SICUREZZA LOGICA NELL'ERA DIGITALE: USCIRE DALLA ZONA D'OMBRA DELLO SHADOW IT

Sulla spinta di iniziative legate all'evoluzione del modello di business e all'aumento di produttività, si è diffuso anche nelle banche il fenomeno dell'IT consumerization, che porta all'utilizzo in contesto lavorativo di tecnologie diffuse in ambito consumer (social network, cloud, servizi online, mobile application e personal device). l'IT deve riprendere la posizione di leadership nel processo di innovazione tecnologica della banca, per fronteggiare i nuovi scenari di rischio che emergono dal passaggio dall'IT consumerization allo shadow IT – ovvero all'utilizzo di strumenti e soluzioni IT all'insaputa dell'azienda e in difformità dalle policy aziendali.

L'evoluzione tecnologica nel mondo consumer e l'introduzione di nuove tecnologie nei processi di business della banca, portano nell'attività lavorativa di ogni giorno nuovi paradigmi e modelli di riferimento che finiscono poi per essere riutilizzati per gli scopi più svariati, spesso all'insaputa dell'IT e della Security aziendale.

Per affrontare in modo efficace questo fenomeno, tanto dal punto di vista delle tecnologie quanto da quello della governance, è necessario da un lato mettere in campo un nuovo approccio alla sicurezza e dall'altro fare ricorso ad una metodologia dedicata alla gestione dello Shadow IT con l'obiettivo di offrire al tempo stesso il giusto equilibrio tra esigenze di sicurezza, supporto del Business, controllo dei rischi e compliance normativa.

CONSUMERIZATION E SHADOW IT

Anche se l'ingresso nella zona d'ombra dello Shadow IT può avvenire nei modi più svariati e ad opera di attori diversi, è solitamente possibile individuare una certa omogeneità nelle modalità di evoluzione di questo fenomeno all'interno delle banche.

Le aree aziendali più proattive, sotto pressione a causa di obiettivi sempre più sfidanti, si scontrano con fattori che frenano la propria efficienza: policy e requisiti di sicurezza stringenti e complessi, difficoltà di supporto alle tecnologie più innovative, lentezze burocratiche, costi elevati.

Abituati all'utilizzo di tecnologie proprie del mondo consumer, i referenti delle aree di Business iniziano a valutare soluzioni estranee all'IT aziendale, come il ricorso a servizi e infrastrutture esterne e l'utilizzo di device ed applicazioni personali.

L'utilizzo di soluzioni esterne all'IT della banca, seppure adeguate alle esigenze, comporta un indebolimento delle procedure di gestione e controllo delle informazioni aziendali.

Nuovi processi e servizi di business sono così erogati facendo affidamento su organizzazioni e sistemi estranei all'azienda e spesso senza coinvolgere adeguatamente l'IT, la Security e le altre strutture aziendali che dovrebbero essere coinvolte nel processo di selezione, acquisto e configurazione di soluzioni e servizi IT interni ed esterni, con il rischio che questi ultimi non siano conformi alle policy e ai requisiti aziendali.

UN NUOVO APPROCCIO ALLA SECURITY

Nell'ottica di questa evoluzione, le banche devono mettere in campo un nuovo approccio alla sicurezza delle informazioni.

La Security deve inserirsi il più presto possibile nel ciclo decisionale del Business e supportare adeguatamente le nuove richieste, cercando di ridurre al massimo gli impatti sulla produttività e sull'efficienza e fornendo gli strumenti necessari al supporto dei nuovi modelli operativi e di business sui quali la banca sta investendo.

È di conseguenza necessario che la Security si orienti verso un nuovo modello operativo, ricoprendo essa stessa un ruolo di consulenza nei confronti delle aree di Business, cercando di comprenderne le nuove esigenze e fornendo le funzionalità di sicurezza necessarie con la stessa facilità, elasticità e velocità dei servizi e delle soluzioni consumer, magari facendo ricorso, per prima, all'utilizzo diretto di queste tecnologie.

La Security non può e non deve diventare un freno per l'innovazione e il cambiamento.

Allo stesso tempo rimane ovviamente fondamentale continuare a tenere sotto controllo la propria esposizione alle minacce di sicurezza, a garantire il rispetto dei requisiti di compliance normativa e a gestire adeguatamente i rischi. Questi principi sono infatti da sempre alla base di un efficace Sistema di Gestione della Sicurezza delle Informazioni e sono recentemente tornati in auge con le Nuove Disposizioni di Vigilanza 263 (15° aggiornamento) di Banca d'Italia.

I requisiti espressi da queste ultime, in ottica compliance possono essere infatti letti secondo il fil rouge del rischio a cui le banche devono far fronte in presenza di applicazioni che esulino dalla conoscenza e/o controllo dell'IT: situazioni in cui la banca perde la capacità di controllare i propri dati e i flussi che li coinvolgono.

Su tale base, la Circolare 263 prevede che lo sviluppo di applicazioni direttamente in carico alle unità operative e di controllo sia "sottoposto a misure di natura organizzativa e metodologica, tese a garantire un livello di sicurezza comparabile con le applicazioni

sviluppate dalla funzione ICT" e richiede la predisposizione di un "sistema per la gestione dei dati", con particolare riferimento ai dati di bilancio, finanziari e relativi alla gestione del rischio. La compliance in tema di Shadow IT, come delineata dalla Circolare 263, è dunque pienamente in linea con quanto espresso da altre normative rilevanti per il mondo bancario, quali PCI-DSS, SOX e Basel II/III.

LA METODOLOGIA

La metodologia vincente per affrontare le sfide portate dall'IT Consumerization, dallo Shadow IT e, in generale, dal nuovo approccio richiesto alla Security nello svolgimento del proprio ruolo, prevede la configurazione, implementazione ed esecuzione di un Framework per l'IT Consumerization Security Management (ICSM) in grado di indirizzare e guidare tutte le attività necessarie.

L'ICSM Framework prevede quattro fasi, eseguite in modo sequenziale:

Monitor & Discover – Creare consapevolezza a tutti i livelli aziendali sul fenomeno dello Shadow IT; procedere attraverso interviste e questionari o l'utilizzo di strumenti tecnologici, all'individuazione e al monitoraggio di casi ed eventi specifici.

Evaluate – Analizzare le cause del ricorso a soluzioni e modelli non ufficialmente supportati e le relative modalità di utilizzo; valutare il rischio associato ad ogni casistica e, per ciascuna, definire un'azione di remediation: negare, accettare o regolare il caso d'uso specifico, oppure pianificare la realizzazione di un servizio analogo, ma interno alla banca.

Manage & Secure – Realizzare gli interventi di remediation individuati, siano essi di tipo tecnologico che organizzativo.

Operate – Rilasciare le nuove soluzioni realizzate e informare i principali stakeholder circa le corrette modalità di utilizzo di soluzioni e strumenti alla base delle casistiche individuate e regolate.

Al solito, in applicazione del principio di miglioramento continuo, le fasi previste dall'ICSM Framework sono ripetute ciclicamente, incrementando ad ogni iterazione il livello di maturity della banca nel gestire il fenomeno in oggetto e, di conseguenza, anche il livello generale di sicurezza.

Allo scopo di rendere il più efficace possibile l'applicazione del Framework descritto, occorre definire con cura l'ambito di copertura, le metodologie e gli strumenti da utilizzare, come ad esempio gli strumenti o le metodologie da impiegare nella fase di discovery o per l'analisi del rischio. Questi parametri devono essere definiti tenendo conto di svariati fattori, tra i quali rivestono particolare importanza gli obiettivi e le strategie di business della banca, la sua cultura in termini di innovazione tecnologica e il suo livello di preparazione e strutturazione su tematiche legate al mondo IT e della security.

CONCLUSIONI

Considerando che l'innovazione e l'efficienza operativa sono alla base della crescita del business aziendale, compito di ogni organizzazione che si trovi in un mercato competitivo come quello bancario è quello di fornire al Business tutti gli strumenti, IT e non, necessari per lavorare al meglio.

Dove ciò non avviene, il rischio è che gli strumenti siano reperiti esternamente, in difformità dalle policy aziendali e all'insaputa dell'IT e della Security.

Ovviamente la strategia corretta non è ignorare il fenomeno e i relativi rischi, ma fare in modo che l'IT e la Security si riprendano la leadership dell'innovazione tecnologica guidando e supportando in modo adeguato questa esigenza.

Sonia Crucitti
Associate Partner, Spike Reply