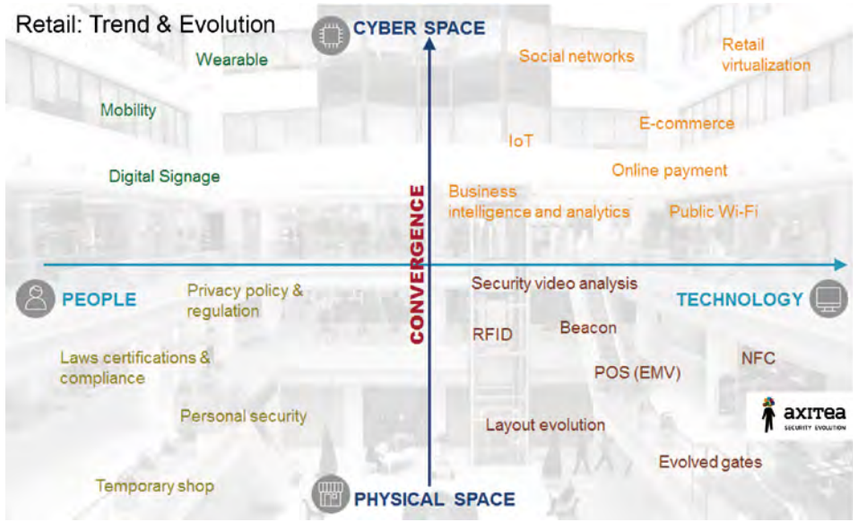
Attacchi combinati, la nuova minaccia per i retailer. Le soluzioni di un Global Security Provider

a colloquio con Maurizio Tondi, VP Strategy & Operations Axitea
a cura della Redazione

L'evoluzione del sistema distributivo al dettaglio sta determinando nuovi paradigmi per la sicurezza. Il tema dell'attacco combinato (IT + Phy) interessa i retailer tanto quanto la sottrazione di dati. Può farci un quadro della situazione a livello globale?

Da un lato il settore del Retail a livello globale è attraversato – per quanto riguarda la Sicurezza – da eventi e vulnerabilità assolutamente non dissimili da altri contesti industriali; ma dall'altro, proprio per alcune specificità operative, rappresenta un incrocio particolarmente previlegiato, una sorta di "melting pot" nella quale si fondono e risultato più evidenti gli effetti della convergenza tra fisico e cyber e tra uomo e tecnologia. Mi spiego meglio: da tempo parliamo di integrazione ma mai come ora e forse mai come nell'articolato sistema di distribuzione (dalla grande distribuzione organizzata, al dettaglio, ai punti vendita) minacce, attacchi, furti ed atti criminosi in genere stanno interessando tutto il "place", a tutti i livelli della filiera da un alto e tutti gli stakeholder dall'altro. Questo sostanzialmente perché il percorso di forte trasformazione del settore interessa aspetti giuridico-normativi, di compliance, di comportamento e di "awareness" e di attiguità tecnologica (IT, TLC, IoT, Mobility).

Il furto, la rapina, la sottrazione di merce e di denaro, la frode, l'atto predatorio e le differenze inventariali si intrecciano con sottrazione di dati sensibili, "data breaches", furti di identità, credenziali, carte di credito, database di clienti, profili di acquisto e proprietà intellettuali.. Non solo emergono, quindi, le evidenze più tipiche dell'attività predatoria tradizionale, ma quelle di attacchi e sottrazione di dati legati al cyber crime, basti ricordare i casi eclatanti di Target (70 milioni di clienti), Home Depot (56 milioni di carte di credito), Sally Beauty, etc. Ma la dimensione non conta. Il mix tra limitata informazione, consapevolezza e fragilità tecnologiche intrinseche o di configurazione, rende potenzialmente attaccabili e violabili aziende di ogni dimensione. Spesso le piccole, le meno protette, diventano il punto di vulnerabilità per attaccare poi le grandi organizzazioni. E spesso, sempre più, l'uomo è l'elemento più debole di questa catena. In Italia, inoltre, la mancanza di obbligatorietà nel denunciare il furto informatico, falsa le dimensioni e la portata del fenomeno dal punto di vista della gestione del rischio e del danno. La superficie target degli attacchi Cyber è aumentata sensibilmente e ci sono infatti più utenti connessi, più dispositivi utilizzati e più dati digitali a disposizione. Se è vero che nel segmento del Retail ed in particolare nella gestione fisica del punto vendita, si sono ultimamente introdotti pattern di acquisto, propensioni e criteri tipici di market place ed e-commerce, è emersa anche pericolosamente una diversa postura di Sicurezza e di esposizione al rischio, tipica dell'interazione on line; è certamente evidente che vulnerabilità e debolezze legate alla posizione geografica ed all'architettura del punto vendita, al layout, alla disposizione dei varchi e degli accessi, agli impianti tecnologici, all'ergonomia dei punti di pagamento, ai magazzini e al comportamento dei dipendenti e dei fornitori, rappresentano oggi potenziali punti di attacco ai sistemi ed all'infrastruttura informatica e di comunicazione. Gli attacchi Informatici, inoltre, sono diventati sofisticati e di difficile rilevamento con i tradizionali sistemi di difesa, gli strumenti di attacco sono facilmente disponibili a poco prezzo e non richiedono particolari competenze.



Quali sono gli schemi difensivi per un retailer che da un cyber-attack può avere i maggiori danni per la sua reputazione?

Il primo livello di protezione è definitivamente la conoscenza e l'informazione. La consapevolezza del rischio, sia esso fisico o cyber, è certamente il principale elemento per costruire un adeguato sistema di difesa. La conoscenza di pratiche di successo – che si sono rivelate vincenti nel contrastare con efficacia la recrudescenza della minaccia – realizzata attraverso il confronto con operatori specializzati che abbiano nel proprio bagaglio professionale queste esperienze a livello nazionale ed internazionale, è sicuramente un asset da considerare come schema difensivo di massima. Attacchi come lo spear phishing, il watering hole ed attacchi di social engineering hanno tutti poi come obiettivo proprio le "persone". Ed i danni non solo materiali ma anche reputazionali e di immagine rappresentano un elemento di massima attenzione. La continuità operativa, ed a volte la sopravvivenza stessa di un'organizzazione, può essere messa fortemente a rischio. Immaginiamo nell'ambito fashion l'impatto della sottrazione dei nuovi modelli di una collezione, piuttosto che l'utilizzo abusivo di immagini o del brand da qualche parte nel mondo, su qualche sito web. Quindi il tema del comportamento e della cultura è centrale per proteggersi da furti e frodi ma anche dalla

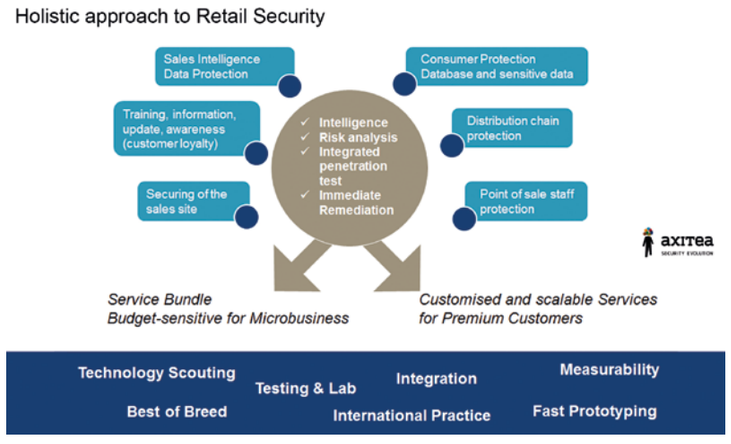
sottrazione di dati molto sensibili. Poi certamente la tecnologia: è vero che tanti nuovi dispositivi non sono stati progettati per essere nativamente sicuri (dispositivi mobili, dispositivi specializzati e device IoT) e tanti di questi rappresentano proprio gli elementi di trasformazione ed innovazione applicata al Retail per amplificare la superficie di vendita, avvicinare sempre più i consumatori ed aumentare definitivamente le vendite, ma tecnologie innovative di intelligence e di prevenzione, l'ottimizzazione dei sistemi di protezione esistenti e di monitoraggio rappresentano strumenti e contromisure efficaci. Un'architettura integrata di servizi, procedure e strumenti che segua l'intero life cycle della sicurezza e che sia a disposizione dei Security Manager, rappresenta la barriera più rilevante anche alle trasformazioni morfologiche degli attacchi.

E' possibile individuare un modello di "sicurezza olistica" per un retailer, che coordini sotto un'unica regia le azioni per la difesa del patrimonio aziendale nei confronti delle diverse minacce a cui può essere esposto?

Un approccio di tipo olistico è definitivamente la risposta più attuale e più efficace alle mutate condizioni di attacco, di minaccia e di gestione integrata del rischio soprattutto nel settore del Retail in cui si radicalizza la convergenza tra fisico ed informatico ed in cui sono molteplici i potenziali punti di vulnerabilità: varchi, ingressi, accessi, mezzi di trasporto, parcheggi, personale, fornitori, partner, consulenti, sistemi informativi aziendali, sistemi tecnologici, dispositivi fissi e mobili. Ed in cui – come in altri settori – soprattutto nelle grandi organizzazioni emerge anche una debolezza strutturale anche in termini di Ownership. Spesso le Aziende sono per natura guidate dal Profit&Loss e da una predisposizione mentale nella gestione del rischio orientata pericolosamente all'accettazione della "forza maggiore" e della "conformità normativa" e di fatto meccanismi di protezione istantanea non sono applicati. Peraltro, tutti gli attacchi del passato conosciuti si sono dimostrati "trasversali" coinvolgendo elementi informatici, fisici, umani ed organizzativi ed evidenziando definitivamente la necessità di un approccio olistico ed integrato, per essere efficaci nella riduzione dei rischi. L'approccio a "silos" per la sicurezza fisica, informatica e per la protezione del capitale umano si è rivelato assolutamente insufficiente ed inadeguato.

Qual è la visione operativa di Axitea, che si propone come Global Security Provider focalizzato sul mercato verticale del Retail?

Axitea si inserisce in questo contesto ed opera attraverso differenti esperienze operative ed una singola, unificata ed integrata proposizione dedicata al presidio ed alla difesa dello spazio fisico-cyber del Cliente, indirizzando così il fabbisogno complessivo di sicurezza delle aziende impegnate oggi nella ricerca di livelli di protezione professionale e di elevata qualità. Axitea valorizza da un lato l'esperienza, le specificità e le prerogative di un Istituto di Vigilanza che ha sempre operato nel settore del microbusiness e della protezione di negozi, esercizi commerciali, punti vendita e catene di distribuzione, perfezionando la formazione delle proprie Guardie Giurate, la disponibilità delle proprie Centrali Operative e la "cultura" della gestione degli allarmi e degli interventi. Di contro, attraverso centri di competenza – recentemente rinnovati in termini di tecnologie innovative e professionalità – per la realizzazione e gestione di soluzioni di video sorveglianza, video analisi, protezione perimetrale, monitoraggio e messa in sicurezza di punti sensibili dell'infrastruttura informatica del Cliente, con tecniche, metodologie e strumenti di intelligence, management e remediation. La system integration rappresenta per Axitea l'asset operativo più rilevante, nella realizzazione delle soluzioni innovative per il mercato Retail. Ad esempio l'utilizzo dell'infrastruttura di videosorveglianza anche per realizzare analisi video finalizzate al marketing analytics, coniuga le necessità di produttività di punti vendita, centri commerciali e supermercati con l'efficientemento e la riduzione dei costi, migliorando ingaggio, capture rate e valore delle vendite attraverso funzionalità di heat mapping, hot zone, visual merchandising, controllo della coda, controllo scaffali, controllo cestelli e carrelli, articoli abbandonati. Inoltre nell'integrazione della gestione del punto vendita, è centrale la proposizione di Axitea per la protezione personale dei dipendenti realizzata attraverso portable e wearable device dedicati all'anti-rapina e anti-aggressione. Le soluzioni satellitari sviluppate specificatamente per il retail, rappresentano il punto di incontro tra sicurezza e logistica per ridurre i rischi legati al furto del mezzo e della merce trasportata, fornire assistenza in caso di emergenza dalla Centrale Operativa, gestire la localizzazione, il posizionamento, i controlli gestionali sui consumi dell'intera flotta. Le applicazioni dedicate inoltre alla gestione della "catena del freddo" progettate da Axitea consentono di monitorare in tempo reale la temperatura negli appositi vani di carico, attraverso un controllo ed un supporto continuativo da remoto, oltre a fornire report analitici, report grafici, avvisi di superamento soglie e l'integrazione con sensori di IoT. Visione, scouting tecnologico, integrazione dei sistemi, conoscenza approfondita delle best practice di settore e servizi sono i contributi cruciali che Axitea mette a disposizione del mercato.



Axitea è la società leader in Italia nel settore della sicurezza, specializzata nello sviluppo di soluzioni integrate e personalizzate. Con oltre 1.500 dipendenti, Axitea offre servizi per la sicurezza di aziende, attività commerciali, istituzioni, residenze private, mezzi e beni mobili. L'offerta prevede l'integrazione di tecnologie innovative personalizzabili, la capacità di progettazione, di gestione delle infrastrutture e sistemi e un portfolio completo di servizi di sicurezza e di vigilanza. L'azienda è presente su tutto il territorio nazionale, grazie alle proprie filiali, alle Centrali Operative e alla rete degli Axitea Partner, società affidabili, accuratamente selezionate e certificate. Circa 32.000 clienti in tutta Italia hanno già scelto Axitea per la loro sicurezza.

CONTATTI - AXITEA SPA
marketing@axitea.it
www.axitea.it