LA RIVISTA DEI DIRETTORI AMMINISTRATIVI E FINANZIARI

# ANDAF magazine

2
Anno 16 - n. 2
Aprile 2019
Trimestrale
Copia omaggio

## AGILE FINANCE PER LA LEADERSHIP DIGITALE DEL CFO

## LA NECESSITÀ DI INCREMENTARE LA SICUREZZA INFORMATICA DELLE AZIENDE

ISSN 2281-468X

Poste Italiane S.p.a. – Spedizione in abbonamento postale – 70% Roma AUT.C/RM/26/2004

# LA NECESSITÀ PER LE AZIENDE DI INCREMENTARE LA PROPRIA **SICUREZZA INFORMATICA**


***NEL PIENO DELL'ERA DELLA DIGITAL TRANSFORMATION SI TENTA, CON L'EMANAZIONE DI SPECIFICHE NORME DI LEGGE, DI POTENZIARE LA SICUREZZA INFORMATICA DELLE AZIENDE. L'INSUFFICIENZA DEGLI INVESTIMENTI NELLA CYBERSECURITY È PERÒ ANCORA CAUSA DI UN ELEVATO RISCHIO.***



di ROBERTO CECILIA SANTAMARIA
*Managing Partner Agic Technology*

e MARCELLO MANCINI
*Associate Partner AiComply*

Il tema della sicurezza informatica nel nostro Paese rappresenta oggigiorno un punto di massima allerta per diverse aziende.
L'emanazione delle più recenti normative comunitarie e italiane in tema di protezione delle persone fisiche (con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati) e di sicurezza delle reti e dei sistemi informativi, unitamente all'aumento del numero degli attacchi informatici, hanno certamente contribuito alla generazione di una maggiore consapevolezza del rischio cyber cui le aziende sono quotidianamente esposte.
L'accrescimento del livello di attenzione è ben riscontrabile anche da un punto di vista economico; si pensi, infatti, che nel 2018 gli investimenti delle aziende italiane per la sicurezza informatica sono aumentati di circa il 12% (come si evince dal Rapporto sulla sicurezza ICT elaborato nel 2018 da Clusit) rispetto al precedente anno.

Va inoltre evidenziato lo stretto legame esistente tra l'aumento degli investimenti in cybersecurity e il propagarsi della digital transformation, i cui impatti nel quotidiano sulla sicurezza informatica delle aziende sono molteplici.
Si pensi, ad esempio, all'evoluzione nell'utilizzo di internet, che rappresenta oggigiorno per le imprese di tutti i settori e di tutte le dimensioni un fondamentale strumento di collaboration. Infatti, la collaborazione in azienda avviene sempre meno attraverso incontri di persona e sempre più attraverso l'ausilio della rete internet, che rende possibile la comunicazione a distanza e in tempo reale, e la condivisione di dati e informazioni.

Oppure, ancora, si pensi a come stanno cambiando le aree di lavoro attraverso l'adozione di modelli organizzativi delle attività basati su un utilizzo efficiente e produttivo degli spazi fisici. Il prendere piede del *Modern Work Place* comporta l'abbandono del concetto del posto di lavoro legato a un luogo fisico a favore della possibilità di lavorare da qualunque posto, in qualunque momento e da qualsiasi dispositivo, mantenendo sempre elevata la produttività. Un modo di lavorare più agile, insomma.
Sia internet che il *Modern Work Place* contribuiscono al cambiamento radicale del concetto di sicurezza informati-




ca cui siamo abituati: il potenziamento della nostra capacità di comunicare, indipendentemente dal fatto che ci troviamo in ufficio oppure dalla parte opposta del pianeta, comporta una dispersione geografica del dato e delle informazioni. Nella vecchia concezione di sicurezza informatica era sufficiente "mettere al sicuro" il perimetro dell'azienda entro cui il dato veniva gestito; oggi non è più così, dal momento che il dato è per lo più maneggiato al di fuori dell'impresa (ad esempio, attraverso notebook o smartphone). Anche il più recente sviluppo di tecnologie in grado di rendere i sistemi informativi capaci di prestazioni fino ad ora proprie soltanto dell'intelligenza umana ha posto numerose problematiche dal punto di vista della cybersecurity.

Si pensi, infatti, che l'Intelligenza Artificiale si basa su aspetti quali l'analisi dei big data, il riconoscimento delle immagini, l'elaborazione del linguaggio naturale, ecc.; tutti temi sensibili in ambito di protezione dei dati personali e di tutela delle libertà e dei diritti fondamentali dell'essere umano.

D'altro canto, l'Intelligenza Artificiale potrebbe lei stessa rappresentare un valido supporto per l'implementazione della cybersecurity. Infatti, piattaforme basate sull'Intelligenza Artificiale potrebbero essere adoperate per rilevare autonomamente ed eliminare minacce cyber in tempo reale (ad esempio, *ransomware, brute force, trust attack*, ecc.).

**Una sintetica panoramica sull'evoluzione normativa**

I Legislatori dei Paesi Membri dell'UE stanno mostrando una forte attenzione alla tutela della sicurezza informatica, lavorando per unificare le prospettive nel settore della cybersecurity. Il Regolamento UE nr. 679/2016 (anche *General Data Protection Regulation* o GDPR), di cui se ne è più ampiamento sentito parlare da un anno a questa parte, ne è un esempio.
Il GDPR, che dal 25 maggio 2018 è divenuto definitivamente applicabile nei Paesi Membri dell'UE, all'art. 32 prevede in capo ai titolari e ai responsabili del trattamento l'obbligo di mettere in atto misure tecniche e organizzative idonee a

garantire un livello di sicurezza adeguato al rischio connesso al trattamento.
Analizzando tale previsione normativa, risultano evidenti due requirement:

- la necessità di adottare misure tecniche e organizzative;
- la necessità di effettuare un'analisi dei rischi per ciascun trattamento.

Relativamente alle misure tecniche e organizzative, va detto che queste devono essere in grado di gestire la sicurezza informatica sia dal punto di vista della governance dei sistemi informativi, sia da quello delle soluzioni tecnologiche da adottare.
Invece, in relazione all'analisi dei rischi, è utile evidenziare che già nella sezione introduttiva del GDPR il concetto di rischiosità assume un ruolo fondamentale.
In particolare, il "considerando nr 83" specifica che per mantenere la sicurezza il titolare o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi. Nella valutazione del rischio per la sicurezza dei dati sarà opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati.
Appare quindi evidente una forte inversione di rotta rispetto alla previgente normativa nazionale in tema di protezione del dato personale (il D.Lgs. 196/2003 noto anche come *Codice Privacy*), in quanto quest'ultima prevedeva l'adozione delle misure minime di sicurezza ben individuate all'interno dell'allegato B "Disciplinare tecnico in materia di misure minime di sicurezza" del *Codice Privacy*.
Il GDPR, al contrario, non individua l'elenco delle misure minime da adottare ma si limita a citare alcuni esempi. È pertanto in capo al titolare o al responsabile del trattamento stabilire quali misure tecniche e organizzative adottare, sulla base di una preliminare analisi del rischio cui sono esposti i trattamenti.

Un'altra normativa di recente emanazione, sensibile al tema della cybersecurity, è la Direttiva 2016/1148 (meglio nota come Direttiva NIS), attuata nel nostro ordinamento dal D.Lgs. 65/2018.
In sintesi, tale Direttiva intende definire una strategia nazionale di cybersecurity e le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi volto a prevenire i rischi, a minimizzare l'impatto degli *incident* e a garantire la continuità del servizio.
Il D.Lgs. 65/2018 si rivolge a specifiche categorie di soggetti (gli operatori di servizi essenziali quali, a titolo meramente esemplificativo, imprese dei settori energy, trasporti e bancario, ecc.) e prescinde dal concetto di trattamento del dato personale su cui si fonda invece il GDPR.
L'art. 12 del D.Lgs. 65/2018 prevede, in capo ai suddetti operatori di servizi essenziali, l'obbligo di adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi relativi alla sicurezza della rete e dei sistemi informativi che utilizzano nello svolgimento delle loro attività. Il D.Lgs. 65/2018 è quindi perfettamente in linea con le previsioni del GDPR.
Anche nel settore della Pubblica Amministrazione, nel corso del 2017, sono state pubblicate in Gazzetta Ufficiale le "Misure minime per la sicurezza ICT delle Pubbliche Amministrazioni" elaborate da AgID. Si tratta di un documento che individua le misure preventive da porre in essere per impedire il successo di un attacco informatico.
Appare quindi evidente una sinergia tra il GDPR, il D.Lgs. 65/2018 e le "Misure minime per la sicurezza ICT delle Pubbliche Amministrazioni" indirizzata al potenziamento della cybersecurity.
Lo scopo del Legislatore non è quindi quello di combattere i singoli attacchi informatici, ma piuttosto quello di bloccare il cybercrime attraverso una strategia condivisa sia a livello europeo che nazionale.

**Gli attacchi informatici: un trend in crescita**
Secondo il Rapporto elaborato nel 2018 da Clusit (Associazione Italiana per la Sicurezza Informatica, costituita nel 2000 e composta da un gruppo di esperti che si occupa della ricerca sulla cybersecurity finalizzata alla pubblicazione annuale di un rapporto statistico) sulla sicurezza ICT in Italia e nel mondo, il 2017 è stato l'anno del *malware* (si pensi che il 95% circa degli attacchi informatici avvenuti nel corso del 2017 ha utilizzato come vettore di attacco il *malware*) con 1.127 attacchi "gravi" registrati a livello mondiale – circa il 7% in più rispetto al 2016 – e un danno di quasi 10 miliardi di euro per l'Italia.
Sempre dal Rapporto sulla sicurezza ICT, elaborato nel 2018 da Clusit, emergono altri dati significativi di seguito riportati. La maggior parte (il 76% circa) degli attacchi complessivamente registrati è stata classificata come cybercrime, perché si tratta di attacchi finalizzati a sottrarre denaro, informazioni, o entrambi.
Nel 2017, rispetto al 2016, la crescita percentuale maggiore di attacchi gravi è stata osservata in relazione alle categorie *Multiple Targets* (+353%), *Research/Education* (+29%) e *Software/Hardware Vendor* (+21%), seguite da *Banking/Finance* (+11%), *Healthcare* (+9%) e *Critical Infrastructures* (+5%).

A fronte dell'aumento degli attacchi informatici molte aziende stanno decidendo di puntare su tecnologie avanzate, ad esempio il *cloud computing*, per elevare i propri standard di sicurezza e tutelarsi da eventuali attacchi informatici. Secondo le più recenti indagini di mercato, la spesa in sicurezza informatica delle aziende italiane ha raggiunto un valore di 1,19 miliardi di euro – in crescita del 9% su base annua – dopo aver registrato un incremento del 12% nel 2017.
A trainare il mercato sono soprattutto le grandi imprese con il 75% della spesa complessiva, concentrata su adeguamento al GDPR e su componenti di sicurezza come *network security, business continuity & disaster recovery,* ed *endpoint security*.
La maggior parte delle aziende che investe nella sicurezza

informatica lo fa stanziando risorse solo in caso di necessità, sono poche le aziende che definiscono piani di investimento strategici nella sicurezza informatica.
Al momento, gli investimenti delle aziende in cybersecurity non appaiono quindi ancora adeguati alla minaccia.

**Implementare la sicurezza informatica in azienda: un esempio di approccio metodologico**

La sicurezza informatica, intesa come l'insieme dei mezzi e delle tecnologie tesi alla protezione dei sistemi informativi in termini di disponibilità, confidenzialità e integrità, deve basarsi sia su aspetti di governance che su aspetti tecnologici.
Pertanto, le aziende che intendono potenziare la propria sicurezza informatica dovranno in primo luogo effettuare una rilevazione di tutti gli asset informatici e delle minacce, delle vulnerabilità e dei rischi a questi connessi. Successivamente, sarà possibile individuare le misure di sicurezza maggiormente idonee da adottare, che potranno essere di duplice natura: misure di governance e misure tecnologiche.

L'approccio da seguire è pertanto basato sui seguenti step:

- effettuare un inventario degli asset;
- effettuare una gap analysis;
- individuare le azioni correttive necessarie (remediation plan/action plan).

Tra le misure di governance rientrano, a mero titolo di esempio, l'adozione di modelli organizzativi per la gestione delle normative sopra richiamate, l'analisi dei rischi, la chiara definizione di ruoli, responsabilità e compiti, la formalizzazione dei processi, la gestione dello smart working, ma anche la formazione degli utenti. Spesso, infatti, il fattore umano rappresenta l'anello debole della catena della cybersecurity; l'educazione è quindi una componente fondamentale per diffondere i principi della cybersecurity.
Tra le misure tecnologiche rientrano invece, a mero titolo di esempio, le soluzioni informatiche messe a disposizione dai grandi player del mercato della cybersecurity (ad esempio, Microsoft, McAfee, Symantec, Sophos, ecc.).
A prescindere dalla natura delle misure di sicurezza da implementare, è ad ogni modo necessario tenere a mente il tipo di rischio che si desidera mitigare; inoltre, è anche opportuno pensare alla cybersecurity come ad una misura preventiva, in modo da ridurre il rischio di incidenti.
Ciò premesso, unitamente ai cambiamenti al nostro modo di lavorare dovuti alla digital trasformation, per implementare la sicurezza informatica è necessario porsi un quesito: cosa vogliamo proteggere?
Sicuramente la risposta puntuale a questa domanda ce la potrà fornire il risultato dell'analisi dei rischi ma, in generale, è possibile concludere che sarà necessario:

- proteggere l'identità di chi accede a un sistema;
- proteggere i dati residenti nel sistema;
- proteggersi dalle minacce cui sono esposti i sistemi.

Come suddetto, la sicurezza informatica non può più limitarsi a difendere il perimetro aziendale. La possibilità di collegarci ai sistemi aziendali da qualsiasi luogo implica che la linea di difesa debba essere ampliata all'identità digitale e alla gestione degli accessi. Inoltre, l'autenticazione attraverso password non è più sufficiente: la maggior parte delle violazioni alle infrastrutture aziendali avviene proprio in seguito al crack di una chiave di accesso.
È quindi necessario affiancare alle password altri criteri di identificazione, quali ad esempio tecniche di *Multi Factor Authentication* basate su dati biometrici o token.
In questo modo la protezione dell'identità assicura che ciascun account desideri accedere a un sistema informativo debba prima superare un robusto processo di riconoscimento e autenticazione.
Relativamente alla protezione del dato, invece, è anzitutto necessario che questa sia commisurata alla tipologia del dato stesso. Quindi, una classificazione preliminare del dato può consentire di indirizzare meglio le misure di sicurezza. Bisogna inoltre considerare che il dato può essere archiviato su vari dispositivi che escono anche al di fuori del perimetro aziendale (ad esempio gli smartphone) e che può essere condiviso con altri utenti. È pertanto raccomandabile implementare una protezione persistente che segua i dati ovunque si trovino, garantendo che rimangano protetti indipendentemente da dove sono archiviati o con chi sono condivisi.
In ultimo, la definizione di chi possa accedere ai dati e quali operazioni vi possa eseguire rappresenta un'altra misura di protezione del dato.
Per quanto attiene alla protezione dalle minacce, si rileva invece la necessità di individuare comportamenti sospetti in tempo reale, in modo da intercettarli tempestivamente e limitare in questo modo i danni.
Lo sviluppo tecnologico può rappresentare un valido supporto per l'implementazione delle misure di sicurezza informatica; la *Digital Transformation* è infatti in grado di offrire soluzioni automatizzate basate sul *machine learning* e sull'Intelligenza Artificiale per la protezione dell'identità, del dato e per l'intercettazione delle minacce.

I meccanismi di protezione sopra descritti sono già fruibili nelle soluzioni tecnologiche a disposizione delle aziende (soprattutto in quelle basate sul *cloud computing*). Si tratta, molto spesso, di funzionalità attivabili a fronte di investimenti minimi se commisurati al rischio sotteso.
Ad esempio, attraverso la piattaforma Microsoft Office 365, oggi utilizzata dalla maggior parte delle imprese, è possibile potenziare la sicurezza informatica con un investimento contenuto grazie a strumenti di *Identity and Access Management*, *Information Protection* e *Threat Protection*. Nonostante tutto ciò, risultano ancora poche le organizzazioni che decidono di implementare in maniera adeguata la propria sicurezza informatica. Anche se i fornitori di soluzioni tecnologiche stanno investendo molto nella cybersecurity, siamo ancora lontani da un accettabile livello di sicurezza informatica.

AGIC Technology

# Cybersecurity & Data Protection

**16 aprile 2019**
*Microsoft House - Milano*

**17 aprile 2019**
*Microsoft House - Roma*

Due incontri dedicati alla **Cybersecurity** con un focus sullo stato attuale del **GDPR** attraverso l'analisi di casi pratici.

Per info e prenotazioni:
www.agictech.com

Nel pieno dell'era della **Digital Transformation** si tenta, con l'emanazione di specifiche norme di legge, di potenziare la **Cybersecurity** nelle aziende, attraverso soluzioni tecnologiche che, unite alle opportune misure di governance, assicurino la **protezione del dato** e la **prevenzione** da attacchi informatici.

**TECHNOLOGY**
AT YOUR SERVICE

**INFO & CONTATTI**
www.agictech.com
info@agictech.com

**LE NOSTRE SEDI**
Milano Roma Brindisi
Bologna Napoli Tirana

Gold Microsoft Partner
Microsoft