Cyber security, Confindustria: “Primi segni di una nuova era in Italia, lo dicono i dati: ecco perché”

La sicurezza informatica non coinvolge più i soli i responsabili ICT, ma tutte le figure aziendali, fino al top management. Le minacce aumentano, insieme alla consapevolezza che nessuno è al sicuro. E così, grazie anche al GDPR e alla crescente opera di sensibilizzazione, cresce la domanda di cybersecurity, Vediamo i trend

Alberto Tripi
Delegato di Confindustria per la Cybersecurity e Vicepresidente Anitec-Assinform con Delega agli Studi e Indirizzi Strategici

La sicurezza delle risorse e degli asset ICT è oramai un tema centrale in tutte le organizzazioni. Non è più solo materia per i responsabili dell'ICT, ma del top management. Essa infatti si va sempre più affermando come prerequisito per ogni tipo di attività produttiva o di servizio. Questa che finora era forse una solo una sensazione ora è confortata dai numeri. **La spesa in cyber security nel 2017 è cresciuta del 10,8%, a 900 milioni di euro; cinque volte in più rispetto alla media del mercato digitale italiano. Stiamo entrando insomma nell'era della cyber security trasversale e pervasiva nelle e tra le organizzazioni.**

Gdpr e Nis principali driver della spesa cyber security

La crescente attenzione alla **Cyber security** consegue sia all'aumento delle minacce, sia all'evoluzione del quadro regolatorio a livello europeo, con l'entrata in vigore nel maggio di quest'anno del General Data Protection Regulation (**GDPR**) e con il recepimento della **direttiva NIS** (Network Information Security).

Il GDPR uniforma la legislazione dei paesi membri in materia di protezione dei dati personali e pone in capo alle aziende nuovi obblighi.

Il NIS, volto a rafforzare la capacità di gestione della sicurezza di reti e sistemi a livello europeo, è stato recepito nel Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica in Italia (2017) ed anche dal Piano Triennale per l'Informatica nella Pubblica Amministrazione 2017-2019.

Nessuno è esente da rischi

Nessuna organizzazione è esente da rischi. Negli ultimi due anni sono stati violati i sistemi di aziende che operano a livello mondiale ed **è cresciuta rapidamente la diffusione di malware in grado di colpire in modo indistinto operatori telefonici, utility, ospedali, enti pubblici, piccole imprese e professionisti.**

Ad accrescere i rischi concorrono le tecnologie mobili e la necessità, in logica di integrazione evoluta, di aprire i sistemi a partner clienti e fornitori.

Le app, sia quelle a supporto delle attività del personale interno e a maggior ragione quelle destinate al dialogo con i clienti ed interlocutori esterni, sono una leva potentissima di innovazione, ma sono spesso ancora acerbe sotto il profilo della sicurezza.

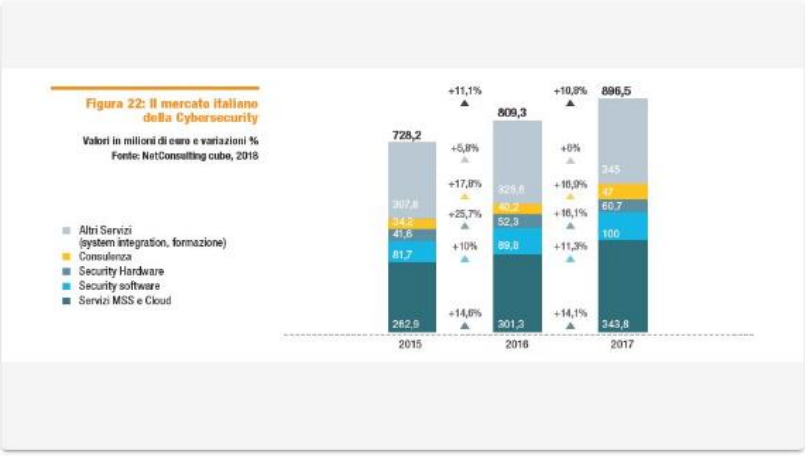
L'apertura dei servizi ICT aziendali a terzi, o a servizi di terzi, sta crescendo moltissimo, e per di più non avviene più solo con API, ma anche con tecnologie **IoT**. Queste ultime consentono scambi di dati e informazioni tra oggetti connessi rendendo possibili cose sino a pochi anni fa inimmaginabili, dall'ambito urbano a quello logistico, ma si presentano anche come nuovi canali per attacchi e quindi ampliano il perimetro da proteggere a nuove componenti software e di rete e ad appliance connesse alla sensoristica.

Cresce la domanda di cybersecurity

La conferma della centralità della tematica non viene però dalle parole o dalle visioni, viene dai dati. **La domanda di cybersecurity in Italia, come si diceva all'inizio, è cresciuta nel 2017 del 10,8%, ad un tasso cinque volte superiore a quello del mercato digitale italiano, sfiorando i 900 milioni di euro (dati Netconsulting). E ci si aspetta che il trend prosegua anche per i prossimi anni.**

Alla progressione 2017 hanno contribuito varie componenti. Sia quelle che incidono maggiormente sulla spesa, come i ***security managed services*** e la ***cloud security*** (+14,1%); sia quelle riguardanti ambiti minori in valore assoluto, ma non meno rilevanti, come ***l'hardware*** **e** ***software security*** (rispettivamente cresciuti del 16,9% e 11,3%, spinti dagli investimenti su ***endpoint*** **e** ***network security, application security*** **e** ***threat intelligence***) oltre che dalla spesa per consulenza (+16,9%). Significativo, anche se con ritmi di crescita meno sostenuti (+6%) l'apporto degli altri servizi del mercato Cybersecurity, come quelli per ***vulnerability assessment*** su sistemi tradizionali, apparati mobili e applicazioni, e il supporto al *security & risk assessment.*

Le soluzioni di ***threat intelligence*** – basate prevalentemente su algoritmi di ***machine learning*** e **Intelligenza Artificiale**, e trasversali a vari ambiti, rappresentano il segmento più dinamico (+18,7% nel 2017 e in ulteriore crescita nei prossimi anni).



La spinta del GDPR

Come anticipato, a rafforzare il trend di crescita del mercato della Cybersecurity ha contribuito la richiesta di supporto al percorso di adeguamento al GDPR, provenuta da aziende ed enti soprattutto nella seconda parte del 2017 e nei primi mesi del 2018. Ma non è tutto qui, perché **l'impianto stesso del GDPR innesca attività operative e manutentive di sicuro spessore** e che proseguiranno almeno nel medio termine. Basti pensare che esso impone attività continue riguardanti

- **la mappatura di tutti i dati trattati**, la valutazione e il conseguente adeguamento delle misure di protezione, inclusi i sistemi di crittografia;
- la possibilità dell'interessato di esercitare il **diritto d'accesso ai dati trattati e il diritto all'oblio**;
- il **diritto alla portabilità dei dati,** ovvero di ricevere e trasferire liberamente a un altro titolare i propri dati personali;
- la **notifica all'authority e agli interessati eventuali incidenti o *data breach***.

In molti casi – enti pubblici e realtà appartenenti al mondo sanitario, che trattano dati su larga scala – l'adeguamento sta determinando anche cambiamenti organizzativi, con la creazione di nuove figure, come il **DPO** (Data Protection Officer), e in ogni caso la revisione della documentazione e dei processi relativi ai vari attori coinvolti nella gestione dei dati (titolare, responsabile, incaricati), portando alla costruzione del cosiddetto "Organigramma della Privacy".

Cybersecurity, trend in crescita

In conclusione, e anche in Italia, sia per la crescente coscienza della centralità della sicurezza informatica nel business, sia per le spinte che provengono dalla normativa, **per la Cybersecurity è atteso un trend in crescita e la progressiva apertura nuovi fronti, con il coinvolgimento di un sempre maggiore novero di imprese ed un ulteriore impegno delle amministrazioni pubbliche**. La stima è di una crescita del mercato tra l'11 e il 13% tra il 2018 e il 2020. Ci si attesterà sui valori di crescita più elevati quanto più le aziende, e non solo quelle di grandi dimensioni, attribuiranno ruoli e responsabilità specifiche per la sicurezza informatica e coinvolgeranno quote sempre più rilevanti del personale alla tematica. **La sicurezza informatica, infatti, non coinvolge più i soli specialisti, ma tutte le figure aziendali**. E infatti, parte importante della spesa in Cybersecurity riguarda e riguarderà proprio le competenze e la formazione a tutti i livelli e in tutti gli ambiti, ciò che presuppone anche una sensibilizzazione continua e coerente, per portata e impegno, alla continua evoluzione delle problematiche da affrontare.

A quest'ultimo riguardo, quello della sensibilizzazione, una nota positiva c'è, e non da poco. Viene dalla collaborazione sempre più stretta tra il **Dipartimento delle Informazioni per la Sicurezza** (DIS, operante in seno alla Presidenza del Consiglio dei Ministri), **l'AgID** e Confindustria. Essa ha permesso di inserire la cyber security tra i temi chiave dell'innovazione digitale nei programmi territoriali di sensibilizzazione della rete dei **Digital Innovation Hub** regionali promossi da Confindustria e dei **Competence Center** per le imprese di **Industria 4.0** costituendo la spina dorsale di conoscenze e competenze qualificate rispetto ad alcune dimensioni essenziali di robotica, additive manufacturing, realtà aumentata, Internet of Things, **cloud**, **big data** e analytics.

Ne sono nate iniziative che in poco più di un anno hanno già coinvolto centinaia di aziende di ogni settore e dimensione, e che proseguiranno, con l'obiettivo di moltiplicare i buoni risultati già raggiunti.