SICUREZZA INFORMATICA IN BANCA

Le ultime novità in ambito normativo

Quali sono le **ultime novità** del **panorama normativo** per quanto riguarda la **cybersecurity** nel **settore bancario**? A un framework già corposo si aggiungono la **Direttiva NIS2** e il **Regolamento Dora**, entrambi approvati dal **Parlamento europeo** e già instradati al recepimento da parte dei vari Paesi dell'Unione. Tra **assestamento del GDPR**, modifiche alla **legge antiriciclaggio**, linee guida in materia di **esternalizzazioni** ed entrata in vigore della **PSD2** e del **Cybersecurity Act**, aumentano gli stimoli e i vincoli proposti dal legislatore (ma sarebbe meglio dire dai legislatori, vista la portata internazionale della disciplina) non solo **per aumentare il livello della sicurezza** in un mercato delicato come quello finanziario, ma anche per favorire nuove opportunità di collaborazione ed economie di scala sul piano del **risk management.**

PERCHÉ, AL DI LÀ DEGLI OBBLIGHI DI LEGGE, OGGI SERVONO BARRIERE INFORMATICHE ADEGUATE

I rischi aumentano per tutte le imprese, e in particolare per quelle del settore finanziario: dotarsi di strategie e soluzioni di cybersecurity e risk management non significa solo ottemperare agli obblighi di legge, ma soprattutto proteggere il business.

+53%
la crescita dei cyberattacchi in Italia da gennaio a giugno 2022

1.141
il numero di attacchi cyber gravi, che registrano un incremento dell'8,4% rispetto al primo semestre 2021

45%
gli attacchi gravi con effetti molto importanti sono stati quasi la metà del totale

+76,7%
l'aumento degli attacchi nel settore Financial-Insurance durante il primo semestre 2022

Fonte: Rapporto Clusit 2022

I DISPOSITIVI SU CUI BASARE LO SVILUPPO DELLE STRATEGIE E DEGLI STRUMENTI DI DIFESA:

DIRETTIVA NIS2

Approvata dal Parlamento europeo il: 10 novembre 2022.

Cosa prevede: Rafforzamento di un framework comune in materia di cyber sicurezza, introducendo tra gli altri un sistema sanzionatorio armonizzato a livello comunitario

Su che ambiti si estende: pone il focus della cybersecurity sugli Operatori dei Servizi Essenziali, ovvero società che forniscono un servizio essenziale la cui interruzione avrebbe un impatto significativo sull'andamento dell'economia o della società.

REGOLAMENTO DORA
(DIGITAL OPERATIONAL RESILIENCE ACT)

Approvato dal Parlamento europeo il: 10 novembre 2022.

Cosa prevede: punta a garantire la resilienza operativa delle aziende del settore Fintech rispetto ai rischi cyber.

Su che ambiti si estende: oltre agli istituti di credito tradizionali, il nuovo regolamento si applica ai **gestori di servizi di pagamento elettronica**, ai provider di servizi di informazione sui conti, alle società di investimento, ai gestori di wallet di criptovalute e di portali di interscambio di monete digitali, agli attori del mondo del trading, alle agenzie di rating del credito e agli assicuratori, e **a tutti gli intermediari che si collocano lungo la catena del valore Finance**, inclusi i **provider di soluzioni ICT.** Si parla quindi di circa **20mila potenziali soggetti interessati.**

NIS2: POTENZIARE LA CYBER SICUREZZA SU PROCESSI E SERVIZI ESSENZIALI:

Così si rafforzano le buone pratiche della Direttiva NIS

Da una norma comune di difesa contro le minacce informatiche all'interno dell'Unione Europea.

→ Alla rideterminazione e all'ampliamento dell'ambito di applicazione delle norme in materia di sicurezza dei dati, con particolare riferimento alle aziende che gestiscono servizi essenziali.

La nuova rilevanza delle supply chain

Dalla responsabilità circoscritta alla singola impresa titolare di un servizio.

→ All'estensione a tutti gli stakeholder che intervengono lungo la supply chain e la catena del valore, che sono quindi tenuti ad analizzare e valutare i rischi di sicurezza dei sistemi informativi con strumenti di vulnerability assessment e penetration test, a gestire i rischi informatici con piani ad hoc di continuità operativa e gestione delle crisi, attività di monitoraggio e strategie di incident response.

Un approccio da condividere con i partner

Dall'esecuzione di attività di controllo standard e periodiche, basate sulla lettura di parametri generici.

→ A una valutazione complessiva, periodicamente aggiornata, della propria esposizione al rischio di riciclaggio.

40° AGGIORNAMENTO DELLA CIRCOLARE 285/2013 DI BANCA D'ITALIA

Il **30 giugno 2023** entrerà in vigore un importante aggiornamento della Circolare 285/2013 della Banca d'Italia, che prevede **l'attuazione degli Orientamenti EBA** in materia di **gestione dei rischi IT e relative misure di sicurezza**, con rilevanti innovazioni relative a governance, gestione dei progetti ICT e governo dei cambiamenti. L'aggiornamento coinvolge le strutture aziendali di controllo appartenenti alla II linea di governo, con particolare riferimento alla neonata figura dell'**IT Risk Manager**.

PER UN SETTORE FINTECH SEMPRE PIU' RESILIENTE, LE NOVITA' PREVISTE DAL REGOLAMENTO DORA:

L'introduzione del principio di proporzionalità

Da una serie di criteri di assegnazione delle responsabilità non ben circoscritti

→ Al principio di proporzionalità, che nel valutare la responsabilità degli operatori Fintech tiene quindi conto delle loro dimensioni, della loro natura, dell'ampiezza e della complessità dei loro servizi, oltre che delle loro attività e operazioni e del profilo di rischio complessivo.

Più controllo sul lavoro dei fornitori di servizi ICT

Da una lacuna normativa sul ruolo e sulle responsabilità dei fornitori di servizi ICT, e in particolare dei cloud provider

→ Alla definizione di una autorità di sorveglianza capofila alla quale sono conferiti poteri idonei a garantire l'adeguato monitoraggio dei fornitori di servizi tecnologici che assolvono una funzione critica per il funzionamento del settore finanziario. I provider saranno quindi sottoposti a un quadro di sorveglianza dell'Unione.

Verso la creazione di procedure di reporting condivise

Da un framework disomogeneo da Paese a Paese

→ All'obbligo condiviso di stabilire e attuare un processo di gestione per monitorare e registrare gli incidenti connessi alle ICT, per classificarli e determinarne l'impatto e segnalarli alle autorità competenti se ritenuti gravi. Per il trattamento della segnalazione sarà utilizzato un modello comune e le entità finanziarie devono inviare segnalazioni iniziali, intermedie e finali, informando utenti e clienti qualora l'incidente abbia o possa avere un impatto sui loro interessi finanziari.

PROPOSTA DI AGGIORNAMENTO DELLA CIRCOLARE 285/2013 IN MATERIA DI OUTSOURCING

La Circolare 285/2013 potrebbe essere ulteriormente modificata nel momento in cui fosse approvata una proposta di aggiornamento che introduce un possibile schema di segnalazione sugli accordi di esternalizzazione sugli intermediari vigilati, volta ad adottare un approccio il meno oneroso possibile, ma preservando al contempo le informazioni funzionali all'**individuazione di eventuali fenomeni rischiosi**.
L'intento è quello di **coinvolgere tutti i soggetti vigilati** anche se non destinatari di norme europee (ad. Es.: intermediari finanziari ex 106 TUB).

Augeos Services and technology to create value
info@augeos.it Augeos S.p.A. Rivoli (To) I Milano (Mi)