowanie wzmożonego ruchu);
- Dezinformacja - fałszywe wiadomości;
- Zagrożenia inne niż złośliwe oprogramowanie (malware) - błędy ludzkie, nieprawidłowe konfiguracje systemów, wypadki mające wpływ na systemy informatyczne;
- Ataki na łańcuchy dostaw.

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Na co zwraca uwagę raport ENISY?

- **Wzrost zagrożeń związanych z oprogramowaniem ransomware**.
- **Zwiększone próby ataków** cyberprzestępców **na infrastruktury krytyczne**.
- Ataki **ransomware** zakłócające działalność placówek zdrowia publicznego, szpitali, służb ratunkowych oraz sektorów transportu i energii.
- **Ataki na łańcuchy dostaw**, które **w badanym okresie osiągnęły duży poziom oddziaływania**.
- **Cyberprzestępczość „jako usługa" (**„Hakerzy do wynajęcia") **-** nowy trend związany z cyberprzestępczością, która staje się częścią zorganizowanej działalności przestępczej. Modele działalności przestępczej - należą do nich np.:
  - ransomware jako usługa (ang. Ransomware-as-a-Service - RaaS),
  - phishing jako usługa (ang. Phishing-as-a-service - PhaaS)
  - dezinformacja jako usługa (ang. Disinformation-as-a-service – DaaS).

Przykład cennika cyberprzestępców

Pozycja	Cena
Zhakowanie poczty korporacyjnej	$10-20
Pakiet „nieinteligentnych” eksploitów	$25
Pakiet „inteligentnych” eksploitów	$10-3000
Podstawowy kryptograf (do wstawiania „złego” kodu) na początku plików)	$10-30
SOCKS bot (do obchodzenia firewalli)	$100
Bombardowanie atakiem DDoS	$30-70/dzień; $1200/miesiąc
Botnet	$200 za 2000 zombie
Botnet dostosowany do DDoS	$700
Kod źródłowy trojana ZeuS (do phishingu)	$200-250
Windows rootkit (do instalowania szkodliwych drajwerów)	$292
Zhakowanie konta Facebook lub Twitter	$130
Zhakowanie konta gmail	$162
Wysyłanie spamu	$10 za 1mln przesyłek
Wysyłanie phishingu (przy użyciu bazy adresatów)	$50-500 za 1 mln przesyłek

Zagrożenia dla oprogramowania open source w 2023 r.

Prawie 80% kodu w nowoczesnych aplikacjach to kod, który opiera się na pakietach open source - najsłabsze ogniwo w łańcuchu dostaw oprogramowania

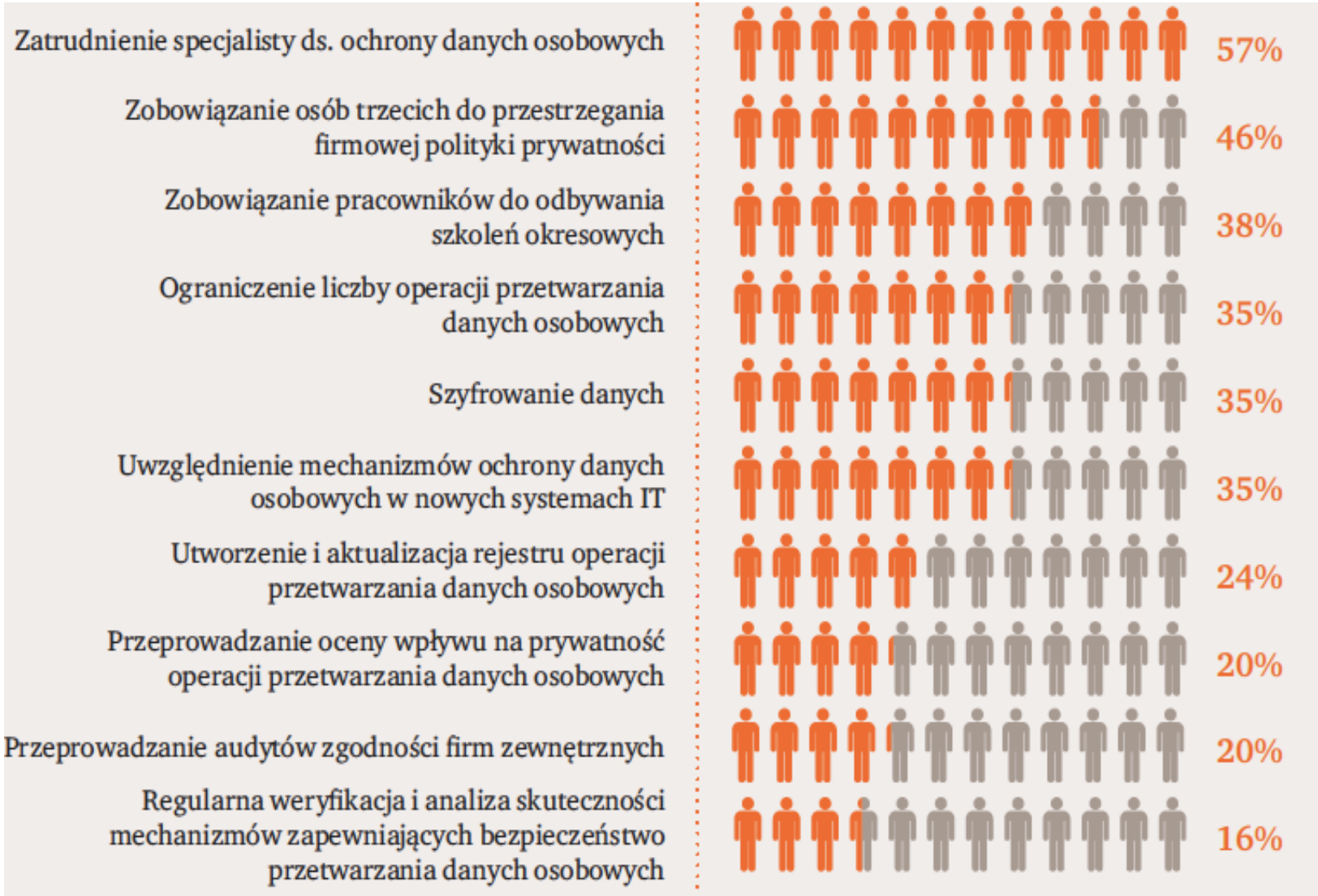
- **Wykorzystanie znanych luk** - ryzyko dla poufności, integralności lub dostępności danego systemu lub jego danych
  - **Działania**: należy przeprowadzać regularne skanowanie oprogramowania open source, a organizacje powinny priorytetowo traktować wyniki w celu optymalizacji alokacji zasobów.
- **Kompromitacja legalnego pakietu oprogramowania** - naruszenie części zasobów już istniejących lub infrastruktury dystrybucyjnej poprzez wstrzyknięcie złośliwego kodu.
- **Ataki polegające na myleniu nazw** - atakujący tworzy komponenty, których nazwy przypominają nazwy legalnych komponentów open source lub systemowych (typosquatting), sugerują godnych zaufania autorów (brandjacking) lub bawią się wspólnymi wzorcami nazewnictwa w różnych językach lub ekosystemach .
  - **Działania**: Sprawdzać charakterystykę kodu zarówno przed, jak i po podłączeniu instalacji, sprawdzać cechy projektu, takie jak repozytorium kodu źródłowego, konta opiekunów, częstotliwość wydawania, liczba dalszych.
- **Zagrożenia operacyjne**:
  - Brak aktualizacji i rozwijania oprogramowanie/komponentów
  - Przestarzałe oprogramowanie – używanie starej, przestarzałej wersji komponentów, mimo że istnieją nowsze wersje.
  - Nieśledzone zależności - deweloperzy projektu w ogóle nie są świadomi zależności od składnika, ponieważ nie jest on częścią listy komponentów nadrzędnych lub ponieważ narzędzia do analizy komponentów oprogramowania go nie.

- **84%** wszystkich baz kodu zbadanych przez Synopsys ma co najmniej jedna znana luka w zabezpieczeniach open source.
- **48%** wszystkich baz kodu analizowanych przez Synopsys zawierało luki wysokiego ryzyka - zostały aktywnie wykorzystane, mają już udokumentowane exploity typu proof-of-concept lub są klasyfikowane jako luki w zabezpieczeniach zdalnego wykonywania kodu.

Żdódło: https://www.csoonline.com/article/3688924/top-10-open-source-software-risks-for-2023.html

Jak się zabezpieczać - trendy i dobre praktyki

Jakie zabezpieczenia ochrony prywatności i cyberzagrożeń wdrażać?



Źródło: PWC - 5. edycja Badania Stanu Bezpieczeństwa Informacji

Opracowanie strategii zapobiegania i reagowania na oprogramowanie ransomware

- Wdrożenie bezpiecznych i redundantnych strategii **tworzenia kopii zapasowych**
- Wdrożenie i audyt **zarządzania tożsamością i dostępem** (najmniejsze przywileje i podział obowiązków)
- **Szkolenie i podnoszenie świadomości** użytkowników (w tym uprzywilejowanych)
- **Rozdzielenie środowisk** deweloperskich, testowych i produkcyjnych
- Przekazywanie i **wymiana informacji** o incydentach z branżą i CERT
- **Ograniczanie dostępu** do znanych witryn ransomware
- **Tożsamości i dane uwierzytelniające** powinny być wydawane, zarządzane, weryfikowane, odbierane i poddawane audytowi dla urządzeń, użytkowników i procesów
- Uprawnienia dostępu i autoryzacje powinny być zarządzane z uwzględnieniem **zasad minimalnego dostępu** adekwatnego do wypełniania obowiązków
- **Plany reagowania i odzyskiwania danych** po ataku ransomware powinny być okresowo **testowane**, aby upewnić się, że założenia i reakcja są adekwatne do ewoluujących zagrożeń ransomware
- Przeprowadzenie oceny **oprogramowania do wykrywania ransomware**, np. narzędziem opracowanym przez CISA, przeznaczonego dla sieci IT i ICS (systemu kontroli przemysłowej)
- **Monitorowanie systemów** w celu szybkiej identyfikacji infekcji
- **Nadążanie za najnowszymi trendami** oprogramowania ransomware, rozwojem i propozycjami zapobiegania

Okupy są coraz wyższe i częściej płacone

- Odsetek firm zatrudniających ponad 100 osób, które zostały dotknięte atakami ransomware, wzrósł na całym świecie – z **37% w 2020 roku do 66% w 2021**.
- Średni płacony okup był prawie pięciokrotnie wyższy niż rok wcześniej i wyniósł **812 tys. dolarów**.
- Trzykrotnie wzrósł też odsetek przedsiębiorstw, które zapłaciły przestępcom co najmniej milion dolarów. Firmy są coraz bardziej skłonne przesłać atakującym okup – w **2021 roku zrobiło to aż 46% (w 2020 roku było to 32%).**

Raport Sophos, 2021, https://avlab.pl/3-na-4-polskie-firmy-padly-ofiara-ransomware/

Co o tym myślisz?

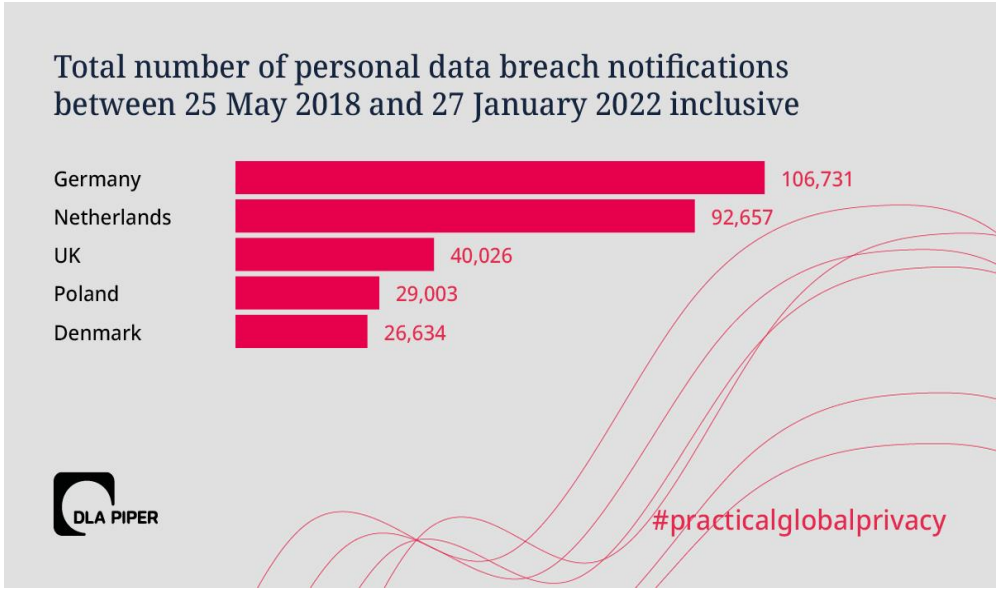
- **26%** ankietowanych z Polski jest zdania, że ich organizacja **nie traktuje cyberbezpieczeństwa dość poważnie**
- **10%** badanych z Polski **nie wie** czy ich organizacja posiada jakiekolwiek cyberzabezpieczenia
- **50%** respondentów z Polski **nie korzysta z VPN** łącząc się z siecią
- Ponad **50%** uczestników badania z Polski **przynajmniej raz w tygodniu omija firmowe zabezpieczenia**, aby móc wykonywać swoje obowiązki (**17% robi to każdego dnia**)
- **10%** badanych **zawsze korzysta z tych samych haseł**
- **10%** resetuje hasło za każdym razem, gdy musi wykonać zadanie, które nie należy do codziennych obowiązków
- Dla prawie **40%** polskich pracowników **zapewnienie bezpieczeństwa urządzeń**, na których pracują nie ma znaczenia
- Niemal **20%** ankietowanych z Polski przyznało, że wykonywanie zadań w sposób bezpieczny jest skomplikowane, gdyż wymaga wpisywania wielu haseł i specjalnych procedur logowania w różnych aplikacjach
- ok. **10%** uważa, że **cyberbezpieczeństwo tylko zabiera cenny czas**, który mogliby poświęcić na pracę

badanie przeprowadzone przez Cisco wśród pracowników polskich firm umożliwiających pracę zdalną – kwiecień 2022

Privacy Enhancing Technologies (PETs)

Technologie zwiększające prywatność (PET) - szeroki wachlarz **technologii, rozwiązań sprzętowych lub programowych**, których celem jest pełne wykorzystanie danych bez **narażania ich prywatności i bezpieczeństwa.**
https://www.enisa.europa.eu/publications/pets-maturity-tool

Poprzez minimalizację wykorzystania danych osobowych, maksymalizację bezpieczeństwa danych i wzmocnienie praw osób PET chroni prywatność osób w usługach lub aplikacjach dostępnych w Internecie bez utraty ich funkcjonalności.

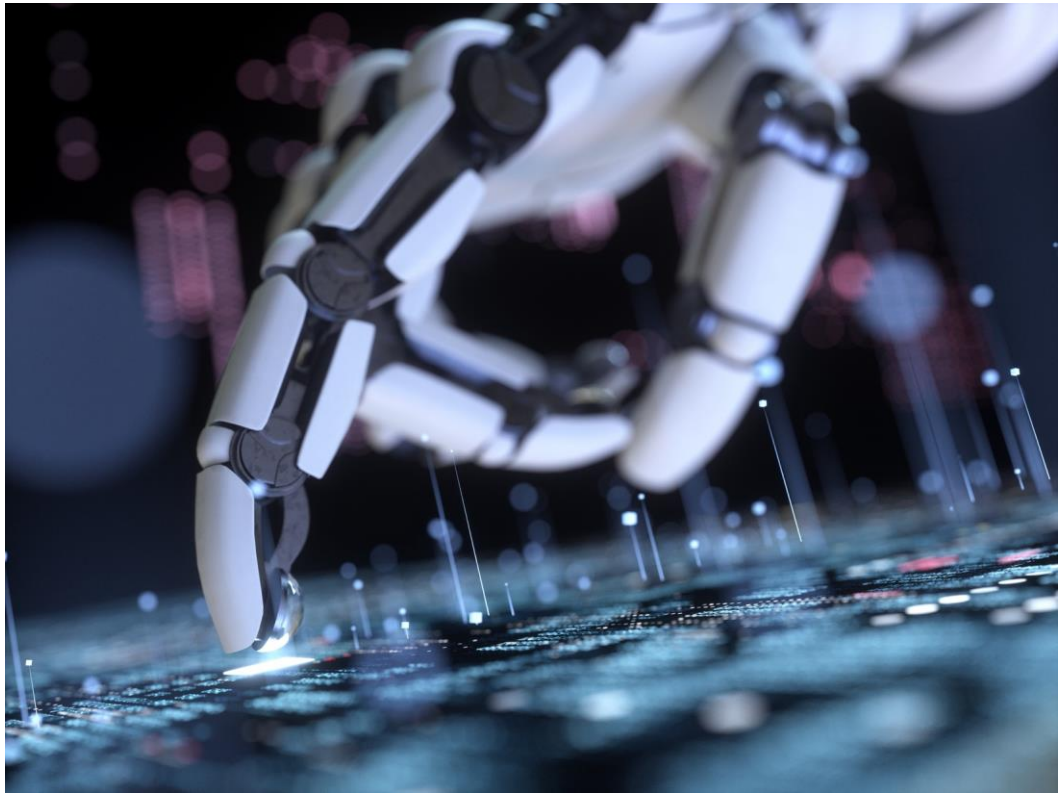


PETs jest ważne z trzech powodów :

1. Uniknięcie kar za naruszenia przepisów prawa - zgodnie z ankietą DLA Piper GDPR Data Breach Survey 2020, grzywny RODO przekraczają **1,6 mld EUR od maja 2018 do marca 2022**
2. Bezpieczna możliwość ochrony prywatności podczas **udostępniania danych**, np. do analizy i przetestowania aplikacji przez organizacje zewnętrzne
3. Naruszenie prywatności zagraża **reputacji firmy**, przykładem może być utrata kursu akcji Facebooka po skandalu z Cambridge Analytica.

PET

- **2021 rok: PET** zostały uznane przez Gartnera za **najważniejszy trend technologiczny**
- Grupa technologii, której celem jest zachowanie **poufności** przetwarzanych danych i **osiągnięcie wysokiego poziomu ochrony danych osobowych** przed naruszeniami oraz atakami hakerów
- W zależności od uprawnień pozwalają na dostęp do danych przy jednoczesnym **zapewnieniu kontroli, bezpieczeństwa i prywatności**
- Przykłady PET:
  - Szyfrowanie homomorficzne
  - Zaufane środowiska obliczeniowe
  - Bezpieczne obliczenia wielostronne/wielopodmiotowe
  - Prywatność różnicowa
  - Osobiste magazyny danych
  - Zaciemnianie
  - Enhanced Privacy ID
  - Pseudonimizacja
  - Szyfrowanie zachowujące format
  - Tokenizacja zachowująca format



Zastosowanie PET na przykładzie daty

1975-04-18

Dane w spoczynku

Hja&12B%2M>

07/12/2014

43-vk-df-43-a5

Szyfrowanie:
- AES
- 3DES

Tokenizacja

Szyfrowanie z zachowaniem formatu:
- FF1
- FF3

Funkcje haszujące

Dane w użyciu

//1975

Od 40 do 49 lat

Maskowanie
- Warstwa prezentacji
- Dynamiczne maskowanie danych

Anonimizacja:
- agregacja

Klient	PESEL	Data ur.	Email	Miasto	Kod poczt.	Nr karty kred.	Typ	Wartość
Jan Nowak	69072206253	22-07-1969	jan.nowak@email.com	Warszawa	PL00-193	6287 8107 3365 9842	Indywidualny	100 344
Dane w spoczynku			**Tokenizacja**					
Hdu Jnkow	67122835031	04-12-1972	0m6.h4jk7@lhu1d.xyk	Kjauiwek	PL60-034	3490 3343 3884 3902	Indywidualny	97 234
Dane w użyciu – Instytucja finansowa			**Detokenizacja**					
Jan Nowak	69072206253	22-07-1969	jan.nowak@email.com	Warszawa	PL00-193	6287 8107 3365 9842	Indywidualny	100 344
Dane w użyciu – Dział obsługi klienta			**Maskowanie**					
Jan Nowak	*******	6253	22-07-	****	0m6.h4jk7@lhu1d.xyk	Warszawa	PL00-193	**** **** **** 9842	Indywidualny	*** ***
Dane w użyciu – Uczenia maszynowe			**Anonimizacja**					
Hdu Jnkow	67122835031	50 do 59 lat	0m6.h4jk7@lhu1d.xyk	******	PL00-	***	3490 3343 3884 3902	Indywidualny	>80 000

Zastosowanie PET w zależności od celu

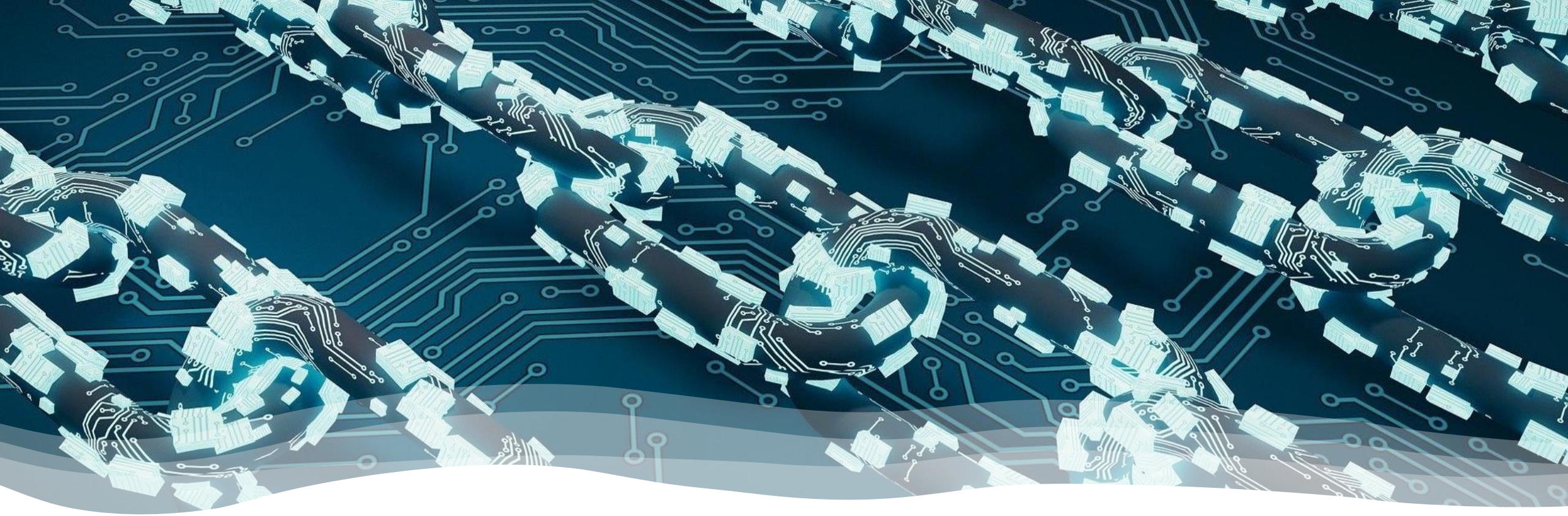
Podsumowanie: Dlaczego warto stosować PET?

PbD

- **Prywatność i bezpieczeństwo** wbudowane w projektowanie systemów przetwarzania danych zgodnie z zasadę ochrony danych w **fazie projektowania** pozwolą na realizację projektów, które będą przetwarzały np. **duży zakres i dużą skalę dane w tym nawet dane szczególne** przy jednoczesnym zapewnieniu spełnienia przez system obecnych i przyszłych wymagań prawnych.

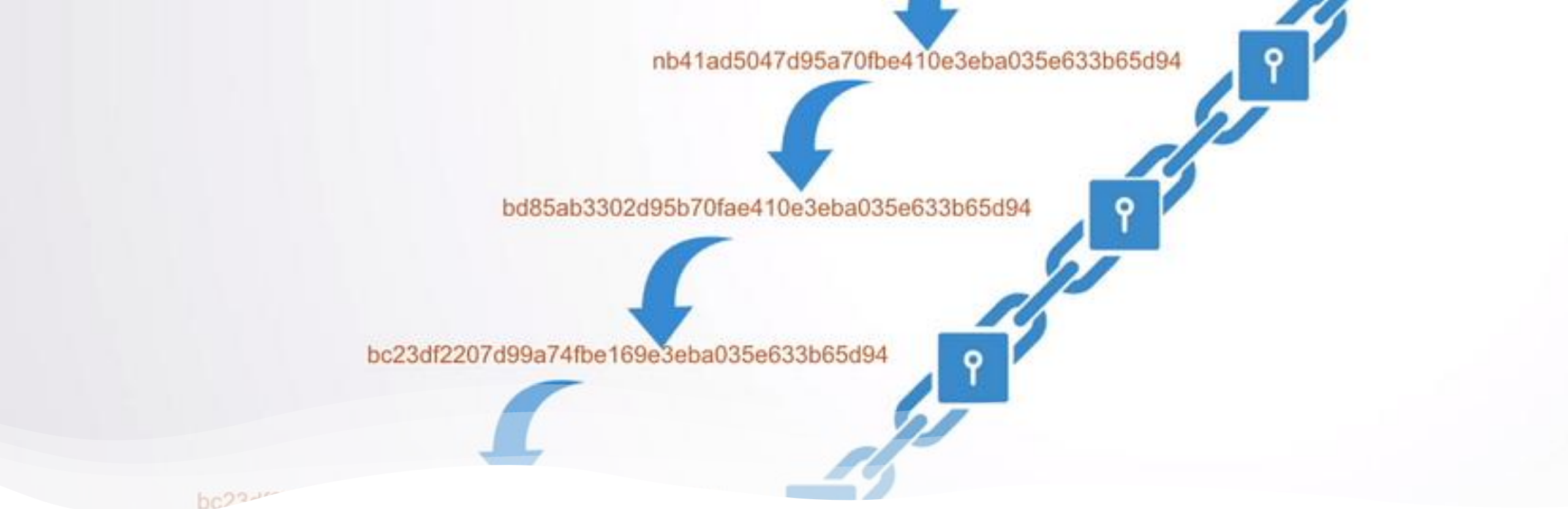
Wtórne przetwarzanie danych

- PET nie tylko pozwalają projektować i budować systemy przetwarzania danych zapewniające bezpieczeństwo i prywatność na adekwatnym do ryzyka poziomie, ale jednocześnie umożliwiają wykorzystanie danych do celów **analitycznych, naukowych, uczenia maszynowego, AI.**



Definicje: Technologia rozproszonego rejestru

- **Technologia rozproszonego rejestru** (również Technologia rozproszonych rejestrów, ang. *Distributed Ledger Technology, DLT*) – rodzaj technologii wspierającej rozproszone rejestrowanie zaszyfrowanych danych. Technologia oparta o rozproszone bazy danych, której rejestry są **replikowane, współdzielone i zsynchronizowane** w ramach konsensusu różnych, rozproszonych geograficznie, osób, firm lub instytucji.



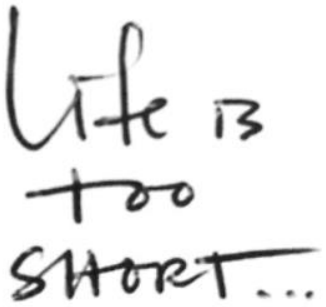
Definicje: Blockchain

- **Blockchain** – łańcuch powiązanych ze sobą bloków przy użyciu kryptografii. Każdy blok zawiera znacznik czasu, dane transakcji i kryptograficzny skrót – hasz (hash) poprzedniego bloku, tworząc **chronologiczny, jednokierunkowy** łańcuch połączonych bloków. **Niezmienność i integralność** blockchain jest zapewniana przez kryptograficzne połączenie bloków, a każda modyfikacja danych zawartych w bloku, który stał się już częścią łańcucha, zmieniłaby jego kryptograficzny hasz użyty w kolejnym bloku.
- 2009r. - Satoshi Nakamoto stworzył na podstawie tej technologii i wprowadził do obiegu kryptowalutę **bitcoin**.
- Technologia blockchain (zwana też „łańcuchem bloków”) jest obecnie postrzegana jako **narzędzie kreowania zaufania w powiązaniach sieciowych**, czyli sytuacjach, w których powodzenie działań zależy od innych osób, firm, instytucji czy urzędów.

Rodzaje blockchain

	Typ blockchain		
	Publiczny	Prywatny	Federacyjny
Dostępny dla wszystkich?	Tak	Nie	Nie
Kto ma do niego wgląd?	Każdy	Tylko zaproszeni użytkownicy	Różnie
Kto może dodawać dane?	Każdy	Zatwierdzeni uczestnicy	Zatwierdzeni uczestnicy
Właściciel	Brak	Pojedynczy podmiot	Liczne podmioty
Czy uczestnicy są znani?	Nie	Tak	Tak
Prędkość transakcji	Niska	Wysoka	Wysoka

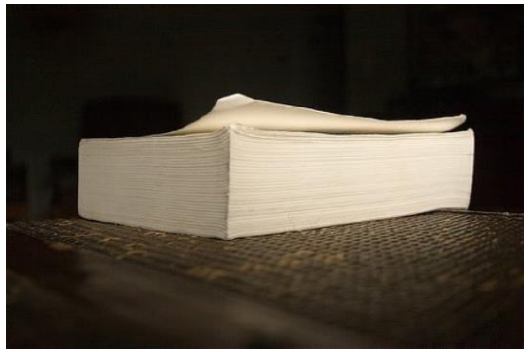
Budowa funkcji haszującej



13bac4a198fc1c1a
4afbf4c8926fb924
67ae41e4649b934c
0495991b7852b855(16)

h

h



8afbf4c8a3b0c41b
914c1c14927ae41e
1636fb92449a2b85
5785b934c49a9914(16)

Podstawowe cechy RR i blockchain

Transparentność

- równy dostęp do danych dla wszystkich użytkowników

Prywatność & anonimowość

- zastąpienie danych użytkowników identyfikatorami

Niezależność

- brak zaufanej instytucji pośredniczącej w weryfikacji transakcji i jej stron

Zaufanie & bezpieczeństwo

- odporność na cyberataki dzięki niezmienności transakcji

Nieodwracalność & efektywność

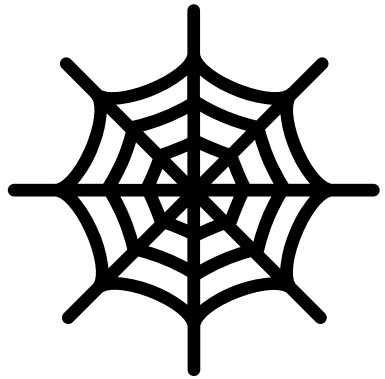
- unikanie czasochłonnego uzgadniania rekordów, dzięki rozproszonym rejestrom

Jak działa transakcja bitcoin?

Przelew bitcoin

Dodaje do bitcoinów:
Klucz publiczny Boba
Własny klucz prywatny

Sieć węzłów (nodów)



Akceptacje przelewu: potwierdzenie cyfrowych podpisów i liczby bitcoinów. Dodanie nieodwracalnej informacji o transakcji do bloku (znacznik zmienny w czasie, ang. Nounce).

Odbiera transakcję

Klucz prywatny pozwala na dostęp do przelanych bitconów.

1. Alicję przelewając bitcoiny Bobowi dodaje do przelewu klucz publiczny Boba oraz podpis własnego klucza prywatnego.
2. Ogłasza transakcję w sieci, której poprawności podpisu cyfrowego oraz ilość bitcoinów jest potwierdzana akceptowana przez sieć.
3. Ostatnim elementem transakcji jest dodanie informacji o niej do bloku, który na zawsze zostanie przypisany do blockchaina.

Blockchain & Zaufanie & Bezpieczeństwo

- **Wysoki poziom bezpieczeństwa** - publiczny blockchain oparty na protokole niewymagającym potwierdzenia zaufania (Trustless) oraz stosowania metod osiągania konsensusu PoW, PoA, PoS lub PoE.
- **Transparentność i otwartość** sieci blockchain wynika z faktu weryfikacji każdej transakcji przez uczestników - nie ma więc możliwości oszustwa tak długo, jak osoba posiada swój klucz prywatny i podpisane nim środki należą do niej.

Ryzyko:

Ryzyko zgubienia/zapomnienia klucza - czynnik ludzki, który trudno wyeliminować.

Rodzaje cyberataków

- **Atak na routing** - ogromna ilość danych transferowana w czasie rzeczywistym pozwala hakerom przechwycić dane w drodze do dostawców usług internetowych, co jest niezauważalne przez użytkowników blockchain.
- **Atak 51%** - do wydobycia zasobów publiczny blockchain potrzebuje ogromnej mocy obliczeniowej. Jeżeli nieuczciwi górnicy przejmą kontrolę nad księgą i zbiorą wystarczającą ilość zasobów, czyli ponad 50% mocy wydobywczej sieci blockchain to mogą przejąć kontrolę nad rejestrem.

  Uwaga: Prywatny blockchain nie jest podatny na atak 51%.
- **Atak Sybil** - nazwa pochodzi od imienia Sybil Dorsett cierpiącej na zaburzenia zespołem wieloosobowym. Atak polega na stworzeniu wielu fałszywych tożsamości kontrolowanych w rzeczywistości przez jedną osobę, co powoduje rozbicie systemu.
- **Atak phishingowy** - wysyłanie fałszywych, ale przekonująco wyglądających e-maili do właścicieli portfeli z prośbą o podanie ich danych uwierzytelniających.

Dziękuję
i
zapraszam na Q & A

Mariola Więckowska

Mariola.Wieckowska@LexDigital.pl

m. +48 601 77 77 90
LinkedIn: https://www.linkedin.com/in/mariolawieckowska