Digitalizzazione e GDPR: cosa cambia nel security management in banca - 1

intervista a Pietro Blengino - Security Manager | Componente Consiglio Direttivo A.N.S.S.A.I.F.

GDPR e grandi organizzazioni: si possono fare i primi bilanci sulle reazioni al Regolamento europeo da parte delle diverse funzioni aziendali?

Tenendo conto che l'adeguamento delle aziende italiane è iniziato con ritardo rispetto ad altri paesi europei e che, pertanto, c'è ancora chi sta correndo per mettersi a posto, penso che oggi sia possibile fare al massimo un punto della situazione, più che tracciare bilanci.

In questo senso, devo dire che le grandi aziende, penso soprattutto alle banche, hanno fatto un grande lavoro, consapevoli dei rischi che le violazioni della privacy possono comportare in termini in primis economici e reputazionali.

Tutti sappiamo bene che ci troviamo di fronte a un radicale cambiamento di approccio da parte del legislatore europeo. Da alcuni mesi non vengono più indicate misure da osservare pedissequamente: per esempio, in caso di data breach con violazione dei dati della clientela e possibili danni, non si era colpevoli se venivano rispettate le misure "minime" determinate per legge.

Oggi l'affermazione del principio di *accountability* pone in capo al titolare del trattamento la valutazione dei rischi e la predisposizione di misure idonee per evitare possibili violazioni. Tralasciamo per un attimo i concetti di privacy by design e by default, per evidenziare che il GDPR ha richiesto alle aziende di rivedere tutti i propri processi per capire quali fossero i rischi ancora scoperti, le falle aperte, gli interventi da adottare.

Parliamo spesso di migliaia di processi rivisti purtroppo solo nell'ultimo anno.

Non voglio dire che sia tutto a posto quanto, piuttosto, affermare che le grandi aziende hanno preso sul serio i nuovi obblighi e si sono impegnate nel percorso di adeguamento.

Ciò non toglie che alla luce del recente attacco hacker ad alcuni server gestiti da Telecom per caselle PEC di magistrati e tribunali civili siano emerse gravissime criticità soprattutto per la Pubblica Amministrazione, oltretutto esclusa dall'applicazione della Direttiva NIS.

Dal suo punto di osservazione, ha rilevato cambiamenti per effetto del GDPR nelle relazioni tra le funzioni preposte alla sicurezza fisica e alla cybersecurity?

Sicuramente l'applicazione dei nuovi obblighi derivanti dal GDPR, anche nella sua declinazione italiana del D. Lgs. 101/2018, ha richiesto una maggiore collaborazione tra le diverse funzioni aziendali. A mio parere, si tratta soprattutto di una collaborazione tra le funzioni di Compliance/Legal e Sicurezza Informatica.

Il ruolo della Sicurezza Fisica è rimasto, secondo me, limitato soprattutto alla gestione della videosorveglianza (area di ripresa, comunicazione alla clientela, profili di abilitazione di accesso alle immagini) e alla gestione del controllo degli accessi per la sicurezza delle sedi e la protezione dei dati.

Quali richieste o indicazioni propone ai fornitori per avere assicurazioni sulla compliance al Regolamento dei sistemi preposti alla sicurezza dei dati?

Dai fornitori mi aspetto innanzitutto soluzioni che garantiscano la piena rispondenza ai dettami del GDPR, con questo intendendo prodotti costruiti secondo i principi della privacy by design e by default in modo da non avere rischi di violazione della gestione dei dati dei clienti o dei dipendenti perché, ad esempio, non erano stati anonimizzati quando necessario.

Allo stesso modo, nel caso in cui il fornitore tratti dati personali per conto dell'azienda committente (quindi, per questo motivo, è stato nominato Responsabile del trattamento) mi aspetto che adotti un atteggiamento di profonda collaborazione nei confronti del committente. Può apparire un'affermazione banale ma, posso assicurare che non è così.

Temo che spesso il fornitore non comprenda appieno le responsabilità che il GDPR pone in capo al titolare del trattamento e trascuri di dare le garanzie richieste. È un momento molto delicato nella vita aziendale e, in passato, abbiamo avuto percentuali decisamente basse nelle risposte.

Più in generale, come valuta gli effetti della digitalizzazione sul sistema bancario e sul futuro delle premises?

I piani industriali di riduzione degli sportelli bancari sono sotto gli occhi di tutti, così come la competizione per l'offerta di servizi online più ampi possibili.

A tutto questo si aggiunga che la competizione ormai non è più soltanto tra banche.

Anche il settore delle BigTech si sta affacciando in modo molto aggressivo. Pay Pal è già una banca a tutti gli effetti. Facebook ha ricevuto il via libera dall'Irlanda per operare nei pagamenti e money transfer. Amazon sta studiano con JPMorganChase & Co. e Capital One, un conto corrente bancario destinato ai propri clienti.

Di fronte a questo scenario in rapida evoluzione, è chiaro che la filiale bancaria sarà prevalentemente il luogo in cui ci si recherà per i servizi di consulenza. Di conseguenza, il ruolo del security manager bancario sarà quello di proteggere non tanto il denaro quanto, piuttosto, le persone e i dati.

Intendo dire che rimarrà un ruolo con caratteristiche peculiari per la necessità di un risk assessment legato alle caratteristiche del territorio e della criminalità. Il professionista dovrà arricchire il suo bagaglio "culturale" di competenze che riguardino la digitalizzazione delle misure di sicurezza e la conseguente protezione da attacchi hacker.

Sono frequenti le notizie in merito alle vulnerabilità dei sistemi di videosorveglianza in cui l'accesso all'intera rete può essere facilmente realizzato da un informatico esperto.

Non ho ancora avuto notizie di hackeraggio di sistemi di impianti di allarme, ma credo che sia dovuto soltanto al minor appeal della notizia rispetto alle altre vulnerabilità.

A tutto questo aggiungerei la sempre maggiore capacità relazionale che un security manager deve avere per spiegare all'interno della propria banca l'importanza delle misure di sicurezza adottate e del loro rispetto da parte del personale.

Troppo spesso vediamo che importanti investimenti di sicurezza vengono vanificati dall'elemento umano che, per trascuratezza o perché ingannato attraverso tecniche più o meno raffinate di social engineering, consente il superamento della misura di sicurezza stessa. La capacità di realizzare, anche in collaborazione con le altre funzioni aziendali competenti, efficaci iniziative di awareness sarà senz'altro una skill che dovrà essere presente nel bagaglio del security manager.