ECONSEC
Technical Security Forum
2017

26 WRZEŚNIA 2017
Warszawa, Hotel Marriott

BEZPIECZEŃSTWO INFRASTRUKTURY PRZEMYSŁOWEJ I ENERGETYCZNEJ – ASPEKTY PRAWNE I TECHNOLOGICZNE. ROLA MECHANIZMÓW SZTUCZNEJ INTELIGENCJI

Sesja I: System ochrony prawnej

- Prawe aspekty cyberbezpieczeństwa i ochrony danych
- Sektor ubezpieczeń wobec problemu cyber zagrożeń – gotowość, zakres, odpowiedzialność itd.
- Odpowiedzialność za bezpieczeństwo w organizacji – jak minimalizować osobiste ryzyko w świetle obecnych przepisów
- Odpowiedzialność za bezpieczeństwo instalacji przemysłowych i przesyłowych w odniesieniu do Rozporządzenia UE o Ochronie Danych Osobowych (RODO)
- Dyrektywa NIS
- Cybercompliance i jak je wdrażać
- Krajowy System Cyberbezpieczeństwa
- Odpowiedzialność za wdrożenie zaleceń w obszarze bezpieczeństwa IT (ICS, OT) – kto ma za to odpowiadać w firmie
- Teoria czy praktyka – skuteczność strategii cyberbezpieczeństwa w firmie.
- Procedury po cyberataku
- Bezpieczeństwo danych w relacjach między spółkami Grupy Kapitałowej
- Zastosowanie mechanizmów AI (Artificial Intelligence)sposobem na zahamowanie rosnącej fali zagrożeń?

Sesja II: Zabezpieczenie infrastruktury krytycznej i przemysłowej - zaawansowane technologie z zakresu „cyber security" i AI

- Ataki na infrastrukturę krytyczną - bezpieczeństwo w sektorze utilities
- Mechanizmy sztucznej inteligencji jako narzędzie do zwiększenia bezpieczeństwa systemów IT
- Usługa Watson for Cybersecurity, biblioteki API, Content Moderator, Custom Image Recognition Service – mechanizmy inteligentnego wykrywania zagrożeń
- Konta uprzywilejowane sposób na hakerów.
- Znaczenie cyberbezpieczeństwa w procesach produkcyjnych
- Wzmocnienia bezpieczeństwa urządzeń i rozwiązań systemów sterowania przemysłowego (ICS, OT).
- Jak skutecznie wykryć naruszenia bezpieczeństwa
- Narzędzia w rękach cyberprzestępców: kradzież tożsamości, phishing
- e-transakcje jak skutecznie zabezpieczyć przed zagrożeniami
- Czynnik ludzki i czynnik finansowy – ich wpływ na cybersecurity w przemyśle i utilities
- Czy warto multiplikować systemy bezpieczeństwa
- Aspekty cyber w strategii firmy – budowanie świadomości problemu wśród kadry zarządzającej
- Security Operation Center – model zintegrowanego systemu bezpieczeństwa w firmie

Sesja III: Aspekty organizacyjne i techniczne wdrożenia systemu zabezpieczeń – studium przypadku

- Jak zorganizować system bezpieczeństwa w przedsiębiorstwie.
- Uczmy się na błędach –przykłady ataków, incydentów i naruszenia bezpieczeństwa
- SCADA – klucz do bezpieczeństwa?
- Znaczenie cyberbezpieczeństwa w procesach produkcyjnych i przemysłowych
- Bezpieczeństwo OT oraz IT w organizacji
- Bezpieczeństwo aplikacji mobilnych w biznesie
- Systemy cybersecurity – inteligentne czy innowacyjne

* Organizator zastrzega sobie prawo korekty programu z przyczyn merytorycznych