ENERGIA KOBIET

13.04.2022

Krzysztof Malesa, NSO

Microsoft

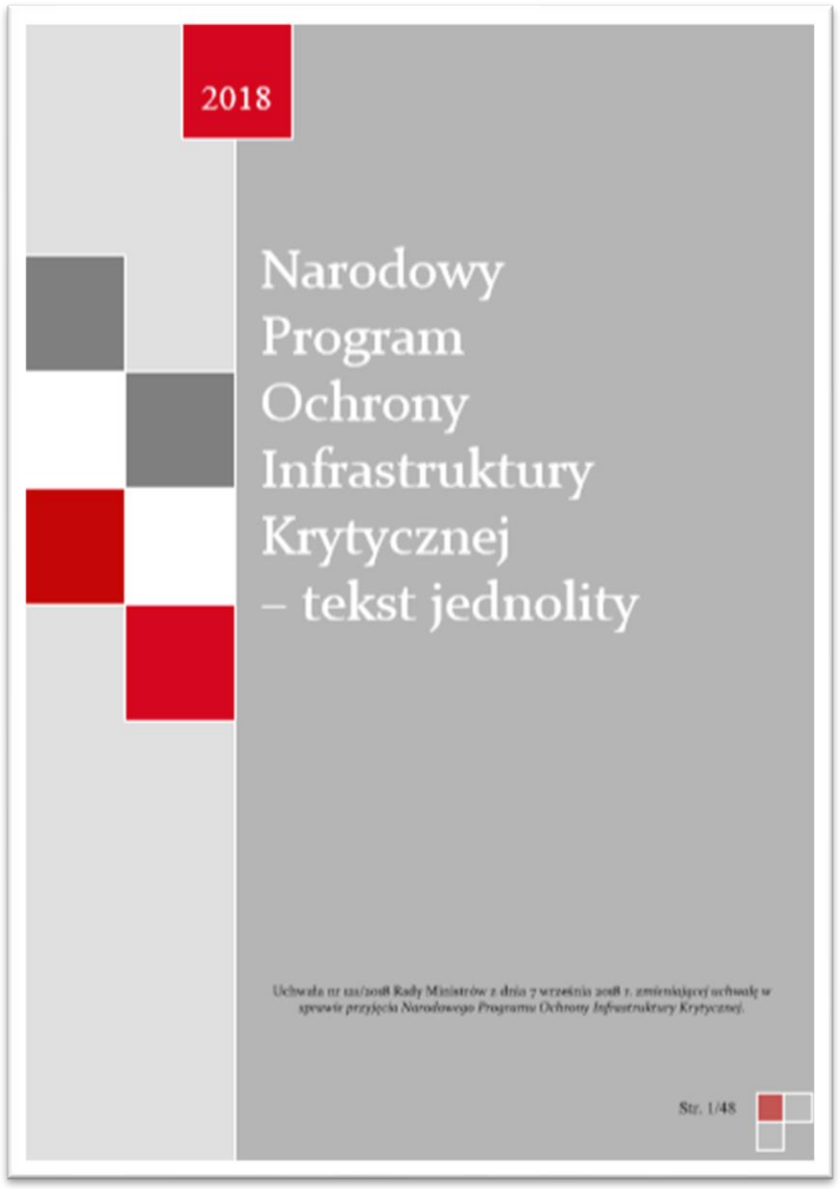
MILESTONE: 21.11.2013

SZCZYT NATO W WARSZAWIE: 8-9 LIPCA 2016

SZCZYT NATO W WARSZAWIE: 8-9 LIPCA 2016

SEVEN BASELINE REQUIREMENTS FOR RESILIENCE:

1. **ASSURED CONTINUITY OF GOVERNMENT AND CRITICAL GOVERNMENT SERVICES**: for instance the ability to make decisions, communicate them and enforce them in a crisis;
2. **RESILIENT ENERGY SUPPLIES**: back-up plans and power grids, internally and across borders;
3. **ABILITY TO DEAL EFFECTIVELY WITH UNCONTROLLED MOVEMENT OF PEOPLE**, and to de-conflict these movements from NATO's military deployments;
4. **RESILIENT FOOD AND WATER RESOURCES**: ensuring these supplies are safe from disruption or sabotage;
5. **ABILITY TO DEAL WITH MASS CASUALTIES**: ensuring that civilian health systems can cope and that sufficient medical supplies are stocked and secure;
6. **RESILIENT CIVIL COMMUNICATIONS SYSTEMS**: ensuring that telecommunications and cyber networks function even under crisis conditions, with sufficient back-up capacity; and
7. **RESILIENT TRANSPORT SYSTEMS**: ensuring that NATO forces can move across Alliance territory rapidly
and that civilian services can rely on transportation networks, even in a crisis.



SYSTEMY IK:

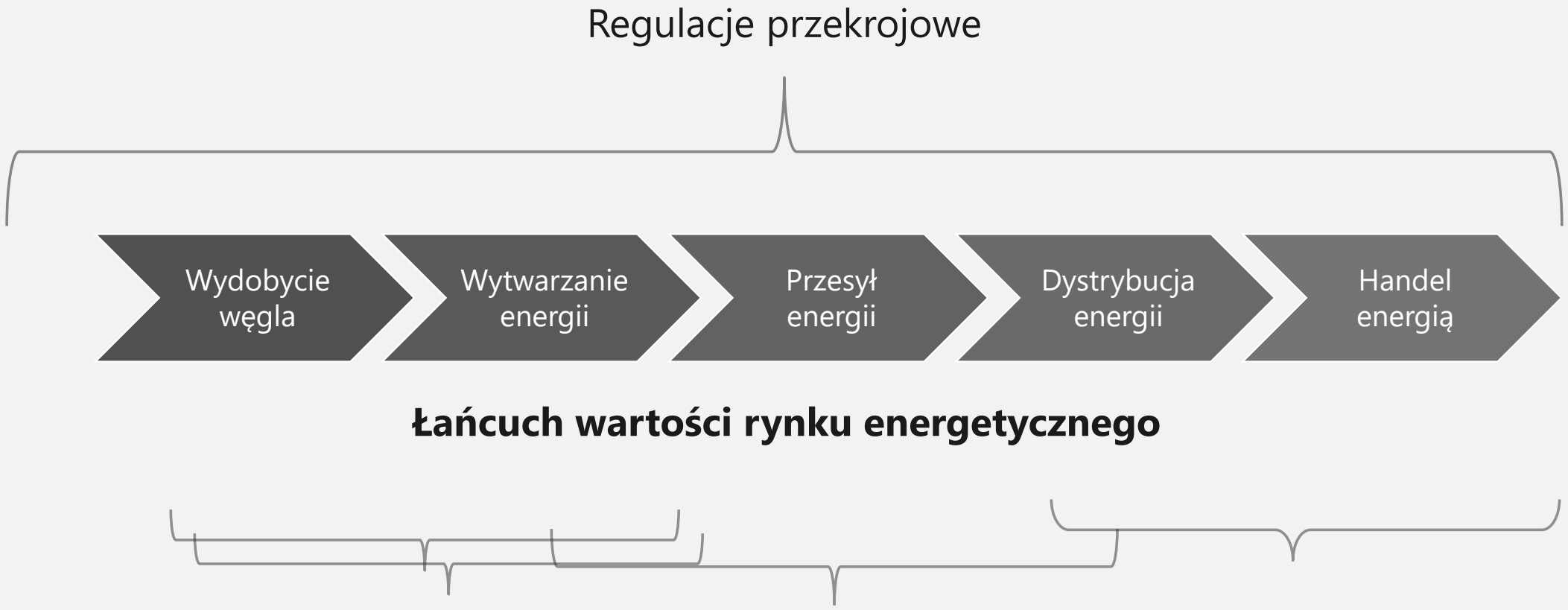
1. zaopatrzenia w energię, surowce energetyczne i paliwa
2. łączności
3. sieci teleinformatycznych
4. finansowe
5. zaopatrzenia w żywność
6. zaopatrzenia w wodę
7. ochrony zdrowia
8. transportowy
9. ratownicze
10. zapewniające ciągłość działania administracji publicznej
11. produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych

BEZPIECZEŃSTWO

Fizyczne	Osobowe	Techniczne
Teleinformatyczne	Prawne	Plany odbudowy

+ LUDZIE / ORGANIZACJA /TECHNOLOGIA

RAMY PRAWNE DLA USŁUG CYFROWYCH



RAMY PRAWNE DLA USŁUG CYFROWYCH – wybrane regulacje

Ustawa o zarządzaniu kryzysowym

- plany ochrony IK zatwierdzane przez RCB i uzgadniane przez MAP/MKiŚ
- Narodowy Program Ochrony Infrastruktury Krytycznej stanowiący wytyczne dla operatorów infrastruktury krytycznej

Ustawa o krajowym systemie cyberbezpieczeństwa

- rekomendacje organów właściwych dla operatorów usług kluczowych, w tym rekomendacje MKiŚ dla spółek energetycznych
- audyty, których wyniki udostępniane są organom właściwym / ABW / RCB

Ustawa o szczególnych uprawnieniach MAP i ich wykonywaniu w sektorze energii elektrycznej, ropy naftowej i paliw gazowych

- pełnomocnik ds. ochrony infrastruktury krytycznej – rekomendowanie rozwiązań Zarządowi
- "złote veto" dla MAP
- Uwaga: nie obejmuje OSD

Rekomendacje organu właściwego (Ministra Klimatu):

- zasady zapewnienia bezpieczeństwa informacji w chmurze obliczeniowej, dla operatorów usług kluczowych / infrastruktury krytycznej.

Krajowy Plan Odbudowy

- środki UE na transformację energetyczną (m. in. NABE)
- obligatoryjny standard chmury obliczeniowej dla nowych inwestycji finansowanych z europejskich instrumentów finansowych
- transformacja energetyczna = transformacja cyfrowa

Wspólna infrastruktura informatyczna państwa

- standardy cyberbezpieczeństwa chmur obliczeniowych
- tajemnica przedsiębiorstwa dopuszczona do przetwarzania w chmurze publicznej

UWAGA: w żadnym z powyższych dokumentów nie ma zapisów zabraniających chmury!

WSPÓŁDZIELONA ODPOWIEDZIALNOŚĆ

Odpowiedzialność Administratora

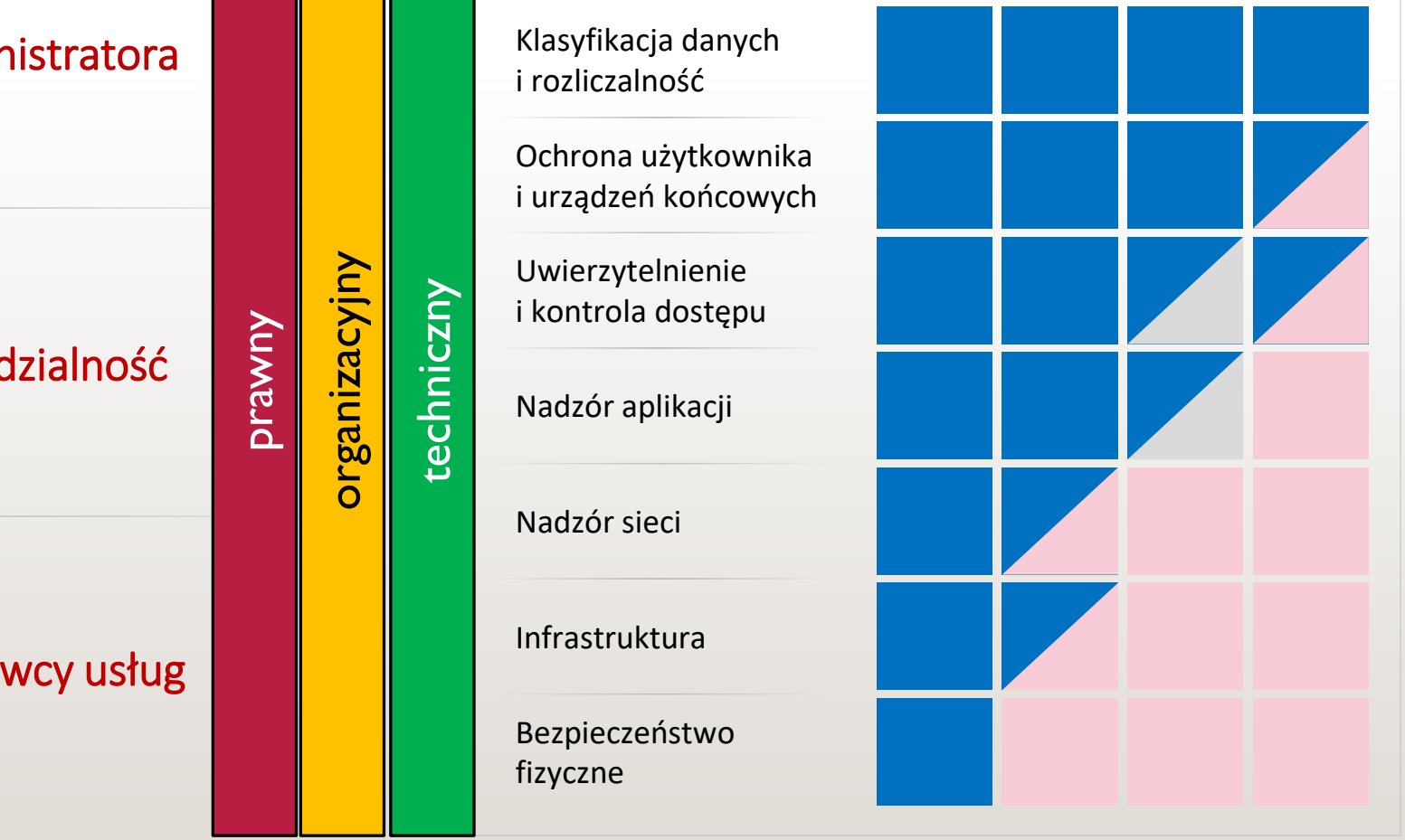
Współdzielona odpowiedzialność

Odpowiedzialność dostawcy usług

prawny

organizacyjny

techniczny



Microsoft

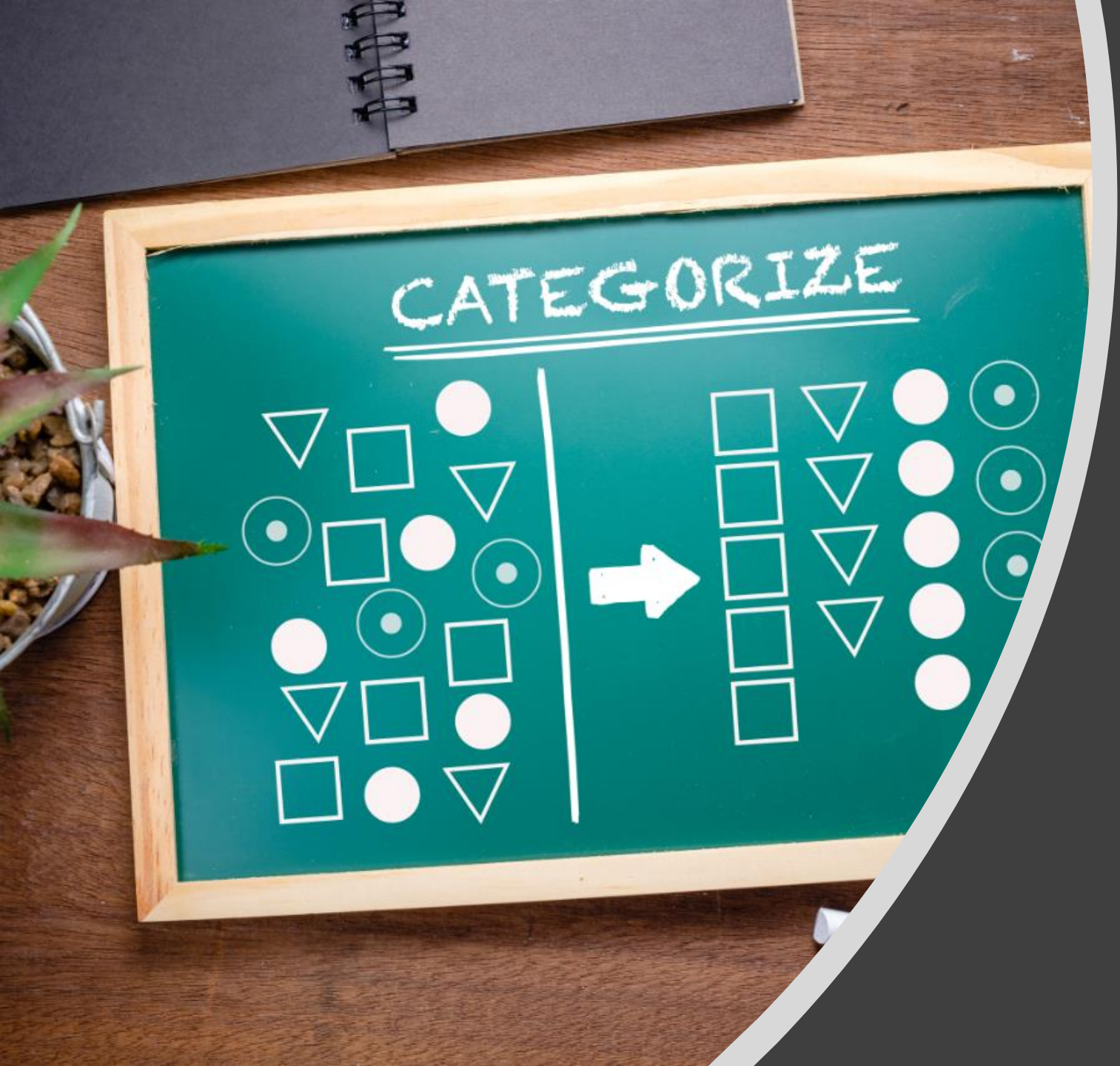
COMPLIANCE AS A SERVICE

Dzisiaj	A za chwilę…
RODO, Schrems II, standardowe klauzule umowne, lokalizacja danych, transfery danych, podmiot przetwarzający, komunikat KNF, normy ISO, długość łańcucha outsourcingowego, rodzaje szyfrowania, dostęp do danych, ciągłość biznesowa…	AI Act Digital Markets Act + Digital Services Act Digital Operational Resilience Act Dyrektywa NIS 2 Data Act (znane jako „rodo dla danych przemysłowych") Cybersecurity Act i certyfikaty ENISA Dyrektywa CER (Critical Entities Resilience) Standardy Gaia-X lub European Alliance for Data, Edge and Cloud Nowelizacja uksc, nowelizacja prawa bankowego…

Dostawca chmury W CENIE USŁUGI nieustannie utrzymuje zgodność z wymogami

BEZPIECZEŃSTWO INFRASTRUKTURY KRYTYCZNEJ W SYTUACJI NARASTAJĄCEGO ZAGROŻENIA KONFLIKTEM ZBROJNYM

OBSZAR BEZPIECZEŃSTWA	RYZYKA PRZED 24.02	NOWE, DODATKOWE RYZYKA
FIZYCZNE	• Kradzieże / wandalizm • Protesty ekologów • Terroryzm	• Atak kinetyczny / zniszczenie infrastruktury • Siłowe przejęcie / zniszczenie mienia • Utrata kontroli nad częścią terytorium kraju
OSOBOWE	• Wyciek informacji • Zemsta skonfliktowanego pracownika • Radykalizacja / szantaż / zwerbowanie pracownika	• Sabotaż od wewnątrz, w tym skierowany na IT • Pozyskanie danych od kluczowego personelu • Utrata kluczowego personelu (mobilizacja, również w zewnętrznych firmach)
PRAWNE	• Wrogie przejęcie • Utrudnianie działania na rynku • Vendor lock	• Nacjonalizacja majątku • Zrywanie kontraktów • Problemy z płatnościami
TECHNICZNE	• Pożary / klęski żywiołowe • Awarie energetyczne • Awarie techniczne	• Ograniczenia w dostawach prądu • Niedostępność Internetu i GSM • Reglamentacja paliw (agregaty prądotwórcze!)
TELEINFORMATYCZNE	• Podatności w systemach SCADA • Braki w świadomości / cyberhigienie • Architektura podatna na ataki	• Kampanie malware (wiper, ataki na SCADA) • Blokada usług kluczowych (energetyka, rejestry państwowe, usługi finansowe) • Niedostępność sprzętu/części na rynku
CIĄGŁOŚĆ DZIAŁANIA	• Niska świadomość / dojrzałość organizacji • Błędne wdrożenie BCM – nieakceptowalny RTO I RPO	• Długotrwałe zerwanie łańcucha dostaw • Brak lub nieadekwatność rozwiązań i zasobów pozwalających na utrzymanie RTO i RPO



Sztuczna inteligencja w bezpieczeństwie

Arystoteles (III w. p.n.e.)

Twórca “ładu wśród pojęć”

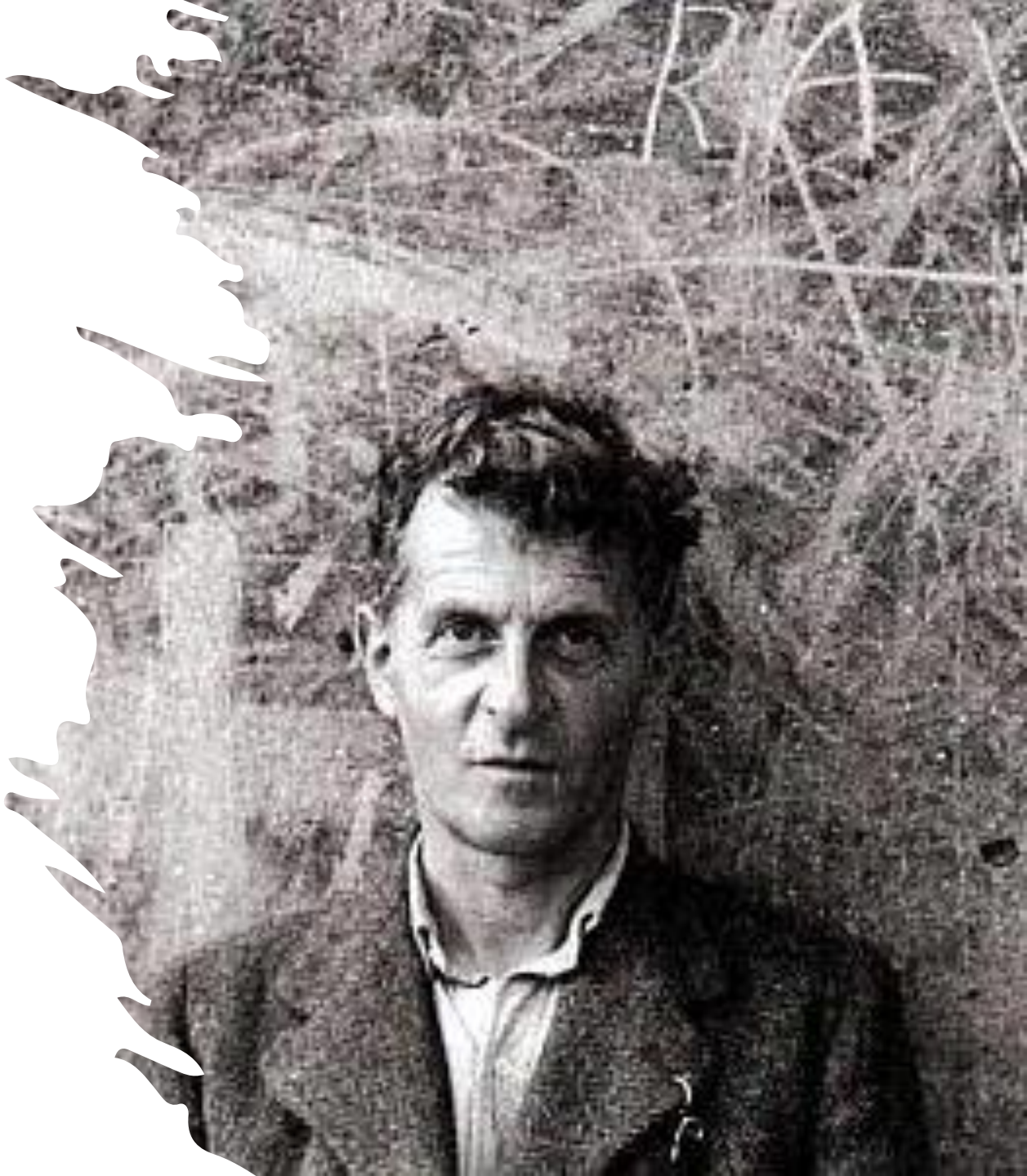
ZAŁOŻENIA DO OPISU RZECZYWISTOŚCI

- kategorie mają ostre granice
- każdy obiekt należy tylko do jednej kategorii
- przynależność do kategorii na zasadzie prawa wyłączonego środka (*tertium non datur*)
- wszystkie obiekty w kategorii mają równy status

Definicyjny model kategoryzacji ze względu na warunki konieczne i wystarczające (WKW)

XX wiek:

rewolucja w opisie rzeczywistości, destrukcja modelu WKW



Ludwig Wittgenstein:

„Co jest wspólnego dla obiektów w danej kategorii? Nie ma jednej cechy wspólnej dla wszystkich - widzimy skomplikowaną siatkę zachodzących na siebie i krzyżujących się podobieństw; podobieństw w skali dużej i małej”.

AI I ML W SŁUŻBIE BEZPIECZEŃSTWU

- Wykrywanie anomalii
- Skanowanie zabezpieczeń
- Uwierzytelnianie kontekstowe
- Automatyzacja reagowania na incydenty
- Odpieranie zautomatyzowanych ataków
- Wykrywanie malware
- Ochrona przed phishingiem
- Analiza behawioralna
- Automatyczna kategoryzacja informacji

REDEFINICJA CYBERBEZPIECZEŃSTWA?

OBSZAR BEZPIECZEŃSTWA	PRZYKŁADOWE ROZWIĄZANIE OGRANICZAJĄCE RYZYKO
FIZYCZNE	• Analiza behawioralna zapisu z kamer • Reduplikacja danych w oddalonej lokalizacji
OSOBOWE	• Systemy ochrony tożsamości • Zarządzanie uprawnieniami
PRAWNE	• Analizy biznesowe w AI • Analiza tekstów kontraktów – wyszukiwanie niebezpiecznych zapisów
TECHNICZNE	• Optymalizacja procesów przez edge computing • Rekonfiguracja usług chmurowych • Alternatywne połączenie z data centers (światłowód, satelita)
TELEINFORMATYCZNE	• Rozwiązania IT do ochrony sieci, urządzeń, infrastruktury, danych, aplikacji i tożsamości
CIĄGŁOŚĆ DZIAŁANIA	• Wsparcie AI dla planowania BCM • Automatyzacja zarządzania incydentami

Microsoft

Dziękuję!

Krzysztof Malesa
kmalesa@microsoft.com
linkedin.com/in/krzysztofmalesa