Certificato n.1420.2022

WEBINAR

Cyber Security della rete informatica aziendale: soluzioni tecniche e obblighi di legge

Focus sulla gestione di un *data breach*

4 LUGLIO 2024 – ORE 9:30/13:30

E' un dato di fatto che gli attacchi informatici siano aumentati in maniera esponenziale, colpendo in diversi modi tutte le aziende, a prescindere da dimensioni e settore di competenza.

I rischi che ne derivano per l'integrità e la disponibilità non solo dei dati personali di cui l'azienda è titolare, ma più in generale di tutti i dati aziendali, possono essere molto elevati, potendo verificarsi anche il blocco della produzione fino a che non sia ripristinata la rete informatica aziendale.

Il webinar si propone di approfondire il tema della Cyber Security, per indicare, anche attraverso l'esame di casi pratici, misure/soluzioni tecniche per contrastare il rischio di attacchi informatici ed assicurare una corretta ed adeguata gestione dei dati informatici aziendali.

Saranno nel contempo oggetto di analisi anche gli obblighi di legge legati per lo più alla normativa a tutela dei dati personali, con uno specifico focus sulle modalità di gestione e notificazione di un data breach.

I partecipanti potranno interagire coi docenti, con domande/richieste di chiarimenti.

Destinatari

Il seminario è rivolto a Imprenditori, Legali rappresentanti, Direzione e Servizi di supporto IT/informatico, Direzione Legale, Data Protection Officers, Direzione e Uffici Qualità

Relatori

Paolo Sardena - Co-Fondatore di Intuity azienda specializzata in cyber security, dal 2020 parte del gruppo IMQ. Inizia ad occuparsi di sicurezza informatica nel 1999 esplorandone nel tempo tutte le sfumature, dagli aspetti tecnologici, di governance arrivando più recentemente a riconoscere nell'essere umano la più efficacie e sottovalutata, delle difese. Al momento ricopre il ruolo di Senior Security Advisor e Business Developer per IMQ Intuity.

Avv. Mattia Salerno - Associate Partner dello Studio Pirola Pennuto Zei e Associati, componente delle Practice Regulatory, Compliance & Data Protection e IT&IP. Ha maturato importanti esperienze nell'assistenza a gruppi multinazionali per consulenza in materia di protezione dei dati personali e nuove tecnologie. È DPO di diverse Società. Ha coordinato progetti per conto di organizzazioni complesse, finalizzati all'implementazione di programmi di compliance, sia a livello di gruppo, sia a livello locale.

Durata e modalità di svolgimento

4 luglio, dalle ore 9:30 alle ore 13:30, webinar.

Modalità e quota di iscrizione

1. Quota di partecipazione: Associato ANIE € 220,00+IVA – Non associato € 320,00+IVA

2. Iscrizione on-line

3. Pagamento: con carta di credito o con bonifico bancario.
   Per pagamento con bonifico bancario inviare copia del pagamento a
   formazione@anieservizintegrati.it e amministrazione@anieservizintegrati.it
   In mancanza dell'invio della distinta di pagamento, l'iscrizione non si perfeziona.

4. Successivamente saranno inviate le modalità di partecipazione al webinar

PROGRAMMA

09:30 **Cyber Security**: la rivoluzione digitale che la nostra società sta vivendo porta con sé vantaggi evidenti e rischi nascosti, uno di questi è la sicurezza informatica. Diamo uno sguardo a questo fenomeno per comprenderne le dinamiche e le proporzioni, capire dove siamo e dove stiamo andando.

Anatomia di un attacco informatico: esploriamo cosa succede quando un'azienda diventa obbiettivo di un attacco cyber, per comprendere quali sono i rischi concreti per il business.

Analisi di alcuni casi reali: cos'è successo e quali conseguenze ci sono state per l'azienda e per gli individui che la compongono.

Azioni di mitigazione: quali sono le principali azioni di mitigazione che possiamo introdurre, a breve, medio e lungo termine.

11:25 Pausa

11:35 **La normativa in materia di privacy: misure di sicurezza e Data breach**

- Framework normativo: il Regolamento Generale sulla protezione dei dati N. 2016/679, il D.lgs. 196/2003 come modificato dal D.lgs. 101/2018, i Provvedimenti del Garante Italiano e del Comitato Europeo per la protezione dei dati.
- Data Breach: definizione, disposizioni normative e standard di settore per la valutazione della severità della violazione.
- Gestione dei data breach: le azioni pratiche da porre in essere e le funzioni aziendali coinvolte.
- Prevenzione: cosa fare per prevenire i data breach e attenuarne gli effetti dannosi? Distinzione tra sicurezza informatica (misure tecniche) e sicurezza umana (misure organizzative).

La direttiva NIS 2: i nuovi assetti organizzativi della Cyber Security

- Framework normativo sulla cibersicurezza: cosa ci aspetta?
- La gestione dei rischi di cibersicurezza, l'attività di assessment, gli adempimenti in capo alle imprese e gli impatti sugli assetti organizzativi delle imprese.
- Il ruolo dell'Agenzia per la cybersicurezza nazionale e del Computer Security Incident Response Team "CSIRT" e gli obblighi di notifica degli incidenti informatici.
- I sistemi europei di certificazione della cibersicurezza.
- Controlli e sanzioni.

Analisi Casi pratici

13:30 Chiusura lavori