Konferencja

LEKSYKON CYBERBEZPIECZEŃSTWA

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

Platforma komunikacyjna PTI - MS Teams PTI

Bezpieczeństwo informacji jako pojęcie z zakresu cyberbezpieczeństwa

Dr inż. Krzysztof Świtała

Cyberprzestrzeń

- Art. 2 ust. 1b ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej stanowi, że przez cyberprzestrzeń rozumie się **przestrzeń przetwarzania** i wymiany **informacji** tworzoną przez **systemy teleinformatyczne**, określone w art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, wraz z powiązaniami pomiędzy nimi oraz relacjami z **użytkownikami**

Zgodnie z art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne system teleinformatyczny to zespół współpracujących ze sobą **urządzeń** informatycznych (ang. hardware) i **oprogramowania** (ang. software) zapewniający **przetwarzanie**, przechowywanie, a także wysyłanie i odbieranie **danych** (ang. content) przez **sieci telekomunikacyjne** za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy - Prawo telekomunikacyjne.

Regulacje prawne odnoszące się do problematyki cyberbezpieczeństwa

- **Cyberbezpieczeństwo** (art. 2 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa – UKSC) to odporność **systemów informacyjnych** na działania naruszające **poufność, integralność, dostępność** i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;
  - Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa stanowi wdrożenie Dyrektywy 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 (NIS):
    - Podstawowym celem niniejszej dyrektywy jest osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii, aby poprawić funkcjonowanie rynku wewnętrznego.
    - Wspomniany akt prawa UE nie odnosi się do obowiązków podmiotów publicznych - w tym jednostek samorządu terytorialnego.
- **Bezpieczeństwo sieci i systemów informatycznych** (art. 4 pkt 2 dyrektywy NIS) - oznacza odporność sieci i systemów informatycznych, przy danym poziomie **zaufania**, na wszelkie działania naruszające **dostępność,** autentyczność, **integralność lub poufność** przechowywanych lub przekazywanych, lub przetwarzanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne;

Regulacje prawne odnoszące się do problematyki cyberbezpieczeństwa

- **Cyberbezpieczeństwo** (art. 2 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa – UKSC) to odporność **systemów informacyjnych** na działania naruszające **poufność, integralność, dostępność** i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;
  - Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa stanowi wdrożenie Dyrektywy 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 (NIS):
    - Podstawowym celem niniejszej dyrektywy jest osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii, aby poprawić funkcjonowanie rynku wewnętrznego.
    - Wspomniany akt prawa UE nie odnosi się do obowiązków podmiotów publicznych - w tym jednostek samorządu terytorialnego.
- **Bezpieczeństwo sieci i systemów informatycznych** (art. 4 pkt 2 dyrektywy NIS) - oznacza odporność sieci i systemów informatycznych, przy danym poziomie **zaufania**, na wszelkie działania naruszające **dostępność,** autentyczność, **integralność lub poufność** przechowywanych lub przekazywanych, lub przetwarzanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne;

ISO 27032 - standard dotyczący wytycznych w zakresie bezpieczeństwa w cyberprzestrzeni

- Cyberbezpieczeństwo wg ISO 27032 to zachowanie **poufności, integralności i dostępności** informacji w cyberprzestrzeni, czyli złożonym środowisku obejmującym interakcje ludzi, oprogramowania i usług w Internecie za pomocą urządzeń technicznych i sieci z nim połączonych, które nie istnieją w fizycznej postaci.

ISO 27000 - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Przegląd i terminologia

- **Bezpieczeństwo informacji** (ISO 27000 - Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Przegląd i terminologia) – zachowanie **poufności, integralności i dostępności informacji**; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Normy z zakresu bezpieczeństwa informacji

- ISO/IEC 27000 – Fundamentals and vocabulary – norma zawiera podstawowe zasady, koncepcje i słownictwo wykorzystywane w standardach serii 27000.
- ISO/IEC 27001 – Specification for an Information Security Management System – norma określa wymagania dla budowy i funkcjonowania systemów zarządzania bezpieczeństwem informacji.\
- ISO/IEC 27002 – Code of Practice for Information Security Management – norma zawiera wytyczne do budowy systemów zarządzania bezpieczeństwem informacji.
- ISO/IEC 27003 – Information security management system implementation guidance – norma zawiera wytyczne do budowy systemów zarządzania bezpieczeństwem informacji pomocne przy ich wdrożeniu.
- ISO/IEC 27004 – Information security management measurements – norma dotyczy opomiarowania zarówno procesów zarządzania bezpieczeństwem jak i poszczególnych zabezpieczeń funkcjonujących w ramach systemów zarządzania bezpieczeństwem informacji.
- ISO/IEC 27005 – Information security risk management – norma zawierać będzie wytyczne dla procesu zarządzania ryzykiem. Przewiduje się, iż będzie ona oparta o wydany w 2006 roku brytyjski standard BS 7799-3. Wydanie oficjalnej wersji planowane jest na rok 2009.
- ISO/IEC 27006 – Requirements for bodies providing audit and certification of information security management systems – norma określa wymagania dla jednostek przeprowadzających audyty certyfikacyjne systemów zarządzania bezpieczeństwem informacji.
- ISO/IEC 27007 – Guidelines for Information security management systems auditing – norma definiuje dobre praktyki dla przeprowadzania audytów wewnętrznych i certyfikacyjnych systemów zarządzania bezpieczeństwem informacji.
- ISO/IEC 27011 – Information security management guidelines for telecommunications – norma stanowi rozszerzenie ISO 27001/27002 o dobre praktyki dla przemysłu telekomunikacyjnego.
- ISO/IEC 27031 – ICT readiness for business continuity – standard dotyczy ciągłości działania.
- ISO/IEC 27032 – Guidelines for cybersecurity – standard dotyczący wytycznych w zakresie bezpieczeństwa w Internecie.
- ISO/IEC 27033 – IT network security – jest to standard dotyczący bezpieczeństwa sieci teleinformatycznych.
- ISO/IEC 27034 – Guidelines for application security – standard bezpieczeństwa dla aplikacji.
- ISO/IEC 27799 – Security Management in Heath – wersja ISO 27002 dedykowana dla sektora medycznego.

Dziękuję za uwagę