LA RESILIENZA OPERATIVA DIGITALE (DORA)

NEI SERVIZI FINANZIARI:

CULTURA, PREVENZIONE E MITIGAZIONE DEI RISCHI

14 e 15 febbraio 2023

Con la diffusione della digitalizzazione e dei servizi ad essa collegati i settori finanziario e fintech devono attrezzarsi e imparare a reagire tempestivamente alle minacce in continuo aumento di attacchi informatici.

Nel mese di dicembre scorso sono state pubblicate nella Gazzetta Ufficiale della UE:

- il **Regolamento DORA** *(Digital Operational Resilience Act)* **per la difesa unica europea** che ha l'obiettivo di disciplinare in maniera uniforme la "resilienza operativa" nel settore finanziario in tutta l'Europa.
- la **Direttiva DORA**
- ed anche la **NIS2**

Tali normative impatteranno con le loro regole sull'intero ecosistema finanziario a prescindere dalle dimensioni e dal fatturato delle aziende e dei loro fornitori. Nel processo di adeguamento alla cyber resilienza saranno coinvolti direttamente i vertici aziendali. La gestione del rischio, gli obblighi di segnalazione, l'esecuzione di test di resilienza e la condivisione di dati comporteranno obblighi più rigorosi e severi. Il focus della normativa riguarderà anche la gestione dei rischi ICT derivanti da terze parti e i fornitori sono direttamente coinvolti per il rispetto delle nuove disposizioni.

Banche, Assicurazioni, operatori fintech e gestori di crypto-asset e tutti i relativi fornitori ed outsourcer dovranno **adeguarsi ai nuovi requisiti entro dicembre 2024** e sarà fondamentale evitare ritardi. DORA accanto ad alcuni elementi di novità, quali la vigilanza centralizzata sui fornitori, armonizza una serie di adempimenti già previsti da altre normative. DORA prevede nei prossimi mesi l'emissione di numerosi documenti tecnici, ma grazie al fatto che a livello globale sono state emesse al di fuori dell'UE diverse altre normative sulla resilienza è possibile, già da ora, indirizzare correttamente gli opportuni adeguamenti.

Il corso, molto pratico e basato sul libro (in corso di pubblicazione) **Manuale di resilienza[1],** si prefigge non solo di presentare quali siano gli adempimenti previsti da DORA, ma anche i possibili riferimenti (normativi, framework, buone pratiche…) utilizzabili per una corretta implementazione.

[PROGRAMMA]

(*) Ore 8.45 prova collegamento – ore 9.00 apertura dei lavori

La resilienza operativa nella normativa e la sua evoluzione

- Dalla continuità operativa alla resilienza operativa, differenze e sinergie
- L'iter legislativo di DORA, la strutturazione della norma, gli RTS
- Il perimetro di applicazione della normativa
- Le normative sulla resilienza al di fuori della UE

I pillar di DORA: analisi degli impatti e alcune utili indicazioni operative

- La gestione dei rischi informatici
  - I framework di sicurezza
  - Le analisi dei rischi
  - Le misure di sicurezza
  - Le metriche per valutare efficienza ed efficacia delle misure implementate
- La gestione, classificazione e segnalazione degli incidenti informatici
  - Strumenti e processi per intercettare gli incidenti
  - Valutazioni quali quantitative degli incidenti
- I test di resilienza operativa digitale
  - Tipologie di test
  - La selezione dei fornitori per l'esecuzione dei test
- La gestione dei rischi derivanti da terzi
  - Le normative sulle esternalizzazioni
  - Il processo di valutazione dei fornitori
  - La valutazione dei servizi in cloud
  - La valutazione da parte di terzi
  - Gli aspetti contrattuali

[1] Giancarlo Butti, **Manuale di resilienza,** (pp. 600) ITER

Il monitoraggio dei fornitori

Exit strategy ed exit plan e relative test

- La condivisione delle informazioni

L'interazione con le altre normative

Le sanzioni

Ore 13.00 chiusura dei lavori

(*) Il corso si svolgerà nell'arco di due mattine consecutive con gli stessi orari

RELATORE: **Giancarlo BUTTI**

Ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Si occupa di ICT, organizzazione e normativa dai primi anni 80. È membro del Comitato Scientifico del CLUSIT. Auditor, security manager ed esperto di privacy; affianca all'attività professionale a quella di divulgatore. Oltre 140 corsi, seminari e master universitari presso ISACA, CLUSIT, ITER, CETIF, IKN, AIIA, UNIVERSITA DI MILANO, POLITECNICO DI MILANO, UNIVERSITÀ DEGLI STUDI SUOR ORSOLA BENINCASA NAPOLI, CEFRIEL, UNISEF,… Ha all'attivo oltre 800 articoli e collaborazioni con oltre 30 testate, 25 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha inoltre partecipato alla redazione di 25 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT… Socio e già proboviro di ISACA/AIEA è socio del CLUSIT e del BCI, partecipa a numerosi gruppi di lavoro. Ha inoltre acquisito le certificazioni/qualificazioni: LA BS7799, LA ISO/IEC27001, CRISC, CDPSE, ISM, DPO, CBCI, AMBCI.

Quota di partecipazione

comprensiva di materiale didattico su formato elettronico:

Euro 500 + 22% Iva a partecipante

Per iscrizioni e ulteriori informazioni Tel. 02/36577120 - email: informa@informabanca.it

Le informazioni sulle modalità di collegamento alla videoconferenza verranno fornite al partecipante al momento dell'iscrizione