

Bezpieczna organizacja to świadomi ludzie i kontrolowane dane

18.09.2025 ARCUS Secure Day 2025 • Edukacja
i technologia w służbie cyberodporności ✨

Dorota Semik-Szczurak, Bakotech



Nowa rzeczywistość zagrożeń

Praca hybrydowa zmieniła wszystko

Cyfrowa transformacja i rozproszony model pracy dramatycznie powiększyły powierzchnię ataku. Dane podróżują między biurem, chmurą i domowymi urządzeniami pracowników.

- ❌ 60% naruszeń danych wynika z błędu ludzkiego - to nie technologia zawodzi, lecz świadomość



Skala problemu w liczbach



60%

naruszeń bezpieczeństwa miało związek z czynnikiem ludzkim, takim jak błędy użytkowników, nieostrożność czy manipulacje socjotechniczne (Verizon 2025 DBIR)



99%

nie zablokowanych zagrożeń emailowych to ataki socjotechniczne lub phishingowe linki (Fortra 2025 Email Threat Intelligence Report)



10%

użytkowników klika w linki (według GPT z 2024 roku), a 6,5% podaje swoje dane logowania



45%

pracowników nie otrzymało żadnego szkolenia z zakresu bezpieczeństwa od pracodawców (Keepnet Labs, 2024 Security Awareness Training Statistics)

Podstawowy problem w zakresie bezpieczeństwa: ludzie i dane.

Musisz zapewnić bezpieczeństwo bez
wpływu na wydajność.



Świadomość użytkowników: Pierwsza linia obrony

Pracownicy to najsłabsze ogniwo, ale także najsilniejszy punkt obrony. Skuteczność organizacji zależy od tego, czy jej ludzie potrafią rozpoznać zagrożenie i odpowiednio zareagować.

→ Ciągłe, angażujące szkolenia

Nie jednorazowe webinary, lecz systematyczne budowanie nawyków bezpieczeństwa

→ Symulacje ataków phishingowych

Regularne testy w bezpiecznym środowisku wzmacniają czujność

→ Kultura zgłaszania incydentów

Pracownicy muszą czuć się bezpiecznie, zgłaszając podejrzone sytuacje



Terranova Security: Skuteczne budowanie świadomości



Dane pod kontrolą w świecie hybrydowym

Wyzwania ochrony danych w pracy rozproszonej

Mobilność danych

Informacje przemieszczają się między urządzeniami, chmurą i sieciami domowymi

Shadow IT

Nieautoryzowane aplikacje i usługi zwiększają ryzyko wycieków

Błędne udostępnienia

Przypadkowe wysłanie wrażliwych danych niewłaściwym odbiorcom

Regulacje i zgodność



NIS2, DORA, RODO

Nowe i rozszerzone ramy prawne wymuszają ścisłą kontrolę nad danymi osobowymi, procesami biznesowymi i infrastrukturą krytyczną.



Rosnące kary finansowe

Naruszenia przepisów mogą skutkować karami sięgającymi 4% globalnego obrotu oraz długotrwałymi szkodami reputacyjnymi.



Audytowalność procesów

Raportowanie incydentów i dokumentacja zgodności stają się obowiązkiem prawnym, nie opcjonalnym elementem strategii.



Wsparcie technologiczne

Terranova (świadomość bezpieczeństwa) i Digital Guardian (DLP) zapewniają kompleksowe wsparcie zgodności z wymogami regulatorów.

Digital Guardian: Kompleksowa ochrona danych



Dane w ruchu

Monitorowanie i kontrola transferu informacji przez email, komunikatory i aplikacje chmurowe



Dane w spoczynku

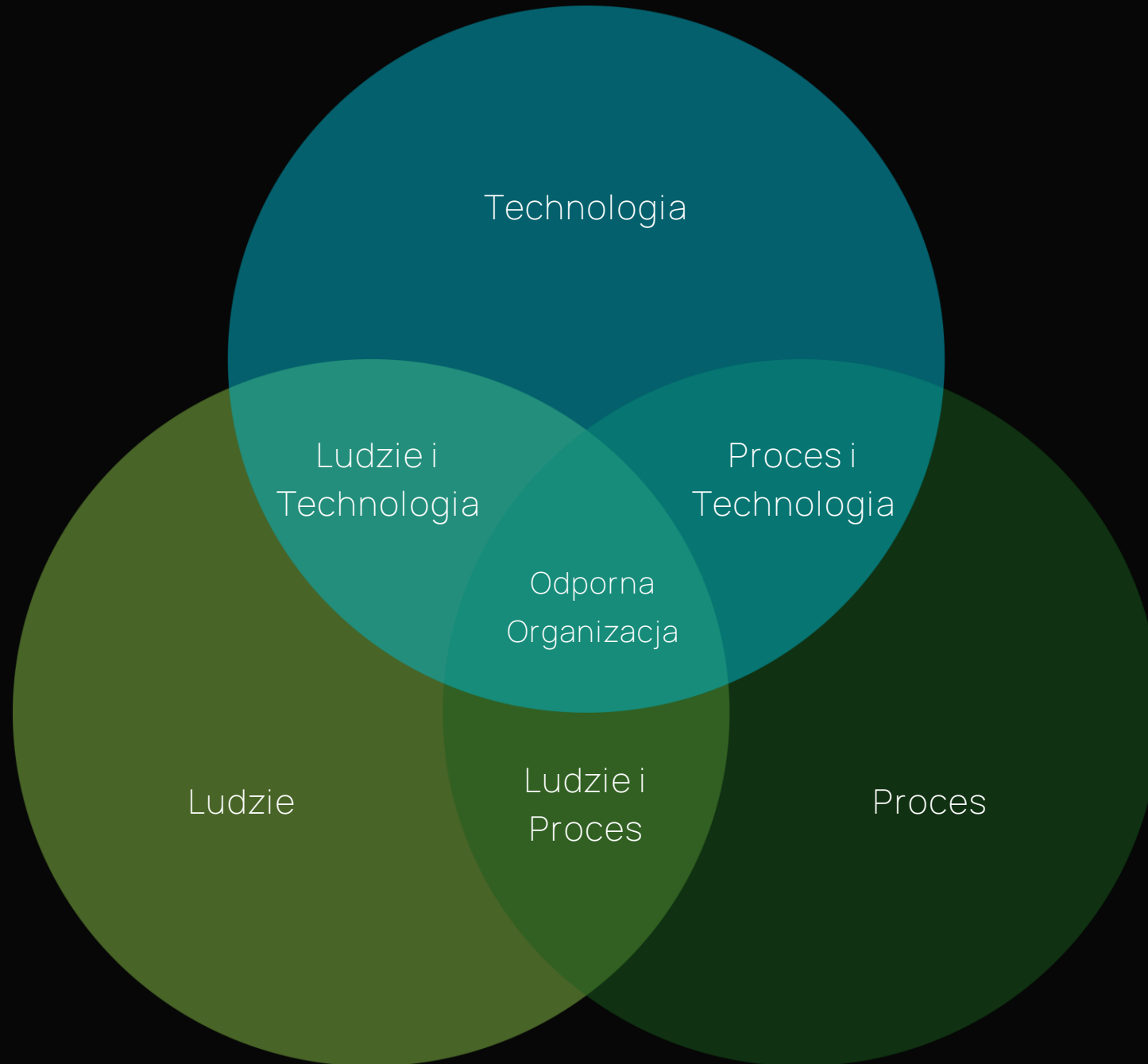
Ochrona plików przechowywanych na serwerach, w chmurze i na urządzeniach końcowych



Dane w użyciu

Kontrola aktywności użytkowników podczas pracy z wrażliwymi informacjami

Digital Guardian zapewnia pełną widoczność i kontrolę nad danymi organizacji, niezależnie od lokalizacji pracowników.



Podsumowanie



Świadomość = Pierwsza linia obrony

Inwestycja w edukację swoich pracowników



Dane pod kontrolą = Stabilność

Wdrożenie skutecznego systemu DLP



Integracja = Odporność

Holistyczne podejście do bezpieczeństwa



FORTRA **bako tech**[®]

Dziękuję!

Fortra@bakotech.com

