Konferencja

LEKSYKON CYBERBEZPIECZEŃSTWA

Warszawa, 31 lipca 2020 r., godz. 10.00-13.00

Platforma komunikacyjna PTI - MS Teams PTI

Zarządzanie ryzykiem standardy i regulacje

Ewa Marzec Katedra Prawa Informatycznego WPiA UKSW

RYZYKO wybrane definicje

- Wg. IEC 61508 ***Ryzyko*** *jest miarą stopnia zagrożenia , wyrażającą zarówno stopień szkodliwości jak i prawdopodobieństwo jego wystąpienia.*
- PN-EN ISO 9000:2015-10 określa **ryzyko** jako wpływ niepewności.
- **Ryzyko operacyjne** – ryzyko straty wynikającej z niedostosowania lub zawodności wewnętrznych procesów ludzi i systemów technicznych lub ze zdarzeń zewnętrznych (rekomendacja M/2004, KNB).

Definicja ryzyka wg. PN-ISO/IEC-27005:2014

Ryzyko w bezpieczeństwie informacji jest związane z potencjalną sytuacją, w której określone zagrożenie wykorzysta podatność aktywów powodując w ten sposób szkodę dla organizacji.

Ryzyko mierzone jest jako kombinacja prawdopodobieństwa zdarzenia i jego następstw.

Definicja ryzyka wg. PN-ISO 31000:2018

Ryzyko to skutek niepewności w odniesieniu do ustalonych celów (wpływ niepewności na cele).

Zarządzanie ryzykiem to skoordynowane działania dotyczące kierowania i nadzorowania organizacji w odniesieniu do ryzyka.

Porównanie ISO 27005 i ISO 31000

Definicja ryzyka w bezpieczeństwie informacji z ISO 27005

- Potencjalna sytuacja, w której określone **zagrożenie** wykorzysta **podatność** aktywów lub grupy aktywów powodując w ten sposób **szkodę** dla organizacji

NEGATYWNE

Różnica

Definicja ryzyka z ISO 31000

- **Wpływ niepewności na cele**

NEUTRALNE

- **Zarządzanie ryzykiem** to systematyczne stosowanie polityki procedur i praktyk zarządzania do zadań ustalania kontekstu ryzyka, jego identyfikowania, analizowania wyznaczania, postępowania z ryzykiem oraz monitorowania i komunikowania ryzyka za PN 62198
- **Zarządzanie ryzykiem** to skoordynowane działania dotyczące kierowania i nadzorowania organizacji w odniesieniu do ryzyka za ISO 27005

Pojęcie ryzyka i zarządzanie ryzykiem w regulacjach prawnych

- Krajowe Ramy Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych Dz.U.2017.2247 t.j. z dnia 2017.12.0
- Rozporządzenie Prezesa Rady Ministrów Podstawowe wymagania bezpieczeństwa teleinformatycznego. Dz.U.2011.159.948 z dnia 2011.08.01
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa Dz.U.2018.1560 z dnia 2018.08.13
- Dyrektywa Parlamentu Europejskiego I Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Dz.U.UE.L.2016.194.1 z dnia 2016.07.19

Dziękuję za uwagę.