SECURITY/2. A colloquio con Nicola Sotira, dg della Fondazione Gcsec e di Poste Italiane

Proteggete il vostro business

In uno scenario di iperconnettività in rapida crescita, dai dispositivi medicali alle autovetture, all'uso dei sensori nel contesto emergente delle smart city, la sicurezza diventerà una questione di rilevanza sociale. Come per le imprese è già una questione di rilevanza strategica

Dall'industriale al digitale, società e imprese su scala globale risentono oggi di un profondo salto di paradigma: il capitale intangibile e giacimenti di know-how grazie ai nuovi strumenti dell'Ict sono, infatti, per la prima volta disponibili su fonti potenzialmente aperte a tutti. Connettività diffusa, Big Data, Internet delle cose, Cloud Computing sono tutti fenomeni che oltre a mutare i processi organizzativi e produttivi stanno incidendo profondamente sugli equilibri della nostra vita quotidiana. Basti pensare che il 90% dei dati disponibili è stato creato negli ultimi due anni, che i social network permettono già a miliardi di persone di esprimere e comunicare le proprie idee in tutto il mondo alla velocità di un click e che nel 2020 il numero di device connessi alle reti toccherà quota 80 miliardi. Abbiamo affrontato l'impegnativo argomento di questa che molti studiosi definiscono come la quarta rivoluzione industriale, soffermandoci in particolare sulle nuove frontiere che attengono alla protezione delle informazione nell'era della cyber security, con **Nicola Sotira**, responsabile per la Tutela delle Informazioni di Poste Italiane.

Lei è alla guida della Fondazione Gcsec di Poste Italiane. Quali azioni intendete mettere in campo su un fronte certamente delicato e strategico come quello della sicurezza?
Credo sia importante oggi prima di tutto far riflettere le aziende sulle conseguenze che potrebbe avere un attacco informatico, le ricadute sul business e anche sulle possibili conseguenze legali di cui potrebbero essere chiamate a rispondere. Occorre lavorare sulla sensibilizzazione del management aziendale, la cyber security deve, infatti, essere parte degli obbiettivi del management. Far decollare le iniziative di *Information Sharing*, altro punto strategico per la difesa degli asset aziendali. La condivisione delle informazioni sarà uno dei temi centrali nei prossimi anni. Favorire la collaborazione pubblico-privato in un approccio multi stakeholder è l'altro aspetto che farà la differenza. La complessità in gioco richiede una cooperazione maggiore fra tutti i soggetti coinvolti, nel superamento della logica nazionale.

Nicola Sotira, *dg della Fondazione Gcsec e Responsabile Tutela delle Informazioni di Poste Italiane*

Sensibilizzare è dunque la parola chiave per Fondazione Poste?
È certamente un aspetto strategico. Il fattore umano è decisivo e occorre trasformare quest'ultimo da anello debole a punto di forza nelle organizzazioni e nella società civile. Sono queste le linee su cui si fonda il programma di attività della Fondazione. In questo mese di giugno avremo un primo evento focalizzato sulle infrastrutture critiche, in cui abbiamo applicato la logica della collaborazione pubblico-privato, su una delle tematiche forti anche a livello europeo. Avremo poi una campagna di sensibilizzazione durante la seconda parte dell'anno e sono già stati avviati tavoli di lavoro europei con workshop e progettualità.

A settembre parteciperemo alla quarta edizione del Cyber Security Summit in Romania, supportata anche dall'Itu, occasione in cui ci confronteremo con altre strutture a livello europeo cercando di proporre soluzioni e idee, finalizzate a contrastare il cyber crime.

"*Le reti* – ha osservato il più grande allievo di McLuhan vivente Derrick de Kerckhove – *sono il liquido amniotico entro cui siamo immersi, la connettività è il sistema omeopatico che ci nutre e che guida i nostri movimenti*". Come intendete sviluppare la collaborazione con le università e le imprese?
Quando parliamo di rete oggi parliamo di circa 60 trilioni di pagine web, di 4 zettabytes di dati e circa 4 miliardi di oggetti connessi che si stima saranno 80 entro il 2020. È evidente che con questi numeri padroneggiare il nuovo alfabeto digitale è già una realtà, che deve intersecarsi con la diffusione di una *culture security* adeguata. La Fondazione sta ampliando le collaborazioni con le università e con i ricercatori delle aziende che oggi lavorano nel settore della sicurezza informatica. Inoltre, stiamo collaborando con hacker etici, sul modello della *Responsible Disclosure* già adottato in Olanda con successo. I risultati di queste collaborazioni porteranno a delle pubblicazioni sui temi della Cyber Security indirizzate ai decisori aziendali, e sui circuiti di pagamento e Apt. Oltre a queste iniziative editoriali metteremo in campo alcuni moduli formativi e diversi progetti europei in collaborazione con le università italiane ed estere.

Il processo di *Digital Transformation* implica una progressiva evoluzione dei modi di intendere e di praticare la sicurezza. Nel nostro paese non appare ancora diffusa questa consapevolezza. Cosa possiamo fare?
Nell'era digitale le tecnologie, oltre a trasformare ogni aspetto della nostra vita, offrono alle aziende strumenti per diventare più veloci, più creative, e in contatto diretto con i consumatori. Le opportunità sono enormi, ma il successo dipende anche dalla comprensione dei rischi che queste tecnologie possono generare. I temi della Cyber Security sono i pilastri della trasformazione digitale, la sicurezza non è più una problematica a se stante, ma è diventata una componente del business. Ricordiamoci che il processo di trasformazione digitale ha bisogno di una specifica strategia di Cyber Security che sappia affrontare le nuove minacce, ma anche gli aspetti di conformità normative, che regolano questo delicato ambito. La trasformazione digitale richiede una sicurezza *by design*, che vuol dire: proteggete i vostri dati, proteggerete il vostro business!

Quali sono le nuove frontiere della sicurezza, su cui la ricerca dovrà puntare maggiormente l'attenzione per presidiare le aree di maggiore vulnerabilità?
Oggi parliamo ancora di Infrastrutture Critiche, ma cosa sarà veramente critico nei prossimi anni? Oggi non consideriamo gli autoveicoli come infrastruttura critica, ma proviamo a immaginare una rete che governi la connettività di tutti i veicoli sulle strade e spingiamoci a uno scenario più complesso: quello dei veicoli senza pilota. Non è forse anche questa un'infrastruttura critica? Quali conseguenze avrebbe un attacco a questa rete? Pensiamo ai droni, oggi realtà in crescita, immaginandone lo sviluppo commerciale. Ormai sono molte le aziende che stanno pensando al loro utilizzo per velocizzare le consegne. Anche i droni in scenari più complessi possono essere considerati come un'infrastruttura critica? Quello che oggi non è critico potrebbe esserlo domani, in questo scenario di *sharing economy*, occorre accelerare sul tema dell'*Information Sharing*.

Scusi, cosa vuol dire in concreto?
Che la condivisione di piattaforme condivise sugli incidenti e sulle minacce sarà fondamentale insieme a programmi di Cyber Intelligence che possiamo anche definire come *Competitive Intelligence*. La Fondazione di Poste Italiane ripone molta attenzione ai temi dell'Information Sharing, in quest'area stiamo collaborando, da tempo, a un progetto europeo guidato dalla Polizia Postale. Quest'anno avvieremo, in collaborazione con il mondo universitario, delle atti-

vità di ricerca su tecnologie di *machine learning* applicate alla Cyber Security, considerando che questo ambito sarà la prossima frontiera della sicurezza. Il Mit, proprio su questa problematica, ha già presentato la propria esperienza durante la conferenza "Big Data Security" tenuta da Ieee a New York.

Big Data, *machine learning*, Internet delle cose, pagamenti elettronici: vi sono le competenze per affrontare la qualità e la quantità delle nuove minacce, rese ancora più insidiose dalla capillare diffusione degli smartphone che consentono di effettuare qualsiasi transazione in regime di costante mobilità?
In uno scenario di iperconnettività in rapida crescita, dai dispositivi medicali alle autovetture, all'uso dei sensori nel contesto emergente delle smart city, è evidente che la sicurezza diventerà una questione di rilevanza sociale. Gli scenari di attacco stanno mutando profilo e, mentre oggi parliamo di una insidiosa perdita di dati, in un domani neanche troppo lontano parleremo probabilmente di possibili perdite di vite umane. Gli approcci tradizionali alla formazione sulla sicurezza hanno bisogno di un riesame immediato, dobbiamo rapidamente aumentare gli sforzi per educare una nuova generazione di esperti in sicurezza informatica. È tempo, insomma, di rimodellare la formazione in sicurezza informatica e di ritararla sui paradigmi dello sviluppo professionale continuo.

Siamo di fronte a una vera e propria guerra delle informazioni, sottile e silenziosa in cui non è facile leggere e interpretare dati ed "eventi critici". Bisognerà ripensare la logica dei Soc, ma anche il profilo del *security manager*. State lavorando in questa direzione?
Nei prossimi anni i dati prodotti del nostro Datacenter supereranno quanto è stato prodotto nell'intera storia umana. Il *security manager* avrà il complesso compito di tenere questi dati al sicuro. Tutto ciò richiederà una capacità di gestire pianificazioni, policy e processi, particolarmente complessi. Sempre più rilevanza avranno i Big Data, che richiederanno ai professionisti della security competenze specifiche di Data Analyst. Queste avranno un ruolo fondamentale nella gestione delle frodi, degli incidenti e nelle applicazioni di Cyber Intelligence. In prospettiva il *security manager* sarà sempre di più una figura vicina alle linee di business e si caratterizzerà per una buona capacità relazionale e per il contributo che sarà chiamato a dare sui modelli di sviluppo dell'organizzazione. Consapevole di questo trend, la Fondazione lavorerà con le università, al fine di allineare i processi di formazione e di aggiornamento dei saperi alle effettive esigenze del mercato.

State avviando un'attività editoriale. Può anticiparci qualche titolo e gli ambiti che avete deciso di presidiare con l'aiuto di alcuni tra i massimi esperti del settore?
Stiamo lavorando a due pubblicazioni, la prima affronterà il tema della sicurezza dei circuiti Atm. Oggi la sicurezza approccia questo tema sotto l'aspetto della protezione da attacchi fisici, la ricerca si concentrerà su aspetti legati al crimine informatico che sono in continuo aumento. Un contributo importante a questa ricerca sarà dato anche dal Consorzio Bancomat che pubblicherà, con noi, delle linee guida che condivideremo con le istituzioni e fornitori di soluzioni di Atm. La seconda pubblicazione affronterà il tema degli Advanced Persistent Threat (Apt) e sarà orientata ad analizzare le minacce attuali e la loro evoluzione. Sempre sul fronte della comunicazione occorre ricordare il progetto, già avviato, relativo a una newsletter mensile, che è possibile richiedere sul nostro sito web (www.gcsec.org). Stiamo anche verificando la fattibilità di una pubblicazione specifica sui temi di Cyber Security insieme ad alcune organizzazioni internazionali nell'ottica di coltivare una cultura diffusa della sicurezza che permetta di creare quelle condizioni per fare il "salto" verso la completa trasformazione digitale del nostro paese. Un "salto" che ovviamente dovrà essere fatto in "assoluta" sicurezza, per tutti e per tutto. Noi saremo a vigilare, perché questa prospettiva diventi realtà.

Ma.C.