ACCADEMIA DEI SERVIZI PUBBLICI

Corso di Formazione

"Come impostare un programma di Cyber Security organico, alla luce delle recenti evoluzioni normative e di contesto" *(COD.20.022)*

15-16 giugno 2020

Contesto

La trasformazione digitale e la progressiva integrazione delle tecnologie informatiche in sistemi tradizionalmente "chiusi", come gli impianti industriali, rendono le aziende sempre più esposte al rischio di attacchi cyber finalizzati alla sottrazione di informazioni sensibili o alla interruzione dei servizi erogati. Il livello di esposizione è tale che anche a livello normativo si stanno prevedendo degli specifici obblighi per le organizzazioni. Nella sessione si forniranno gli strumenti per sviluppare un programma di cyber security efficace, che consenta di identificare e mettere in atto le misure necessarie a ricondurre il rischio ad un livello accettabile per l'azienda anche a fronte del nuovo scenario che si apre alle aziende a seguito del COVID-19.

Obiettivi

- Comprendere l'attuale scenario della Cyber Security.
- Condividere i principali elementi teorici e strategici in materia.
- Conoscere i riferimenti per rendere possibili approfondimenti in autonomia.
- Fornire gli elementi per valutare consapevolmente le esigenze della propria realtà anche a fronte del nuovo scenario post COVID-19
- Condividere i principi di valutazione e governo della Cyber Security.

Destinatari

- IT
- CTO
- Resp. Sicurezza
- CISO

Durata e modalità di svolgimento

Il corso di formazione della durata di **6 ore** si svolgerà **in due moduli di 3 ore** ciascuno, il **lunedì 15 giugno e martedì 16 giugno** a partire dalle ore 10.00 in video-conferenza con la piattaforma Zoom; il link con password sarà fornito a tutti gli iscritti con mail individuale.

Di seguito il programma dettagliato.

Programma dettagliato

Lunedì 15 giugno 10.00 – 13.00

LA CYBER SECURITY OGGI

- Il contesto e le sue peculiarità
  - *L'evoluzione digitale e le implicazioni in termini di Cyber Security*
  - *Gli avvenimenti recenti e il panorama delle minacce odierne: tipologie di attacchi e di attaccanti*
  - *Lo scenario Covid-19 e gli impatti sul contesto odierno*
  - *Cosa significano IT/ICT Security, Information Security, Cyber Security, OT/Industrial Security*
  - *Strategicità delle informazioni sensibili e garanzia della continuità operativa: 2 temi ad alta priorità per utility*

- Strategie in materia di Cyber Security
  - *Le evoluzioni delle normative nazionali e internazionali: dalle Infrastrutture Critiche al Perimetro Cibernetico*
  - *Una panoramica degli standard internazionali, delle best practice e dei relativi attori:*
  - *ISO, NIST, ENISA*
  - *ISO 27001*
  - *NIST CSF*

Martedì 16 giugno 10.00 – 13.00

GOVERNARE LA CYBER SECURITY

- Cyber Security Risk Management
  - *I fondamenti del Cyber Risk: "minacce", "vulnerabilità", "impatti", relative metriche e tassonomie*
  - *Cosa significa gestire i rischi cyber secondo la ISO 31000 e la ISO 27005: dall'identificazione alle azioni di rimedio*
  - *L'esecuzione del Cyber Risk Assessment secondo 2 diversi approcci: qualitativo e quantitativo*
  - *Excursus sui principali rischi che interessano il "remote working"*

Pausa caffè

- Cyber Security Program and Strategy
  - *Gli elementi fondanti di programmi e strategie: persone, processi e tecnologie*
  - *La gestione della Cyber Security secondo una visione e un approccio olistico*
  - *I diversi gradi di maturità nella gestione di elementi organizzativi ed integrazione delle tecnologie*
- Q&A con i relatori

DOCENTI

Enrico Ferretti

Managing Director - È in Protiviti dal 2007 ed è responsabile in Italia della practice di Technology Consulting. In precedenza, Enrico ha maturato un'esperienza professionale di più di dieci anni in Accenture, dove ha collaborato con diversi operatori del settore delle telecomunicazioni per i servizi di IT Strategy & Governance, Cyber Security e Service Delivery and Assurance. Durante la sua esperienza professionale Enrico ha gestito numerosi progetti relativamente alle tematiche di: Information & Cyber Security, IT Strategy & Organization, Change Management a seguito di importanti evoluzioni dei sistemi informativi, Data Center Consolidation & Rationalization, IT Asset Management, IT Security & Risk Management, Service Delivery & Assurance, IT Assessment, Business Continuity & Crisis Management.

Gabriele Mandelli

Manager – È un manager della Service Line IT Consulting degli uffici Protiviti di Milano. Ha maturato esperienza significativa in progetti di Information/Cyber Security e Business Continuity in contesti multinazionali. Le principali esperienza riguardano le seguenti aree:
Information/Cyber Security: organizational security, security strategy, risk assessment & management, data classification & protection. Business Continuity: business impact analysis, risk assessment & management, strategie di BC, piani di BC, emergency & crisis management. Awareness & Training.
