SECURITY GOVERNANCE. A colloquio con Stefano Grassi di Poste Italiane

Fiducia, l'asset intangibile più importante

Dai servizi postali a quelli finanziari, assicurativi e digitali, Poste Italiane è diventato una best practice a livello internazionale, grazie alla creazione di un ecosistema favorevole all'innovazione e alla gestione della sicurezza

di Massimiliano Cannata

Un nuovo importante primato per Poste Italiane. Il Gruppo ha ottenuto la certificazione per i servizi Cloud dalla Csa (*cloud security alliance*) da parte della Bsi, a dimostrazione di quanto siano legate la *Governance dell'innovazione* e la *Governance della sicurezza*, in quello che, per usare una celebre definizione di Derrick De Kerckove possiamo chiamare come il "Paese Internet". La sicurezza, nell'universo digitale appare sempre più come il valore che apre l'azienda alla dimensione sociale, al suo ambiente di riferimento, in una parola al contesto in cui opera, dando forma e sostanza alla *corporate responsability*.

Un riconoscimento importante quello della Csa, perché riguarda il punto focale della strategia messa in campo dall'avvocato **Stefano Grassi**, direttore della struttura centrale Tutela Aziendale di Poste Italiane, una strategia che fa comprendere le dinamiche di un'azienda in movimento, che affronterà la privatizzazione potendo vantare conti in ordine e prospettive rilevanti di crescita. Con un utile netto di 1.032 milioni di euro, a fronte di 24.069 ricavi totali, 144.628 dipendenti, 6 milioni di conti correnti, 13.000 uffici sul territorio ci troviamo di fronte a una realtà produttiva e ad asset cruciali per il Sistema Paese, che vanno prima di tutto tutelati e messi a disposizione della collettività.

Di questo ne è consapevole per primo lo stesso Stefano Grassi, che ha creato un apparato integrato di gestione della sicurezza, che osserva gli standard più avanzati in termini di dotazioni tecnologiche, competenze professionali e dotazioni infrastrutturali. Per capire la delicatezza del tema sicurezza basti pensare che circa il 60/70% dei ricavi totali di Poste Italiane arriva dai nuovi servizi finanziari, assicurativi e digitali e che proprio su questo terreno l'azienda mette in vetrina delle *best practices* a livello internazionale: dal Cert al Campus tecnologico, composto di apparati che per logica e impostazione fanno invidia agli operatori del settore tedeschi, americani e francesi, i quali non possono vantare la stessa redditività e soprattutto la stessa propensione alla *culture innovation*.

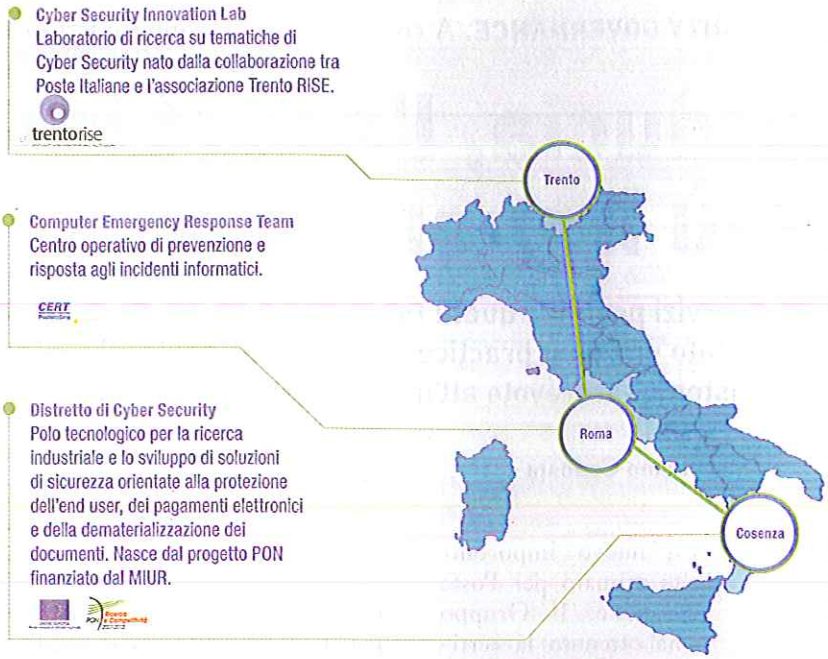
«La nostra caratteristica distintiva – spiega in questa intervista a "L'Impresa" Stefano Grassi – risiede nella capacità di integrazione dei servizi. È il cliente che sceglie la modalità di fruizione che gli è più congeniale, sia recandosi all'ufficio postale (sono circa 2 milioni di clienti al giorno *n.d.r.*) o sempre più tramite web, smartphone o con il postino telematico che porta i servizi a domicilio e nei luoghi di lavoro. Grazie a questa capacità di integrazione, siamo diventati leader in settori più verticali quali le assicurazioni, creando nuovi spazi come la telefonia mobile. In questo frastagliato e stimolante panorama, è evidente che i compiti della sicurezza si evolvono continuamente dovendo rispondere a continue sollecitazioni. Abbiamo sviluppato un modello di security articolato, un vero e proprio ecosistema, che ha richiesto un percorso di maturazione a volte complesso, ma che oggi ci permette di confermare il nostro ruolo di player di riferimento per il Sistema Paese in materia di *cyber security* e innovazione».

Stefano Grassi, direttore Tutela Aziendale e Sicurezza delle Informazioni di Poste Italiane

Quale importanza assumono

l'innovazione tecnologica e la tutela aziendale nella società dei Big data e della connettività diffusa?
Nel complesso incrocio di prodotti e servizi che lei disegna, la sicurezza è come l'aria che respiriamo. Non se ne può fare a meno è il tessuto connettivo, il termine di valore capace di cementare il rapporto tra azienda e cliente, tra azienda e fornitore. La fiducia è l'asset intangibile rispetto a cui cresce la motivazione delle risorse umane che operano nelle stesse strutture aziendali, ma anche la reputation rispetto al mercato e ai clienti che si rivolgono a noi per transazioni delicate, che toccano aree molto sensibili. Basti pensare che il successo di Poste Vita ha trasformato l'Ente in un gigante di 10 miliardi di Premi, per ciò siamo entrati in concorrenza con Generali e Unipol. Essendo ormai Poste Italiane una realtà multipiattaforma e multiservizio, in questo scenario ramificato il ruolo della funzione Sicurezza diventa centrale. Il Patrimonio aziendale risulta costituito da un insieme di componenti di natura eterogenea, che comprende le infrastrutture logistiche e produttive, i sistemi informatici, le risorse umane.

Questa concezione aperta e innovativa della *culture security* ha dei riflessi nella logica organizzativa che orienta le attività della sua struttura?
Quello di Poste è un approccio di *governance integrata della sicurezza*. Se infatti è innegabile che ogni linea di servizio è caratterizzata da specifiche peculiarità in termini di modalità di erogazione, canali di fruizione, risorse coinvolte, è anche evidente che occorre bilanciare opportune misure di protezione e di continuità. Definire un approccio di supervisione integrata e di controllo centralizzato degli aspetti di sicurezza consente di inquadrare potenziali criticità complesse, di definire gli interventi, e di elaborare una mappatura del rischio. Il lavoro del Cert è fondato su questi principi di trasversalità, scambi di know-how, tempestività e competenza.



Marc Augè nel suo ultimo libro parla delle *Nuove paure*. Il grande antropologo individua, in particolare, nell'azienda un luogo in cui diventa cruciale ristabilire un campo di protezione, di garanzia di fiducia per ripartire. Cosa vuol dire questo messaggio per chi lavora quotidianamente per governare la società del rischio?
Voglio sottolineare due termini: responsabilità e persone, questo è il binomio cruciale cui non possiamo sottrarci. Non a caso la struttura che con grande entusiasmo sto guidando è fondata su valori chiari che ci tengo a esplicitare. L'Oggettività, che significa crescita basata sul merito, sulla competenza, sulla misurabilità dei risultati. La Trasparenza, che si realizza nei comportamenti agiti quotidianamente, in un uso intelligente e dosato della comunicazione. Il Senso etico, che si traduce nella correttezza dei comportamenti, ma anche nella risposta alla domanda fondamentale che i pensatori classici si ponevano e ci ponevano: cosa debbo fare per essere veramente uomo. In azienda dobbiamo, osservando i codici professionali giusti, cercare sempre di rispondere a questa domanda. Altro asset valoriale importante: l'esempio. Dobbiamo offrire un modello, farci osservare aprendoci al confronto-giudizio dei colleghi, che nel nostro impegno e nell'impegno dei leader devono trarre la giusta motivazione per raggiungere traguardi sempre più sfidanti.

Come si articola il complesso universo della cyber security nel contesto di Poste Italiane?
Poste Italiane può contare oggi su un vero e proprio Ecosistema di Cyber Security, che convoglia su linee di azione condivise un numero significativo di iniziative di innovazione, partnership pubblico-privato e scambio di

competenze cross-settoriali. Il *Distretto Tecnologico sulla Cyber Security* è oggi dislocato sull'intera penisola italiana ed è composto da tre centri di eccellenza: il *Security Innovation Lab* di Trento, che abbiamo da poco inaugurato e che si focalizza sulla ricerca applicata e sui processi di innovation discovery nel settore; il *Cert* di Roma, che rappresenta la migliore e più completa espressione di Poste Italiane in quanto a capacità di analisi e di erogazione di servizi di sicurezza ad alto valore aggiunto; il *Distretto cyber security* di Cosenza, concepito nell'ottica di creare un Centro Servizi con propensione spiccata per la ricerca industriale e lo sviluppo di prototipi e piattaforme.

A quali criteri si ispira una tale struttura organizzativa?
Il messaggio di fondo che sottende l'intera logica organizzativa è molto chiaro: occorre rispondere alla necessità sempre più concreta che richiede un approccio strategico ai temi di *cyber security*, che non deve essere vista come una raccolta di azioni più o meno specifiche per rispondere, di volta in volta, alla singola minaccia che viene rilevata, ma che deve piuttosto saper sviluppare la capacità di integrare gli aspetti operativi alla capacità di fare innovazione e ricerca, in un flusso di interscambio continuo. Detto in sintesi: il nostro lavoro non si esaurisce nel monitoraggio e contrasto, perché presenta dei profili strategici di prevenzione e di anticipazione che oggi sono decisivi per avere successo.

Su quali "eventi" riconducibili a potenziali minacce bisogna, a suo avviso, porre maggiore attenzione quando parliamo di *cyber security*?
Basta leggere le statistiche per imbattersi in quelle che gli addetti ai lavori definiscono data breach (violazioni degli archivi informativi aziendali), che indicano per il 2013 un totale di oltre 800 milioni di record personali e informazioni sensibili persi a livello global; parallelamente vi sono gli attacchi di tipo DDoS (*Distributed Denial of Service*) che sono in continuo aumento, sia in termini numerici che di potenza: uno dei casi più recenti ha visto la compromissione di oltre 160.000 siti Internet, usati contemporaneamente per lanciare attacchi contro target predefiniti. Un fronte delicato riguarda la Sicurezza dei dispositivi mobili, ormai divenuta una delle criticità più urgenti, anche in risposta alla sovra-produzione di *malware* dedicato a cui stiamo assistendo. Solo nel 2013 abbiamo registrato un incremento di oltre il 600% nel numero di campioni disponibili per effettuare attacchi a piattaforme mobili. Infine, credo vadano prese in considerazione le problematiche inerenti la sicurezza delle infrastrutture *cloud*, usate spesso per sfruttare l'ampia capacità elaborativa disponibile per amplificare gli attacchi.

Come difendersi dal cybercrime?
Un caso emblematico è quello del *phishing* che è una sorta di pesca a strascico. Nell'ultimo quinquennio in Poste abbiamo registrato circa 7.000 attacchi. Per questo ci siamo strutturati in modo sistematico con un sistema *antiphishing* dedicato all'interno della centrale allarmi, creata già nel 2005 con l'intento di ridurre al minimo il tempo di esposizione dei clienti agli attacchi. Questo delicato lavoro che ci vede impegnati, in collaborazione con la Polizia, ci permette di oscurare in tempo reale i siti clone e di predisporre tutte le strategie necessarie a sventare le minacce. Gli attacchi vengono da ogni parte del mondo con siti clone collocati in più di cento nazioni. Questo fa capire come le attività di prevenzione e tutela siano al centro delle attenzioni di Poste Italiane, il perno del coordinamento va individuato nella nostra *security room*, che mette insieme diverse funzioni aziendali, rispondendo a quei criteri di trasversalità e di convergenza che sono iscritti nei nostri valori.

Il progetto del distretto *cyber security* di Cosenza risponde a un'esigenza di formazione di competenze e know-how all'avanguardia?
L'iniziativa che vede Poste in primo piano, insieme ad altri Enti e Aziende (Poste Italiane, Postel, Ntt Data,Cnr, Università della Calabria ecc.) risponde proprio a questo bisogno. È infatti prevista un'azione di formazione, con l'intento di selezionare e far crescere 60 giovani laureati destinati all'attività di ricerca industriale e di sviluppo sperimentale. Il territorio cui ci rivolgiamo è sicuramente difficile, ma ricco di talenti come di fatto si può considerare la Calabria. L'affiancamento di imprese e università darà corpo a quel difficile progresso di trasferimento tecnologico sempre auspicato e mai attuato nel nostro contesto e, cosa assolutamente necessaria in questa fase recessiva che sta colpendo tutta l'Italia e in modo particolare il Mezzogiorno, darà degli sbocchi occupazionali significativi in un'area che ne ha estremo bisogno. Tre sono i grandi versanti di intervento di cui ci occuperemo: la *cyber security*, la protezione dei sistemi di pagamento elettronico e la implementazione dei processi di dematerializzazione sicura. Come vede, la sfida è aperta ed è ricca di opportunità e occasioni di crescita umana e professionale.