Articoli correlati

Cybersecurity: le aziende italiane all'esame di maturità

Il costo del cybercrime e la risposta delle aziende

GDPR: come garantire la compliance e aumentare il livello complessivo di sicure

Le regole d'oro per la Cybersecurity

Gli investimenti delle grandi imprese in sicurezza informatica crescono a due cifre. Ma come si sono orientate finora le aziende e quali sono le priorità per l'immediato futuro, a ridosso della GDPR? Ecco lo stato dell'arte dei maggiori gruppi italiani secondo il primo Barometro Cybersecurity 4.0, elaborato da NetConsulting Cube su un panel di imprese delle Telecomunicazioni, Energy/utilities, Finanza, Industria, Assicurazioni, Servizi/trasporti e GDO, nonché di alcuni enti locali della Pubblica Amministrazione

Anche in Italia, l'escalation degli investimenti in cybersecurity è sotto gli occhi di tutti gli addetti ai lavori: secondo le stime di **Assinform/NetConsulting Cube**, il tasso annuo di crescita dello spending delle aziende nel biennio 2016-2017 ha superato regolarmente l'11%, e per quest'anno le previsioni sfiorano il +12%. Con l'entrata in vigore della GDPR nel prossimo maggio, il ritmo della grande corsa alla sicurezza delle imprese italiane sta ulteriormente aumentando. Ed è molto probabile che non andrà rallentando neppure nella seconda parte dell'anno, perché il futuro è denso di minacce tutt'altro che prevedibili.

Per garantirsi un'efficace prevenzione degli attacchi e una tutela sicura da ransomware e phishing non è detto, però, che sia sufficiente aumentare il budget. Dove e come investire in modo costruttivo? Con quali obiettivi concreti? E con quale certezza di risultati?

Per avere un quadro più completo dello stato dell'arte e dell'orientamento generale delle grandi aziende italiane in materia di sicurezza informatica, la società di consulenza NetConsulting Cube ha presentato a fine 2017 il primo *Barometro Cybersecurity 4.0*, condotto su un panel molto qualificato di 50 tra le imprese top nei settori delle Telecomunicazioni, dell'Energy/utilities, delle Banche, dell'Industria, delle Assicurazioni, dei Servizi/trasporti e della Gdo, nonché di alcuni enti locali della Pubblica Amministrazione.

Classificazione delle aziende: il Maturity Model del Barometro

Gli elementi considerati per la costruzione del Cybersecurity Maturity Index

Argomenti trattati

Personaggi

Rossella Macinante

Approfondimenti

GDPR · Intelligenza Artificiale · Machine Learning · Malware · Network Security · ransomware

Articoli correlati

Il costo del cybercrime e la risposta delle
18 Gen 2018

GDPR: come garantire la compliance e a
11 Gen 2018

Le regole d'oro per la Cybersecurity
07 Dic 2017

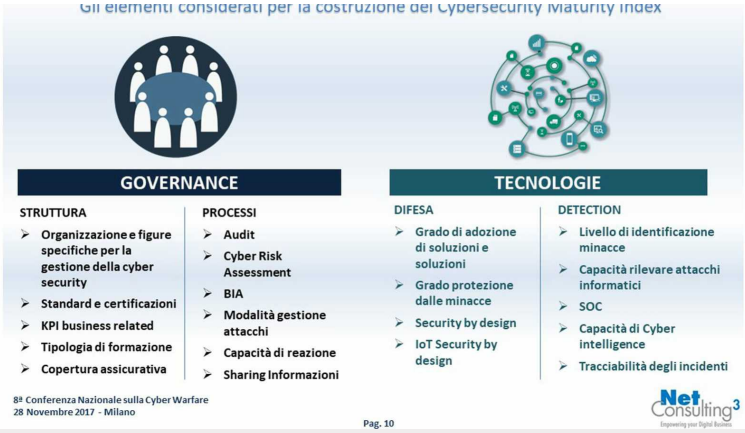

Figura 1 – Classificazione delle aziende: il Maturity Model del Barometro – *Fonte: NetConsulting Cube*

"Con la nostra survey – spiega Rossella Macinante, Practice Leader di **NetConsulting Cube** e responsabile/curatrice del *Barometro Cybersecurity 4.0* – abbiamo voluto toccare tutti gli aspetti, dalla parte di sicurezza a quella perimetrale, fino a quella di protezione dei dati, anche in vista dell'entrata in vigore della GDPR nel maggio 2018. Nella definizione dei campi d'indagine è stato essenziale l'apporto di un advisory board composto dai CSO–Chief security officer dei principali gruppi italiani e da esponenti del mondo accademico, in stretta collaborazione con **Eucacs-European Center for Advanced Cyber Security**".
Partendo dallo screening delle organizzazioni aziendali per la gestione della sicurezza informatica e delle tecnologie adottate per i propri sistemi di difesa e di remediation, il nuovo Osservatorio ha permesso di tracciare il Cybersecurity 4.0 Maturity Model (figura 1): una mappa, cioè, dei posizionamenti attuali delle imprese intervistate, sia sul piano della governance che su quello tecnologico (figura 2).

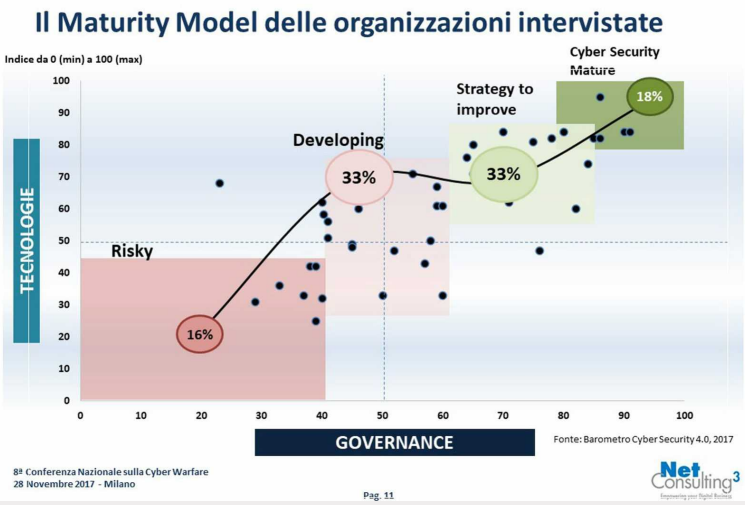

Figura 2 – Il Maturity Model delle organizzazioni intervistate – *Fonte: NetConsulting Cube*

"Quello che emerge dal Maturity Model – nota Macinante – è che il 16% delle grandi aziende risulta ancora in una situazione di rischio: non hanno un assetto organizzativo, né un modello di governance adeguato a gestire la

sicurezza digitale sia al proprio interno sia all'esterno. E neppure dispongono al 100% di quelle tecnologie e di quegli strumenti che consentano di avere un approccio di tipo predittivo delle possibili minacce e non soltanto reattivo nei confronti degli attacchi in corso. C'è poi un terzo d'imprese che si sta attrezzando sul piano tecnologico, e anche velocemente, ma deve ancora progredire in fatto di governance: nel complesso, quindi, quasi la metà del campione si colloca ancora nelle due aree di minore maturità della nostra matrice. Soprattutto per queste aziende, l'entrata in vigore della GDPR dovrebbe costituire una spinta molto forte: non solo per rafforzare le proprie difese per la protezione dei dati, in primis di quelli personali dei clienti e/o consumatori, ma anche per implementare complessivamente il modello organizzativo di gestione della cybersecurity" (figura 3).

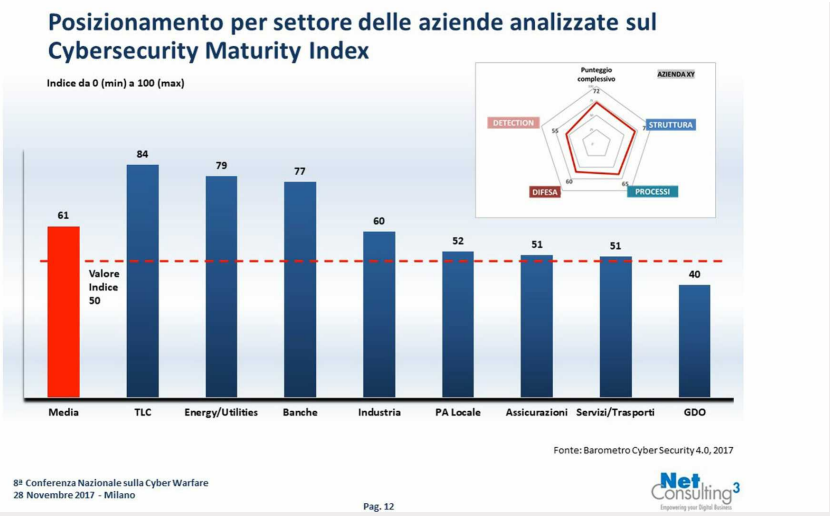

Figura 3 – Posizionamento per settore delle aziende analizzate sul Cybersecurity Maturity Index – *Fonte: NetConsulting Cube*

Tra i settori che meglio si sono mossi per affrontare il crescendo delle cyber minacce con una governance efficace e con soluzioni tecnologiche adeguate, in pole position figurano Telecomunicazioni, Energy/utilities e Banche, seguiti a distanza da Industria, PA Locale, Assicurazioni, Servizi/Trasporti e, come fanalino di coda, GDO.

"Mentre non ha stupito la maggiore operatività delle imprese TLC e delle Banche – nota Macinante – sui temi della sicurezza e della privacy dei dati, sono risultati al di là delle attese i progressi raggiunti dalle Energy/utilities. Le Assicurazioni, invece, devono ancora migliorare sugli aspetti più organizzativi e sui processi, oltre che sui temi della detection e della prevention: hanno mostrato in genere un approccio agli investimenti informatici molto più cauto, a meno che non fossero finalizzati a erogare un nuovo servizio o un nuovo prodotto".

Del resto, ogni azienda ha la sua storia informatica. E quindi anche il processo d'implementazione della difesa cibernetica ha seguito percorsi differenti a seconda delle imprese: c'è chi è partito dalla salvaguardia dei sistemi perimetrali o dei dati all'interno dei server aziendali e chi invece

ha preferito definire innanzitutto il modello di governance, per poi andare in un secondo momento a declinare tutti quelli che sono gli aspetti tecnologici.
Laddove però non si è provveduto per tempo a istituire un ufficio preposto alla cybersecurity esterno all'IT o una figura di riferimento all'interno della Direzione sicurezza aziendale, i processi decisionali sulla gestione della difesa dei sistemi e dei dati e sulle attività di prevenzione dalle minacce hanno subìto necessariamente dei rallentamenti. In questo senso è probabile che l'entrata in vigore del GDPR funga da banco di prova e riveli una qualche disparità tra le aziende più organizzate sul fronte della cybersecurity e quelle più restie ad affrontare la questione nella sua complessità.

Rossella Macinante
Practice Leader di NetConsulting Cube

"L'approccio ottimale – commenta Macinante – parte sicuramente dalle scelte di governance e dalla messa a punto di un modello organizzativo, nonché dalla creazione di una cultura diffusa di prevenzione dei cyber attacchi. Come conferma la nostra survey, in buona parte delle aziende uno dei punti dolenti resta la scarsa diffusione di una cultura digitale trasversale a tutti i livelli, dal top management fino ai livelli impiegatizi e/o operai, che pure aumenterebbe la consapevolezza dei rischi connessi alle minacce informatiche e il livello di attenzione alle modalità con cui queste minacce si possono presentare".
E difatti, tra i principali veicoli di ransomware e phishing figurano ancora le email (o comunque il pc/laptop) del personale interno. In tal senso, oltre alla formazione continua, si rende necessaria anche la pianificazione di attività di simulazione di cyber attacchi per verificare sul campo la reattività dei sistemi implementati e delle persone coinvolte.
"Dopodiché – aggiunge Macinante – il passo successivo sarebbe quello di riuscire a mappare tutti i processi aziendali e a tracciare il percorso dei dati attraverso tali processi. Così, per esempio, nel caso del GDPR non solo si possono individuare i gap rispetto alla normativa e blindare i dati all'interno di cassaforti sicure, ma anche se ne può garantire la tracciabilità".
Buona parte delle aziende intervistate, inoltre, deve passare da un approccio prevalentemente reattivo a uno più predittivo, utilizzando al meglio le soluzioni di threat intelligence/hunting per capire qual è la natura della minaccia e quant'è effettivamente consistente.
Del resto, la strategia tradizionale di blindare a tutti i costi il perimetro

digitale di un'azienda si va rivelando inefficace e insufficiente: non solo perché le minacce esterne sono sempre più sofisticate, ma anche perché nell'era dell'Industry 4.0 e dell'IoT, l'economia è sempre più interconnessa e aumenta la frequenza degli scambi di dati anche tra organizzazioni molto diverse.

E difatti, dalla survey di Net Consulting Cube emergono con chiarezza sia l'esigenza delle aziende di gestire e mettere in sicurezza tutti i macchinari e gli apparecchi connessi sia la preoccupazione di non trovare sistemi in grado di garantire tale sicurezza al 100% (figura 4).

Figura 4– Le priorità d'investimento 2018-2019 – *Fonte: NetConsulting Cube*

Con la crescita degli investimenti in prodotti e servizi attinenti alla cybersecurity, sale anche l'attenzione (e la tensione) dei CIO e dei responsabili della sicurezza informatica nella scelta dei fornitori più adeguati.

"Le risposte delle aziende a tale proposito – rileva Macinante – confermano che per le strategie di cybersecurity ci si affida per lo più a società molto specializzate e focalizzate su questi temi, italiane o estere: spesso israeliane perché dispongono di sistemi tecnologici particolarmente avanzati nella prevenzione e nell'applicazione di soluzioni d'intelligenza artificiale e di machine learning".

I risultati raggiunti dalle imprese con questi nuovi investimenti saranno al centro dell'edizione 2018 del Barometro Cyber Security 4.0, in cui verrà dedicato ampio spazio, in particolare, alle attività intraprese per il GDPR e all'analisi delle eventuali difformità e disomogeneità di comportamento in merito da parte delle aziende stesse. Un altro campo di approfondimento privilegiato per il prossimo Barometro sarà l'effettivo impatto dell'IoT, della fabbrica diffusa e dell'Industria 4.0 sulla sicurezza dei sistemi informativi aziendali, sulle caratteristiche delle soluzioni adottate e sulla tipologia di fornitori prescelti.

Giuseppe Aliverti

Giornalista professionista dal 1991, è entrato nel mondo dei computer nel 1983 per colpa di un Commodore 64. Da allora non ha smesso di smanettare su tastiere e mouse per occuparsi degli universi paralleli del marketing, delle indagini e rilevazioni dei consumi nel mass market e delle nuove frontiere dell'economia, della produzione industriale e della comunicazione digitale.

Articolo 1 di 4