Security Transformation – La Digital transformation passa dalla sicurezza

By **Nadia Garbellini** - 30/10/2018

Si è svolto stamattina l'evento gratuito organizzato da T.net Italia in collaborazione con Fortinet

Il GDPR è ormai in vigore da sei mesi, ma la confusione in tema di sicurezza è ancora tanta. Per rispondere a dubbi e incertezze **T.net Italia**, in collaborazione con il suo storico partner **Fortinet,** ha organizzato il workshop **Security Transformation – La Digital transformation passa dalla sicurezza.**

Il workshop si è aperto con l'intervento di **Francesco Mazzola**, founder di T.net, sullo scenario complessivo attuale. In particolare, Mazzola si è soffermato sulla confusione normativa relativa agli obblighi imposti dal GDPR. L'adozione del regolamento europeo da parte del nostro paese è infatti avvenuta in modo irrituale e non lineare. In primo luogo, il GDPR abroga la Direttiva 95/46/UE, vale a dire quella su cui si basa la legge 196/2003 sulla privacy. Quest'ultima, al contrario, non è stata abrogata, ma novellata tramite il Dlgs 101/2018 – anche se il precedente governo aveva più volte ribadito la necessità di una sua abrogazione. Ne risulta che, oggi, chi si occupa di trattamento dei dati personali deve fare riferimento a tre diverse impalcature giuridiche. Per non parlare delle norme di Garanzia, non presenti nel GDPR, che verranno delineate dal Garante che ha 90 giorni per farlo. In tutto questo, con norme incomplete, frammentarie e a volte persino incoerenti, le imprese rischiano multe salate e persino la reclusione.

Le difficoltà per le organizzazioni, però, non si esauriscono qui: va infatti operata una distinzione tra dati personali sensibili e non, ma soprattutto tra dati aziendali personali e non personali. Questi ultimi, che costituiscono il cuore dei dati aziendali – si pensi ai dati finanziari o ai brevetti – sono quindi al di fuori dell'ambito di applicazione del GDPR, ma devono comunque essere protetti.

Si pensi, inoltre, che il Dlgs 101/2018 prevede che, nel caso delle PA, la compliance debba essere garantita senza oneri aggiuntivi, vale a dire a costo zero. È impensabile che la PA possa aggiornarsi e diventare digitale se non ci si decide ad effettuare degli investimenti in questo senso.

Affrontare il percorso verso la **security transformation** – cioè il cambiamento che il mondo della sicurezza deve affrontare per stare al passo con la digital transformation – deve quindi iniziare ad essere percepito dalle organizzazioni come un investimento necessario.

Quali sono, quindi, i passi principali da compiere in questa direzione?

1. **Assessment As Is**, cioè una fotografia dello stato attuale non solo in termini di sicurezza, ma anche di processi; questi ultimi infatti sono fondamentali perché le misure di sicurezza possano effettivamente essere implementate in modo corretto e quindi efficiente ed efficace. In genere richiede dalle 2 alle 6 settimane
2. **Gap Analysis**, vale a dire la misurazione della distanza tra lo stato delle cose e i requisiti ideali
3. **Matrice del rischio**, che mette in evidenza tutte le criticità al fine di valutare l'indice di esposizione al rischio
4. **Action Plan**, vale a dire la definizione delle priorità e quindi di un piano di implementazione che porti a concludere il percorso tipicamente nel giro di 2 o 3 anni
5. **Audit**

Il secondo intervento è stato a cura di **Alessandro Raciti**, COO di T.net, dal titolo **T.net Security Solutions: System Provider e Integrator insieme per la sicurezza dei dati**.

La relazione di Raciti è infatti incentrata a descrivere il ruolo di T.net, che è insieme System Integrator e Service Provider.

Se il primo si occupa di far comunicare tra loro le diverse componenti hardware e software, anche di vendor molto eterogenei, il secondo si occupa di svolgere funzioni as a Service, che il cliente paga a consumo – come ad esempio fungere da Manager Service Provider.

T.net quindi è in grado di occuparsi della sicurezza aziendale a 360°.

È qui che entra in gioco **Fortinet**, di cui il terzo relatore è rappresentante. **Giorgio D'Armento**, DLB Manager di Fortinet, tratta infatti il tema **Fortinet Security Fabric: Come integrare e proteggere i dati per le aziende**.

Fortinet, multinazionale americana nata all'inizio dgli anni 2000, quando il problema della sicurezza era scarsamente percepito, conta circa 6000 dipendenti (di cui 55 in Italia) con ben 500 ingegneri al lavoro nei dipartimenti di R&D. Questo perché Fortinet, a differenza degli altri competitor, realizza tutto il software in house, senza affidarsi a terze parti. A prova di questo basi osservare il numero di brevetti depositati: più di 500, circa 3/5 volte rispetto ai concorrenti.

Scopo dell'azienda è quello di offrire soluzioni ai problemi in modo pratico. Così facendo, fa proprio l'approccio secondo cui la security non è solo una difesa, ma anche uno strumento di ottimizzazione.

Il cliente vuole automation, e pretende che tutto funzioni all'unisono. I pillars di Fortinet consentono di coprire tutto ciò che c'è in azienda: network, applicazioni, cloud, email, analytics e molto altro.

Fortinet imlementa inoltre la sicurezza interna all'organizzazione, e non solo la protezione dall'esterno. Un **Internal Fragmentation Firewall** permette di fare proprio questo, in modo che eventuali intrusi – o dipendenti sprovveduti – possano avere accesso ovunque senza restrizioni né controllo.

C'è poi tutto il mondo **OT (Operations Technology)** e non solo IT. Rispetto a quest'ultimo, qui le priorità sono ribaltate: poiché la produzione non si deve mai fermare, l'availability del servizio viene prima della confidenzialità. È quindi necessario studiare delle soluzioni specifiche, che consentano di proteggere i dati aziendali senza mettere in pericolo la continuità del workflow.

Infine, ci sono le soluzioni **SD-WAN**, che consentono di risparmiare tempo e denaro nella gestione della connettività. Sappiamo che le organizzazioni diventano sempre più complesse, che si moltiplica il ricorso al cloud, e che le reti di fornitura sono sempre più articolate. Ciò imporrebbe il passaggio a infrastrutture WLAN più costose. Adottare il driver SD-WAN consente invece di prendere connessioni a basso costo, aggregarle e gestirle in modo dinamico.

Tutte le soluzioni di sicurezza sono gestite e monitorate attraverso una singola console, che consente di gestire ogni singolo aspetto della sicurezza aziendale razionalizzando i processi e consentendo un notevole risparmio di tempo e denaro.

Nadia Garbellini