CYBERBEZPIECZEŃSTWO JAKO POSTAWA ORGANIZACYJNA – TECHNOLOGIA TO NIE WSZYSTKO

ARCUS SECURE DAY 2.0

Między regulacją a reputacją – nowa era cyberzarządzania

ZRÓWNOWAŻONY ROZWÓJ

Działania związane z cyberbezpieczeństwem powinny być prowadzone jednocześnie w trzech obszarach:

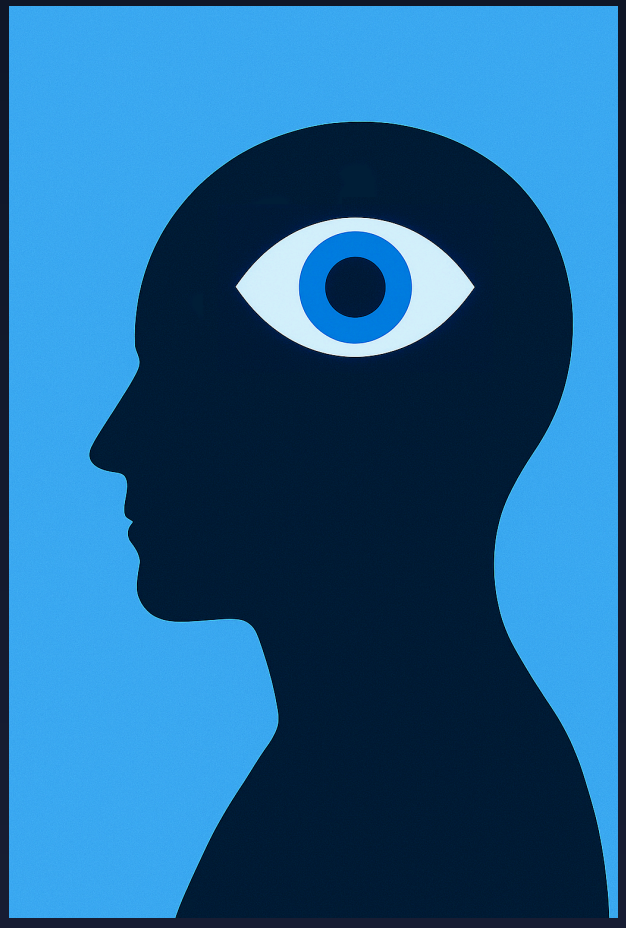
1. Obszar technologiczny
2. Obszar organizacyjny
3. Obszar kompetencyjny

ZRÓWNOWAŻONY ROZWÓJ

Działania związane z cyberbezpieczeństwem powinny być prowadzone jednocześnie w trzech obszarach:

1. Obszar kompetencyjny
2. Obszar organizacyjny
3. Obszar technologiczny

OBSZAR KOMPETENCJI



Świadomość

Wiedza

Zastosowanie

Inbox

You're a lucky winner!

Congratulations! You've won 1 Bitcoin!

CASE - FAKTURA OD SZEFA

OBSZAR ORGANIZACJI

REGULACJE PRAWNE - NIS2

Artykuł 21

Środki zarządzania ryzykiem w cyberbezpieczeństwie

1. Państwa członkowskie zapewniają, aby podmioty kluczowe i ważne wprowadzały odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu.

NORMY - ISO 27001

4.4 System zarządzania bezpieczeństwem informacji

Organizacja powinna ustanowić, wdrożyć, utrzymywać i ciągle doskonalić system zarządzania bezpieczeństwem informacji, w tym niezbędne procesy i ich wzajemne oddziaływania, zgodnie z wymaganiami niniejszego dokumentu.

OBSZAR ORGANIZACJI

ANALIZA RYZYKA

SAMODOSKONALENIE (PDCA - PLAN, DO, CHECK, ACT)

OBSZAR ORGANIZACJI

ANALIZA RYZYKA

Co chcemy chronić? - Zasoby informacyjne

Przed czym? - Ryzyka

W jaki sposób? - Plan postępowania z ryzykiem

OBSZAR ORGANIZACJI

SAMODOSKONALENIE

PDCA - Plan, Do, Check, Act (Planuj, działaj, sprawdzaj, wprowadzaj zmiany)

Zmieniające się otoczenie organizacji - legislacja, zagrożenia

Zmieniająca się organizacja - nowe produkty, usługi, procesy

Incydenty - analiza przyczyn, działania korygujące

PODSUMOWANIE

1. Budowanie kompetencji
2. Analiza ryzyka przed inwestycjami w technologię
3. Samodoskonalenie organizacji jako powtarzalny proces

DZIĘKUJĘ ZA UWAGĘ