FOCUS

CYBER SECURITY

PERCHÉ NON POSSIAMO FARNE A MENO

START MAGAZINE

Paper Cyber Security, perché non possiamo farne a meno
è un prodotto di
Innovative Publishing S.r.l.

www.startmag.it
www.innovativepublishing.it

A cura di
Valerio Giardinelli, Carlo Terzano, Edoardo Lisi

Redazione
Via Sicilia 141, 00187 Roma
T. +39 06 87758077
info@startmag.it

Progetto grafico
L'asterisco di Barbara Elmi

Stampa
Grafica Internazionale S.r.l., Roma
www.graficainternazionale.it

Chiuso in redazione
Dicembre 2022

Allegato omaggio alla rivista quadrimestrale Start Magazine,
anno VI n. 3/2022

CON I CONTRIBUTI SEPARATI DI

SOMMARIO

CAPITOLO I

1.1 Lo scenario globale

La tecnologia digitale è diventata ormai pervasiva. Governi, società e aziende si affidano sempre più al digitale e se la diffusione delle piattaforme tecnologiche, dei dispositivi e strumenti connessi tramite Internet offre una modalità sempre più semplice e immediata di interagire o di utilizzare servizi, allo stesso tempo apre un panorama più complesso di minacce informatiche e un numero crescente di punti critici di attacco. Con la migrazione della società nel mondo digitale, la minaccia della criminalità informatica acquista sempre maggior rilevanza, comportando regolarmente alle organizzazioni costi e danni per centinaia di milioni di dollari. Secondo le stime più prudenziali, il cybercrimine genera almeno 1 dollaro ogni 100 del PIL mondiale con un trend in continua crescita, a seguito sia dell'aumento degli attacchi, sia della maggiore consapevolezza che porta alla luce una parte del fenomeno in passato sommerso[1].

La diffusione del lavoro a distanza indotto dalle misure di contenimento della pandemia ha accelerato l'adozione di piattaforme e dispositivi che consentono la condivisione di informazioni sensibili nel cloud. Il lavoro a distanza ha anche spostato gli scambi digitali dalle reti degli uffici a quelle residenziali, che hanno una maggiore varietà di dispositivi connessi e sono meno protette contro le intrusioni informatiche. È aumentato il bisogno di capacità trasmissive in grado di trasportare enormi volumi di dati e sono state introdotte nuove potenti tecnologie: l'Intelligenza artificiale (AI), l'Internet of Things (IoT), l'edge computing, la blockchain e il 5G. Sebbene questi sviluppi offrano enormi opportunità per migliorare notevolmente l'efficienza, la qualità e la produttività di aziende e società, queste stesse capacità espongono gli utenti a nuovi rischi digitali e cyber, tanto più elevati e pericolosi quanto più si procede verso nuove versioni di Internet, con il metaverso e i suoi spazi virtuali, il suo mondo 3D, le sue interazioni e transazioni, basato sullo scambio di criptovalute.

La crescente esposizione ha determinato, negli ultimi anni, il costante aumento degli incidenti di sicurezza nel patrimonio IT delle aziende, gli attacchi al cloud, ai sistemi di dati e alla catena di approvvigionamento. Se il 2020 era stato definito nel "Rapporto Clusit sulla Sicurezza ICT in Italia" l'anno peggiore di sempre in termini di evoluzione delle minacce "cyber" e degli impatti generati, della loro gravità e danni arrecati, tale tendenza si è purtroppo confermata anche nel 2021. In 4 anni gli attacchi gravi a livello globale sono cresciuti del 32%, ed oltre a una maggiore frequenza, si registra un indice di severità notevolmente peggiorato, moltiplicando così il danno associato.

Gli attacchi informatici mirati e sofisticati aumentano più rapidamente di quanto la maggior parte delle organizzazioni e dei governi possa prevenire, rilevare e rispondere. Le vulnerabilità note nei sistemi informatici sono un numero impressionante. Il totale registrato dal National Institute for Standards and Technology (NIST) degli Stati Uni-

1 The Hidden Costs of Cybercrime, https://www.csis.org/analysis/hidden-costs-cybercrime

ti conta oltre 16.000 vulnerabilità ed esposizioni comuni (CVE)[2], in costante aumento. Lo sfruttamento economico, tramite riscatto, di un incidente informatico, rappresenta l'86% delle motivazioni di attacco nel 2021: si tratta in particolare di azioni rivolte verso bersagli ben precisi, in ambito governativo/militare, il settore informatico, la sanità, l'istruzione, piuttosto che attacchi generalizzati di tipo *multitarget* come in passato.
Queste aggressioni non sono solo condotte da gruppi criminali organizzati. Spesso anche i cosiddetti Stati-nazione "sponsorizzano" azioni di sabotaggio o esfiltrazione di informazioni (es. il recente attacco verso le società blockchain perpetrato dalla Corea del Nord) e, come sostenuto dal Cybersecurity Outlook 2022 del World Economic Forum[3], la dimensione cibernetica diventa un terreno in cui si scontrano gli interessi divergenti dei diversi protagonisti internazionali. Nonostante la crescita delle minacce, il pericolo degli attacchi cyber risulta in discesa nella classifica dei maggiori rischi allo scenario globale. Si tratta tuttavia di una dinamica congiunturale, dovuta alla presenza di situazioni critiche più grandi (pandemia, conflitto russo-ucraino, inflazione e recessione, crisi energetica), ma occorre comunque tenere ancora alta la guardia per evitare che un abbassamento del livello di attenzione possa determinare un ulteriore allargamento del campo di azione del crimine informatico.
In questo scenario di proliferazione delle minacce alla continuità del business, i responsabili informatici sono chiamati a gestire i propri budget bilanciando la necessità di introdurre le innovazioni necessarie per la transizione digitale con gli investimenti necessari a fronteggiare la maggiore esposizione ai rischi. Nessuna azienda è immune, anche le imprese di piccola e media dimensione (PMI) sono diventati un target di attacchi informatici. I motivi per cui le PMI sono entrate nel mirino degli attacchi cyber sono essenzialmente due:

1) lo sfruttamento di tecnologia avanzata, come l'automazione e l'IA, da parte del crimine permette attacchi contemporanei su un gran numero di imprese, mirando soprattutto alle diffuse vulnerabilità delle aziende di dimensione più piccola, e ne aumenta la probabilità di successo. Più ampio è quindi il fronte di attacco, maggiore è la rendita ottenibile anche se il riscatto medio per azienda è proporzionato al target. Del resto mettere a rischio la continuità aziendale e chiudere l'attività è una molla che può spingere le vittime di un attacco a pagare i riscatti. È quindi importante comprendere quanto sia diffuso e compreso il fenomeno tra le PMI.

2) Il secondo motivo è l'opportunità che si apre, aggredendo le PMI, di penetrare nelle maglie delle difese più robuste di grandi imprese clienti. Si tratta dei cosiddetti attacchi alla *supply chain* delle imprese di grandi dimensioni che possono diventare un bersaglio sfruttando il veicolo dei propri fornitori.

2 https://nvd.nist.gov/vuln
3 WEF The Global Risks Report 2022

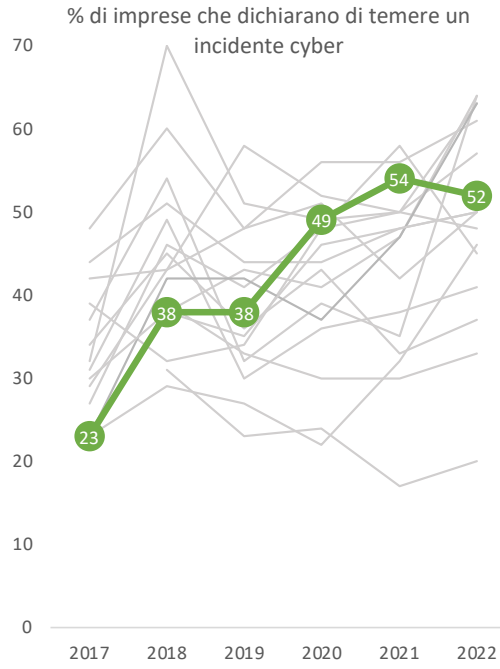
1.2 Per le imprese italiane, la minaccia cyber è al primo posto tra i rischi potenziali

Secondo un sondaggio realizzato da Purplesec[4], circa quattro attacchi cyber su dieci sono rivolti ad imprese di piccola dimensione e circa il 47% delle società intervistate nell'ultimo anno ha subìto almeno un attacco. Il 70% delle piccole imprese si dichiara impreparato a gestire un attacco cyber, e tre aziende su quattro non hanno abbastanza personale per curare la sicurezza informatica, nonostante siano ben consapevoli del rischio.

L'indagine annuale condotta dal gruppo assicurativo Allianz ci fornisce qualche indicazione per comprendere quanto sia radicata tale consapevolezza in Italia. Mentre lo scenario del World Economic Forum raccoglie le opinioni dei maggiori leader politici, economici ed accademici, l'indagine del gruppo Allianz si rivolge direttamente alle figure aziendali che si occupano di *risk management* ed è pertanto una spia importante del *sentiment* delle imprese di fronte a tale fenomeno[5].

La percezione del rischio di incidenti cyber è andata aumentando nel corso del tempo in Italia, con una forte accelerazione nel 2020-2021, probabilmente causata dal maggiore ricorso a soluzioni digitali durante i periodi di lockdown e distanziamento. Mentre nel 2017 il timore di un attacco riguardava meno di un'azienda su quattro, dal 2020 questa preoccupazione è manifestata da più o meno un'azienda intervistata su due. Il rischio di un attacco cyber è considerato dalle aziende italiane la principale minaccia al proprio business, superando le generiche interruzioni di attività (a volte causate anche da un incidente informatico), le catastrofi naturali (che entra tra le prime tre ragioni di preoccupazione), i cambiamenti normativi e regolamentari, la pandemia e le problematiche legate al proprio mercato di riferimento (volatilità, ingresso di nuovi concorrenti, stagnazione dei mercati). A livello europeo, la forte preoccupazione per gli incidenti cyber è condivisa con Austria, Belgio, Danimarca, Paesi Bassi, Sviz-

Percezione rischio cyber



Fonte: Allianz Risk Barometer – varie edizioni

4 https://purplesec.us/resources/cyber-security-statistics/
5 https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

zera e UK. Il confronto con l'indagine 2021 mostra una crescita dei timori per il blocco dell'attività a scopo estorsivo, il cosiddetto *ransomware*, che passa dal terzo al primo posto al pari della violazione dei dati (*data breaches*) e delle vulnerabilità digitali della catena di fornitura, che passano dal quinto al quarto posto.

1.3 Il ruolo critico delle PMI nella cyber resilienza

In un sistema iperconnesso, uno dei punti critici è rappresentato dal differente livello di sicurezza cibernetica delle organizzazioni. Una vulnerabilità di un fornitore può diventare una porta d'ingresso per un attacco cyber, come avvenuto nel caso SolarWinds a fine 2020. L'operazione ha sfruttato le vulnerabilità della piattaforma Orion di SolarWinds per infiltrarsi nelle reti dei grandi clienti del gruppo, tra cui diverse agenzie governative statunitensi, con gravissime ripercussioni anche per la sicurezza nazionale, al punto che è stato avanzato il sospetto che tale azione sia stata perpetrata da hacker di origine governativa.

Per difendersi da questa tipologia di rischio non bastano le singole aziende ma è necessario guardare alla capacità di difesa dell'intero sistema digitale. In questa prospettiva, le piccole e medie imprese collegate alla rete di un'organizzazione più grande, con minori risorse dedicate alla propria sicurezza informatica, possono rappresentare un punto debole che può essere sfruttato da malintenzionati per aggirare i sistemi di protezione delle aziende clienti e diventano un bersaglio privilegiato delle azioni di infiltrazione. Il Global Cybersecurity Outlook del World Economic Forum[6] riporta che nel corso del 2021 il 55% delle PMI ha subìto un attacco informatico e quasi nove intervistati su dieci hanno espresso una forte preoccupazione per la resilienza delle PMI all'interno del proprio ecosistema.

1.4 Le PMI italiane e la digitalizzazione

Stando al *Rapporto regionale PMI 2022*, realizzato da Confindustria e Cerved in collaborazione con UniCredit, in Italia sono 160mila le società che – impiegando tra i dieci e i 249 addetti, per un giro d'affari compreso tra i 2 e i 50 milioni di euro – rientrano nella definizione europea di piccola e media impresa (PMI). Generano, nel complesso, un valore aggiunto[7] di 204 miliardi di euro, apportando dunque un contributo fondamentale allo sviluppo economico del Paese.

Nel rapporto si legge che la digitalizzazione, una delle due grandi direttrici del Piano nazionale di ripresa e resilienza (PNRR) assieme alla sostenibilità, "avrebbe ricadute strategiche e organizzative" sulle PMI, rendendo il loro modello organizzativo "più competitivo e con maggiore propensione all'internazionalizzazione".

Secondo lo studio *Il contributo dei social network e dei canali digital per la crescita e la*

6 https://www.weforum.org/reports/global-cybersecurity-outlook-2022/

7 Ovvero la differenza tra il valore della produzione (fatturato) e il valore degli input utilizzati nel ciclo produttivo (lavoro, materie prime…)

digitalizzazione delle PMI italiane, realizzato da The European House – Ambrosetti e pubblicato lo scorso giugno, "[i] *social network* e i canali *digital* rappresentano un forte abilitatore di crescita del livello di digitalizzazione delle PMI": vengono definiti "una via efficace e veloce per la digitalizzazione", perché sono facili da utilizzare e da scalare; "una volta introdotta la digitalizzazione all'interno dell'impresa in questo ambito", si legge, "l'azienda è poi più facilmente portata a digitalizzare anche gli altri aspetti". La crescita dell'uso dei social network da parte delle PMI, primo passo di un percorso di maggiore digitalizzazione generale, potrebbe produrre fino a 10,2 miliardi di euro in più di valore aggiunto.
L'Italia parte in ritardo, però: il Digital Index PMI di The European House – Ambrosetti la posiziona al diciottesimo posto in Europa per grado di digitalizzazione delle piccole e medie imprese. Le PMI nostrane, in particolare, sono al di sotto della media europea per utilizzo di connessioni veloci e, soprattutto, per competenze digitali. Hanno infatti i livelli più bassi in Europa di specialisti delle tecnologie dell'informazione e della comunicazione (ICT) nei loro organici: il 12 per cento, contro la media del 18 per cento dell'Unione europea. Solo il 15 per cento delle PMI italiane, inoltre, è in grado di fornire internamente percorsi di formazione digitale, contro il 18 per cento della media europea.
D'altro canto, i dati degli ultimi cinque anni segnalano una tendenza alla maggiore adozione di sistemi digitali da parte di queste aziende, all'ottavo posto in Europa per accelerazione e 9 punti al di sopra della media comunitaria. Se l'Italia riuscisse a colmare il divario digitale rispetto alle *best performer* europee (Danimarca, Finlandia, Svezia), la produttività lavorativa delle PMI aumenterebbe del 5 per cento, generando fino a 13,5 miliardi di euro di valore aggiunto: vale a dire il 4,3 per cento del valore attuale, secondo i calcoli di The European House – Ambrosetti.

1.5 Il rischio cibernetico

La pandemia di coronavirus ha dimostrato l'importanza dello sviluppo tecnologico per le piccole e medie imprese, che proprio grazie all'utilizzo di strumenti e servizi digitali hanno potuto garantire la prosecuzione delle attività durante i lockdown e quantomeno contenere l'impatto della crisi. Se i processi produttivi e l'economia intera si digitalizzano, però, lo fanno anche le minacce. Ma la percezione del rischio cibernetico tra le PMI italiane è generalmente bassa. L'informatica e la cybersicurezza (o *cybersecurity*) sono spesso considerate dalle aziende come un costo da mantenere il più basso possibile, e per questo vengono esternalizzate ad agenzie di consulenza[8].

Secondo un'indagine di CyberEdge intitolata *2022 Cyberedge Cyberthreat Defense Report*[9], le società italiane spendono in sicurezza solo il 10,1 per cento del budget allocato per il comparto IT: è il dato più basso tra i Paesi membri del G7, poiché le imprese tedesche spendono il 10,8 per cento; quelle britanniche il 10,9; quelle canadesi l'11,1; quelle

8 Stefanello V., Cybersicurezza in Italia: perché non si trovano candidati?, su *Guerre di Rete, 16/06/2022.*
9 Si veda anche O'Driscoll A., Italy cyber security and cyber crime statistics (2020-2022), su "Comparitech", 22/07/2022.

giapponesi l'11,5; quelle francesi il 12 e quelle statunitensi il 13,7 per cento.
Dedicare un budget minore alla cybersecurity aziendale ha delle conseguenze: nel 2021, infatti, l'87,8 per cento delle organizzazioni italiane ha avuto a che fare con almeno un attacco cibernetico andato a buon fine, rispetto all'85,7 per cento del 2020[10]. E il 47 per cento delle aziende ritiene che esista una possibilità moderata di subire un attacco *ransomware* – si chiamano così quegli attacchi informatici che prevedono la sottrazione di dati alla vittima per ottenere un riscatto (*ransom*) – nei dodici mesi successivi. Circa due organizzazioni italiane su tre hanno subìto un attacco *ransomware* nel 2021. In quell'anno, stando ai calcoli di Trend Micro[11], l'Italia è stato il quarto Paese al mondo e il primo in Europa più colpito dai *malware* – 6861 attacchi in tutto –, avanzando di tre posizioni nella classifica mondiale rispetto al 2020.
Uno studio di Sophos relativo al 2020, intitolato *The State of Ransomware 2020*, afferma che il 40 per cento circa degli attacchi *ransomware* contro enti italiani è stato bloccato prima che i dati venissero crittografati. I riscatti chiesti sono stati pagati solo nel 6 per cento dei casi analizzati, un dato superiore soltanto a quello spagnolo (4 per cento), il più basso in assoluto. È possibile che le aziende italiane non riescano a comprendere l'effettivo valore dei dati in loro possesso, e che di conseguenza non considerino vantaggioso sostenere una spesa per riprenderne il controllo. Secondo Sophos, in Italia il costo medio di un riscatto dopo un attacco *ransomware* è di 680.000 dollari.
Su tutte le multe per violazioni del GDPR (il Regolamento generale sulla protezione dei dati, n. 2016/679) tracciate dal portale *Privacy Affairs*[12], quelle emesse in Italia sono un'ottantina. Secondo DLA Piper, nel 2021 i soggetti attivi in Italia hanno ricevuto multe connesse al rispetto al GDPR per 69.326.716 euro, il valore più alto, superiore anche a quello della Germania (69.085.000 euro). DLA Piper ha contato 3460 episodi di violazione dei dati personali nel nostro Paese, di cui 1276 nel 2019 e 1574 nel 2020.
Circa nove organizzazioni italiane su dieci hanno stipulato una polizza assicurativa contro i rischi cibernetici, un valore nella media globale. Il 68 per cento degli enti in possesso di un'assicurazione sono protetti dagli attacchi *ransomware*.
I tracciamenti di Cynet rivelano un aumento significativo dei tentativi di *phishing* in Italia all'inizio della pandemia: solo tra il 15 febbraio e il 15 marzo del 2020, il numero degli attacchi di questo tipo è stato di quasi tre volte superiore ai valori abituali. In altri Paesi – come la Germania e gli Stati Uniti – i livelli sono rimasti sostanzialmente invariati.
Il monitoraggio di McAfee, azienda statunitense di sicurezza informatica, ha contato circa 16 milioni di rilevamenti di file malevoli dal dicembre 2020 al luglio 2022 in tutto il mondo: solo in Italia ne sono stati rilevati 403.981, un dato che mette il nostro Paese al quinto posto della classifica internazionale in termini di volume.

10 Fonte: 2022 Cyberedge Cyberthreat Defense Report
11 Fonte: Navigating New Frontiers, Trend Micro, 17/03/2022
12 Si veda GDPR Fines Tracker & Statistics, su "Privacy Affairs"

1.6 I ritardi nella cybersicurezza

Nel complesso, uno studio di Comparitech[13] ha posizionato l'Italia al cinquantaquattresimo posto su settantacinque per livello di cybersicurezza con un punteggio medio di 21.09, il peggiore fra tutti i membri del G7: Canada 11.99, Francia 19.10, Germania 19.57, Giappone 17.71, Regno Unito 9.60, Stati Uniti 19.69.

Solo il 20 per cento dei dipendenti delle aziende italiane, inoltre, utilizza l'autenticazione a due fattori: è il dato più basso tra tutti i Paesi analizzati nel *3rd Annual Global Password Security Report* di LastPass e lontanissimo da quello dei *top adopter* come Svizzera (38 per cento), Paesi Bassi (41 per cento) e Danimarca (46 per cento). Secondo LastPass, in media un dipendente italiano deve gestire ben ottanta password, un numero superato solo dal Belgio con 112. È forse proprio questa sovrabbondanza di password la causa del loro diffuso riutilizzo: in media, i dipendenti italiani utilizzano dodici password uguali per accedere a siti o applicazioni diverse. Secondo IBM, il 20 per cento delle violazioni di dati è riconducibile proprio a credenziali compromesse; il *phishing* è responsabile del 17 per cento, mentre l'errata configurazione dei sistemi cloud di un ulteriore 15 per cento. In Italia il tempo medio impiegato per identificare una *data breach* è di 203 giorni, e di 65 giorni per contenerla. Le società tedesche impiegano in media 128 giorni per identificare una violazione e 32 per contenerla, secondo l'edizione 2020 del *Cost of a Data Breach Report* del Ponemon Institute.

Strategie di cyber-resilienza: l'importanza della Readiness secondo Engineering

Al fine di contrastare la vastità e la varietà delle minacce cyber e la continua evoluzione delle TTPs (Tattiche, tecniche e procedure) degli attaccanti, nelle organizzazioni emerge in modo sempre più importante l'esigenza della *Readiness*, ovvero di migliorare le proprie capacità di mantenersi pronti.

In altre parole, Readiness per le organizzazioni vuol dire testare ed allenare la propria cyber-resilienza in maniera sistematica, automatizzata, e con il supporto delle nuove tecnologie di Big Data Analytics, Artificial Intelligence e Machine Learning.

In questo senso Readiness – come fattore abilitante appunto alla cyber resilienza – si traduce nella capacità di coprire i gap di sicurezza, in una logica di priorità di intervento e di *continuous improvement*, tenendo conto che gli avversari hanno abilità, tecniche e tool di attacco ormai fortemente industrializzate ed all'avanguardia, almeno al pari delle tecniche e tool di difesa.

E Readiness è un tema di natura sia tecnologica, sia organizzativa.

Da un punto di vista tecnologico, l'innovazione al servizio della Readiness si indirizza su tre filoni:

1. Visibilità e monitoraggio di sicurezza a livello estensivo sugli asset digitali
2. Security analytics per migliorare la precisione delle allerte con l'analisi comportamentale Early warning per una prevenzione proattiva.

13 Bischoff P., Which countries have the worst (and best) cybersecurity?, su Comparitech*, 26/09/2022*

Per Visibilità e monitoraggio di sicurezza si intende il Cybersecurity Asset Management, ovvero la capacità di migliorare la visibilità delle configurazioni di sicurezza e delle vulnerabilità degli asset che compongono l'infrastruttura digitale. Ciò può esser fatto utilizzando tecnologie che consentano di allargare il perimetro di monitoraggio ed illuminare i "punti ciechi", ad esempio estendendo la copertura della protezione verso i cloud *workload*; introducendo tecnologie di monitoraggio e *threat detection* sul traffico di rete; convogliando log, telemetrie ed *alert* di questo perimetro esteso verso motori cloud di XDR, ovvero di rilevamento sempre più precisi ed in grado di aumentare la capacità di *detection* e risposta alle minacce che contano.

Alla Security Analytics sarà sempre di più affidato il compito di aumentare la capacità di identificare possibili anomalie e minacce che possano essere sfuggite al primo livello di sicurezza, soprattutto per gli attacchi APT (Advanced Persistant Threat). Dunque Analytics che operino come "motori di secondo livello" e su un perimetro più esteso, aumentando contesto e precisione per identificare minacce nascoste o fornire un "verdetto" più accurato su una anomalia già rilevata.

Si tratta di strumenti di nuova generazione, già oggi disponibili, di User Behavioral Analytics, ovvero tool in grado di analizzare il comportamento degli utenti, che continueranno ad affinare le capacità e la precisone degli algoritmi di Machine Learning e Artificial Intelligence impiegati, e che saranno sempre di più arricchiti e validati con molteplici fonti di cyber threat intelligence. In Italia, strumenti di questo tipo, sono ad esempio disponibili nell'offerta TIM Enterprise, che mette a disposizione soluzioni proprietarie di Telsy, società del Gruppo dedicata alla Cybersecurity.

Gli Early Warning sono invece strumenti di allerta precoce, e che a loro volta – facendo uso di sorgenti qualificate di Cyber Threat Intelligence – aiutano a "tenersi pronti" su diversi fronti: la gestione automatizzata delle vulnerabilità per un patching di sicurezza realmente mirato sulle priorità di mitigazione del rischio; la misura del livello di rischio cui è esposta la superficie digitale dell'organizzazione, censita attraverso Report di Risk Score (ScoreCard) puntuali e associata al monitoraggio automatico e la segnalazione tempestiva di vulnerabilità esposte, account compromessi, e data leaks; l'identificazione di schemi di attacco critici, nascosti, e realmente sfruttabili dagli avversari.

Si è fatta una breve carrellata sugli strumenti tecnologici, ma Readiness significa anche lavorare sull'organizzazione, ed in particolare sulle skill delle persone. Il fattore umano è fondamentale. Occorre prima di tutto allenare la resilienza da un punto di visto organizzativo e delle risorse umane, cioè condurre periodicamente simulazioni ed esercitazioni di attacchi cyber, per testare la capacità di risposta dei team di difesa, e per tenere pronte squadre tattiche di pronto intervento. Bisogna poi investire nella formazione: l'Italia ha bisogno di professionisti IT in grado di definire architetture informatiche robuste e gestire le tecnologie all'avanguardia, con cui prevenire i rischi della cybersecurity, piuttosto che riparare i danni provocati da un attacco andato a buon fine. È necessario

quindi puntare sull'awareness: rendere tutti quelli che lavorano all'interno di un'organizzazione e hanno accesso alla rete consapevoli dei pericoli che possono provenire da comportamenti poco attenti o da disinformazione online.
Peraltro, l'evoluzione del quadro normativo a livello europeo pone particolare risalto alla necessità di potenziare strumenti e capacità organizzative a supporto della Readiness in chiave di miglioramento della capacità di prevenzione, protezione, rilevamento e risposta efficace agli attacchi informatici.
Senza contare che recentemente è entrata in vigore la nuova direttiva per la cybersecurity europea, la cosiddetta Nis 2, che sostituisce l'attuale direttiva sulla si-curezza delle reti e dei sistemi informativi. La Nis 2, in sintesi, stabilisce la base per le misure di gestione del rischio di sicurezza informatica e gli obblighi di segnalazione in tutti i settori coperti dalla direttiva (come l'energia, i trasporti, la salute e le infrastrut¬ture digitali). Rispetto alla precedente Direttiva NIS sono coinvolti anche settori come l'Agroalimentare e l'Automotive, filiere importanti per l'Italia, con adempimenti riparametrati su nuove basi dimensionali. La NIS2 si rivolge infatti alle medie e grandi imprese oltre che alle istituzioni pubbliche nazionali e regionali, con possibile estensione -in fase di recepimento nazionale- anche agli enti locali.

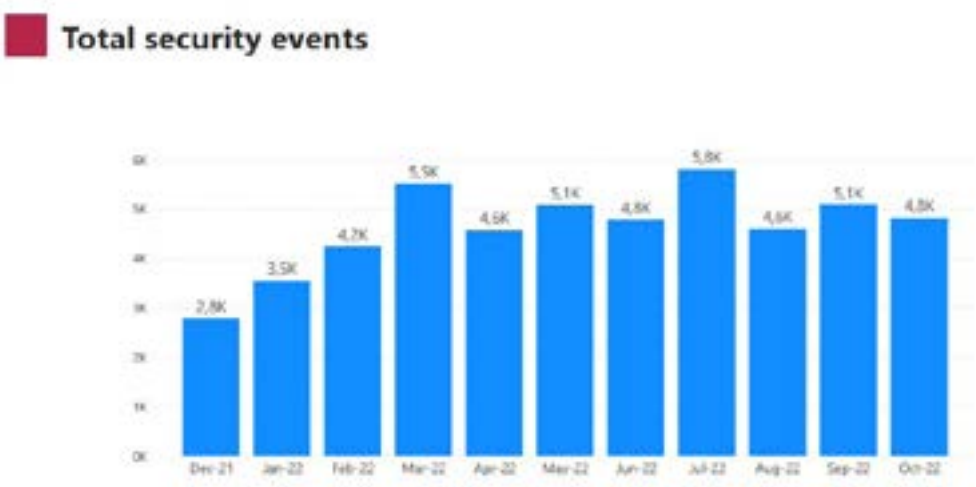
Come difendersi dalle minacce cyber: il Security Patching

Il Patching? Ormai è una pratica piuttosto mandatoria, anche e soprattutto alla luce dell'escalation di attacchi cyber verificatasi nell'ultimo anno. La patch, vale la pena ricordarlo, è una componente software che va a migliorare il software oppure a correggere una vulnerabilità informatica. Ed è una pratica che molte aziende oggi fanno con regolarità, utilizzando tecnologie in grado di identificare la falla o la minaccia.
La parte più critica, però, avviene subito dopo. Una volta individuata la criticità, si sa su quale macchina si è verificata? Si sa se è stata corretta, qual è l'*owner* o a che punto è la risoluzione del problema? Si riesce ad avere un timing e una priorità dell'incidente?
È quando si arriva alla "sistematizzazione" delle tracciature delle vulnerabilità che molte aziende (piccole e grandi) rischiano di non essere dotate degli strumenti adatti per avere una visione a 360 gradi degli interventi necessari a mettere in sicurezza i loro asset. Ed è qui che entra in campo la necessità di avviare il Security Patching. Come? Attraverso un gestionale che, nel momento in cui si ha la consapevolezza di avere una minaccia su un determinato sistema, permette, con un semplice clic, di individuare il punto esatto della vulnerabilità, consente di capire se questa, per esempio, riguarda un computer esposto direttamente su Internet, e quindi con una postura più critica rispetto ad altri, dà la visibilità se chi doveva prendere in carico la risoluzione l'ha fatto e se ha condiviso i suoi risultati, affinché facciano "letteratura" per la risoluzione di altri attacchi.
A descriverlo così, il processo sembra una di quelle "banality" che non si possono non

avere in un'azienda. E invece, oggi la maggior parte delle imprese, pur avendo capito la necessità di mappare tutti i loro sistemi così da avviare quel processo di resilienza che permette non di evitare il rischio (perché il rischio zero non esiste) ma di gestirlo, ancora non hanno piena conoscenza che è possibile avere degli strumenti tecnologici con cui tracciare anche gli interventi per sanare le vulnerabilità. Un processo, questo, la cui importanza è proporzionale alla grandezza del business. Soprattutto quando si parla di imprese con Data Center o che hanno anche ramificazioni internazionali.
Chiaramente, avviare un sistema di Security Patching prevede un investimento iniziale: occorre dotarsi di un layer tecnologico per l'identificazione delle vulnerabilità, implementare il gestionale nei propri sistemi e alimentarlo con più dati possibili, è necessario provvedere alla sua manutenzione.
Ma i benefici in termini di resilienza possono superare di gran lunga gli impegni iniziali per avviare un processo che riduce l'errore umano e quindi il rischio dell'intrusione informatica, così da abilitare quella "readiness" che rimane sempre alla base di ogni strategia di Cybersecurity.

Soluzioni per la sicurezza aziendale: il SOC di Engineering[14]

Le attuali tensioni geopolitiche hanno visto un massiccio incremento degli attacchi cyber. Una guerra che si avvale sempre più di strumenti informatici e che per questo richiede particolari misure per aumentare la cyber resilienza dei nostri sistemi. Monitorare, rilevare e filtrare le anomalie che contano, bloccare le minacce, tutto ciò diventa fondamentale in simili contesti. Per questo Engineering ha messo in campo il suo SOC (Security Operation Centre), un framework che vuole diventare punto di riferimento a livello nazionale nella cyber security.
Il SOC è un luogo di raccolta, correlazione e analisi degli eventi e si basa su avanzate tecnologie di Intelligenza artificiale che incrociano e verificano gli eventi di oltre 22mila



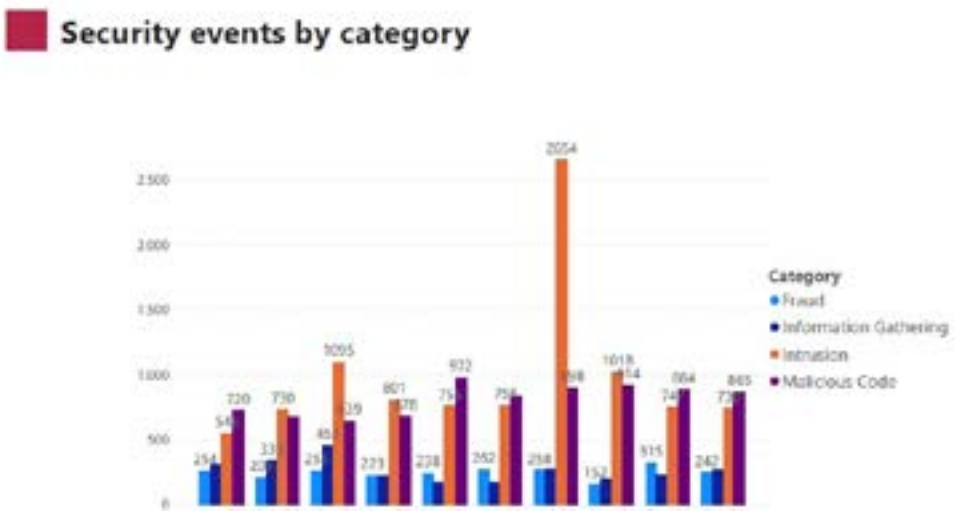
14 *Contenuto a cura di Engineering*

server gestiti dal Gruppo, proteggendo ogni giorno circa 20Pb di dati da un numero impressionante di attacchi. La potenza del SOC è quella di attivare allarmi automatici, anche di fronte a comportamenti all'apparenza leciti, ma che grazie ad un'indagine automatica dello storico dei comportamenti, analisi statistiche o *impossible travel alert* (accessi contingenti da punti distanti) possono invece svelare un attacco in corso. Si tratta quindi di un sistema sia reattivo, sia di prevenzione proattiva, in grado di elaborare risposte indipendentemente dal singolo analista, alzando un muro di fronte ad una potenziale minaccia. Inoltre, "vulnerability scan" e "Threat Intelligence" arricchiscono la capacità diagnostica del software arricchendo le sue informazioni con gli elementi di contesto. Questo permette a SOC e agli oltre 70 analisti che vi lavorano di creare nuove regole di protezione, e di intercettare nuovi schemi di attacco in tempo utile, a fronte di un nemico che cerca sempre nuove falle per insinuarsi nei sistemi, isolando quello che i tecnici chiamano un "rumore di fondo" fatto da minacce che non creano danni perché magari già note e superate.

L'importanza della formazione: la IT & Management Academy di Engineering[15]

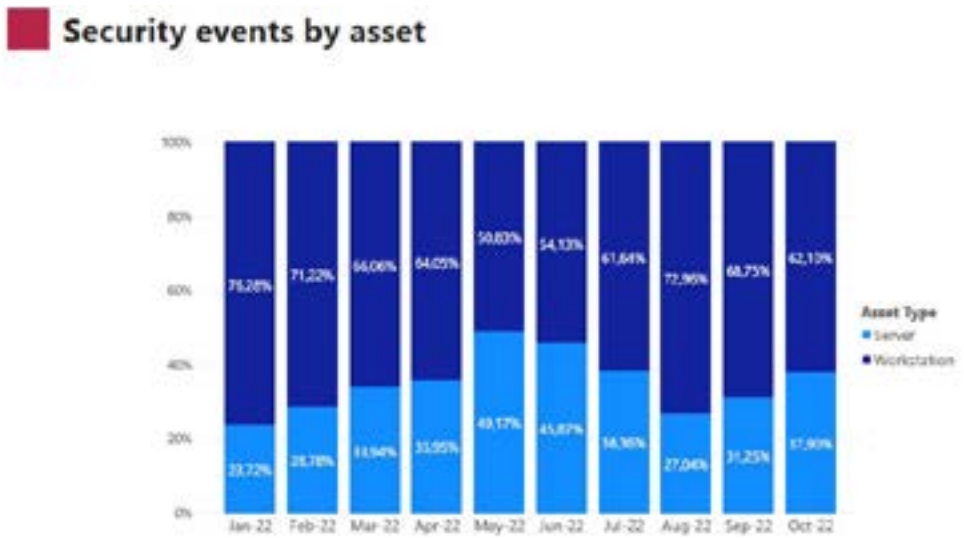
La prima arma per proteggersi dai cyberattacchi e mantenere al sicuro i propri dati? La formazione. È da lì, infatti, che si deve partire per fare in modo che il nostro Paese possa raggiungere, anche in ambito Cybersecurity, quella indipendenza tecnologica sostenuta da esperti in grado di tenere testa alle minacce cyber sempre più insistenti e sempre più evolute.

Insieme a una "formazione tecnologica" bisogna però alimentare anche una vera cultura della cybersicurezza, che prima di tutto deve coinvolgere quanti, con ruoli diversi e diverse funzioni, utilizzano i device aziendali. Questa necessità diventa ancora più impellente oggi, alla luce di un ricorso sempre più massiccio dello smart working, che crea



15 *Contributo a cura di Engineering*

un uso promiscuo, e quindi pericoloso, di device "lavorativi" e device "domestici", così come di reti casalinghe e reti aziendali.
È poi necessario far capire anche al "cittadino comune" l'importanza di non abbassare mai la guardia verso possibili pericoli generati da attacchi cyber.
Secondo il rapporto Clusit, infatti, i *Malware* e i *ransomware* sono gli strumenti preferiti dei criminali informatici per generare profitti, giocando spesso sull'errore umano per mettere in atto vere e proprie truffe, con conseguenze anche gravi. Più in generale, il mercato europeo dei dati, dove questi vengono scambiati come prodotti o servizi, mostra il valore crescente dei dati, registrando un incremento del 4,9 per cento anno su anno, per toccare quota 63,8 miliardi di euro nel 2021, quando nel 2013 il valore si fermava a 47 miliardi di euro.
Questi numeri spiegano perché, sempre più spesso, le cronache riferiscono di attacchi informatici a grandi istituzioni per il furto di dati e perché sia diventato imprescindibile difendersi, formarsi, restare aggiornati.
L'importanza della awareness è uno dei pilastri anche della Strategia nazionale di Cybersecurity 2022/2026, adottata dal Governo e presentata qualche tempo fa dall'Agenzia per la Cybersicurezza Nazionale.
Un principio che trova completamente allineate aziende come Engineering, che sentono la responsabilità, anche sociale, di affiancare imprese e pubbliche amministrazioni nella loro lotta alle minacce cyber.
A questo proposito, ad esempio, l'IT & Management Academy di Engineering, che ogni anno eroga oltre 25 mila giornate di formazione a oltre 10 mila partecipanti, dedica corsi particolari ai temi legati alla Cybersecurity con 20 cicli di formazione e la possibilità di ottenere del¬le certificazioni specifiche. Perché alla base di ogni strategia c'è sempre il fattore umano che può fare la differenza.



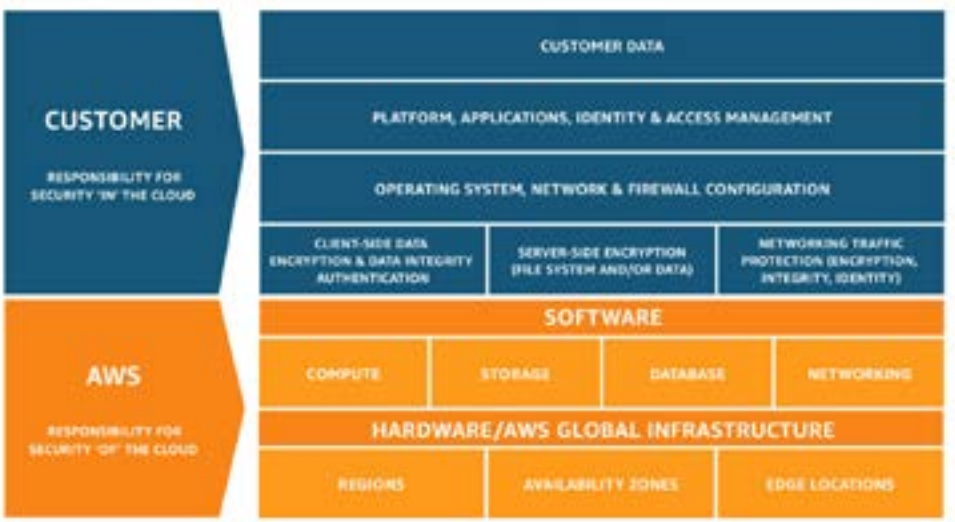
1.7 La mancanza di backup

Un sondaggio di BVA Doxa[16] condotto su trecento piccole e medie imprese italiane di vari settori e pubblicato il 31 marzo 2022, ha fatto emergere come il 27 per cento delle PMI non possieda un backup (una copia di sicurezza) dei propri dati; il dato sale al 43 per cento nel caso delle sole piccole imprese.

Solo il 73 per cento delle aziende intervistate ha detto di disporre di soluzioni di backup: nel caso specifico delle piccole imprese si scende al 57 per cento; in quello delle medie imprese, invece, si sale all'87 per cento. Tra le società che fanno uso di soluzioni di backup, il 62 per cento ne dispone da più di cinque anni, mentre appena il 3 per cento se ne è dotato durante il 2021. Si tratta, secondo BVA Doxa, di un "sintomo che l'accelerazione della digital transformation registrata nel corso degli ultimi due anni non ha determinato un aumento in parallelo della attenzione alla conservazione dei dati e alla propria sicurezza digitale".

Ad avere un backup in cloud – ovvero una soluzione che permette di criptare e sincronizzare in tempo reale i file sui server del centro dati che fornisce il servizio – è il 57 per cento delle aziende intervistate: in questo caso, il tasso di adozione è maggiore tra le piccole imprese (60 per cento) che tra quelle medie (54 per cento).

Il 71 per cento delle aziende italiane che non possiede un sistema di backup dice di non avere intenzione di introdurlo nemmeno nel lungo periodo. Disporre di un meccanismo di ripristino dei dati nel caso in cui questi dovessero diventare inaccessibili – per via di incidenti informatici o attacchi *ransomware*, ad esempio – è però utile a garantire la continuità delle operazioni. Le imprese più scettiche nei confronti del backup ritengono di avere pochi dati di valore da salvaguardare (o di non averne affatto) e di non gestire dati sensibili da proteggere adeguatamente: è un ragionamento che, stando a BVA Doxa, dimostra "una scarsa percezione del potenziale pericolo".



16 BVA Doxa, Conservazione e sicurezza dei dati nelle aziende italiane, 31/03/2022

Lo studio afferma infatti che sette aziende su cento abbiano avuto a che fare con una perdita di dati, la cui causa scatenante è riconducibile nel 34 per cento dei casi proprio all'inefficacia o all'inadeguatezza del sistema di backup. Le imprese che hanno dovuto gestire una perdita di dati hanno subìto un *downtime* (tempo di inattività) di quasi due giorni. Il 52 per cento delle aziende intervistate dichiara appunto che la perdita di dati ha provocato un rallentamento sul lavoro e delle perdite economiche, che il 43 per cento non riesce però a quantificare nello specifico.
Una buona parte dei dirigenti delle PMI italiane intervistati da BVA Doxa non ha mostrato una particolare attenzione alla sicurezza digitale nemmeno nel suo privato: solo il 58 per cento dei manager, infatti, dice di utilizzare un sistema di backup nella sfera privata; sistema che nel 27 per cento dei casi consiste in una copia dei dati su supporto fisico esterno (hard disk o chiavetta USB). Tra chi non ne fa uso affatto, nove volte su dieci sostiene che il backup non rappresenti una necessità.

1.8 Il cloud come paradigma win-win per mitigare i rischi[17]

Il cloud computing consiste nella distribuzione on-demand delle risorse IT tramite Internet, con una tariffazione basata sul consumo. Piuttosto che acquistare, possedere e mantenere i data center e i server fisici, è possibile accedere a servizi tecnologici, quali capacità di calcolo, archiviazione e database, sulla base delle proprie necessità affidandosi a un fornitore cloud specializzato.
Passare al cloud non significa semplicemente abbandonare i propri server on-premise, ma coinvolge un vero e proprio progetto di migrazione da svolgersi nelle seguenti tre fasi.

1. Valutazione. All'inizio del percorso, viene eseguita una *valutazione* della preparazione attuale nei confronti dell'operatività sul cloud della tua organizzazione. Soprattutto, vengono definiti i risultati aziendali attesi e il caso specifico per la migrazione.
2. Mobilitazione. Nella fase di *mobilitazione*, viene creato un piano di migrazione e dettagliato il caso aziendale. Si risolvono le lacune nella preparazione dell'organizzazione rilevate durante la fase di valutazione, con un particolare accento sulla progettazione dell'ambiente di base (la "*landing zone*"), promuovendo la preparazione operativa e sviluppando le competenze sul cloud.
3. Migrazione e modernizzazione. Durante la fase di *migrazione e modernizzazione*, ogni applicazione viene progettata, migrata e convalidata.

Quando un'azienda – indipendentemente dalla sua dimensione – porta i suoi *workload* in cloud, essa da una parte eredita i controlli di sicurezza messi in campo dal cloud provider a protezione della infrastruttura globale e, dall'altra, ne condivide la responsabilità sulla base del cosiddetto Modello di Shared Responsibility descritto nella figura seguente.

17 *Contenuto a cura di AWS*

Come si vede nella figura, relativa allo Shared Responsibility Model di AWS, il cloud provider è responsabile della "sicurezza *del* cloud", nel senso che AWS si occupa di proteggere l'infrastruttura globale su cui vengono eseguiti tutti i servizi offerti nel cloud AWS. L'infrastruttura è formata dai componenti hardware e software, le reti e le strutture che eseguono i servizi Cloud AWS.
Il cliente è responsabile della "Sicurezza *nel* cloud", cioè la responsabilità del cliente verrà determinata dai servizi cloud AWS scelti da un cliente. Questo determina l'entità del lavoro di configurazione che il cliente deve eseguire come parte delle proprie responsabilità di sicurezza. In tutti i casi un cloud provider come AWS fornisce ai propri clienti i servizi di sicurezza cloud necessari a predisporre l'ambiente cloud conforme alle proprie politiche e meccanismi di sicurezza.

2.1 Attacchi più frequenti e più sofisticati

Nonostante la generale sottovalutazione del rischio informatico da parte delle PMI italiane, sia la pandemia sia l'instabilità creata dall'invasione russa dell'Ucraina hanno provocato non solo un'accelerazione alla guerra e alla criminalità cibernetiche, ma anche – così si evince da alcuni studi – un'evoluzione qualitativa delle minacce: gli attacchi cyber, dunque, si sono fatti più frequenti e anche più complessi.

I risultati del *Rapporto Clusit 2022 sulla sicurezza ICT in Italia*, pubblicato a marzo 2022, dicono appunto che nel 2021 "gli attacchi [informatici] nel mondo sono aumentati del 10% rispetto all'anno precedente, e sono sempre più gravi. Le nuove modalità di attacco dimostrano che i cyber criminali sono sempre più sofisticati e in grado di fare rete con la criminalità organizzata". Gli attacchi, poi, "crescono in quantità e in "qualità", con ripercussioni maggiori sugli aspetti di immagine, economici e sociali di un'azienda o di un ente.

Nel 2021 il 79 per cento degli attacchi informatici rilevati da Clusit ha avuto un impatto definito elevato, contro il 50 per cento del 2020: il 32 per cento di questi è stato caratterizzato da un livello di *severity* critico, e il 47 per cento da un livello alto. Sono diminuiti, invece, gli attacchi di impatto medio (-13 per cento) e di impatto basso (-17 per cento).

La stragrande maggioranza (l'86 per cento) degli attacchi informatici effettuati nel 2021 era riconducibile a motivazioni di tipo criminale: il dato è in aumento rispetto al 2020 (81 per cento) e, secondo Clusit, si inserisce in "un trend che non accenna a diminuire". Tra gli attacchi gravi di dominio pubblico, invece, l'11 per cento andava ricondotto ad attività di spionaggio e il 2 per cento a campagne di guerra dell'informazione (*information warfare*). A livello geografico, gli attacchi informatici colpiscono principalmente il continente americano (45 per cento dei casi), ma quelli diretti all'Europa e all'Asia stanno crescendo: dal 16 al 21 per cento nel primo caso; dal 10 al 12 per cento nel secondo.

Una tendenza di *cybersecurity* particolarmente rivelante per l'Italia è la crescita dei *malware* (codici malevoli) e delle *botnet* (reti di dispositivi "infettati" con software maligni): il numero dei server compromessi è cresciuto del 58 per cento. Ma le infezioni si diffondono sempre più anche per via mobile: particolarmente diffuso è FluBot, un *malware* per dispositivi Android che viene distribuito attraverso link di *phishing* condivisi con le app di messaggistica o gli SMS. I settori più colpiti in Italia sono quello finanziario-assicurativo e la pubblica amministrazione, che insieme rappresentano il 50 per cento circa dei casi. Ma la crescita più significativa è stata registrata dal settore industriale, che nel 2020 valeva il 7 per cento dei casi e un anno dopo il 18 per cento.

2.2 Gestire il rischio: i cloud di fornitori specializzati

Considerato lo scenario globale appena descritto, la dotazione di misure adeguate a gestire e contenere il rischio informatico dovrebbe essere la priorità per le imprese, di qualunque dimensione. Un'azienda, dunque[18], dovrebbe anzitutto dotarsi dell'organizzazione e delle tecnologie necessarie a ridurre il rischio che un attacco informatico finisca per essere causa di una lunga interruzione delle attività.

Per farlo, è necessario innanzitutto procedere a un'analisi approfondita volta a individuare le vulnerabilità e le criticità dei propri sistemi, in modo da stilare poi un programma di potenziamento mirato. Andrà garantita la sicurezza dei luoghi in cui si custodiscono i dati e la protezione degli accessi alle reti, ai software e alle applicazioni. Andranno, infine, stanziate risorse per migliorare la cultura aziendale, in modo da diffondere internamente, tra i dipendenti, la consapevolezza dell'importanza della sicurezza informatica. In caso di cyberattacchi particolarmente gravi, oppure di eventi disastrosi (come terremoti o incendi) che arrechino danni seri ai data center, l'azienda potrebbe mitigare il danno attraverso soluzioni di ripristino dei sistemi informatici di base in un sito alternativo o nel cloud.

In questo c'è da rilevare che, a differenza del passato, si diffonde l'idea che i server locali siano meno sicuri di quelli esterni: molte società sono convinte che i fornitori di servizi cloud siano in grado di assicurare una maggiore sicurezza informatica di quanto non possano fare loro stessi. Del resto, è con la stessa logica che si preferisce custodire i preziosi nelle cassette di sicurezza piuttosto che nelle proprie abitazioni: banche e istituti finanziari possono assicurare livelli di protezione più elevati contro i furti e sono coperti dai rischi con assicurazioni. A livello aneddotico si possono riscontrare molti esempi che testimoniano quanto le difese dei grandi fornitori di cloud siano più robuste di quelle delle singole imprese. Una tipologia di attacco rivolta verso i server è denominata DDoS (Distributed Denial of Service). Si tratta di tentativi ostili di bloccare le normali operazioni di un server, servizio o rete inondandoli di traffico Internet, spesso utilizzando più di una macchina per inviare traffico dannoso al loro obiettivo. Un attacco DDoS di circa 0,5 Terabit di dati al secondo (ossia 500 Gigabit al secondo) rappresenta una minaccia in grado di paralizzare la maggior parte dei server. I sistemi di sicurezza dei fornitori di cloud più avanzati sono in grado di assorbire attacchi 5-7 volte superiori.

In effetti, la difesa dei dati è nel massimo interesse delle imprese di cloud. Si stima che la tipica perdita di dati per una grande azienda è compresa tra 10 e 99 milioni di record per incidente e una violazione dei dati di queste dimensioni comporta in media un calo del valore aziendale del 7,27%. Questo dato, per società che vantano capitalizzazioni di migliaia di miliardi di dollari, corrisponde ad almeno un centinaio di miliardi di dollari. Inoltre, nel caso dei grandi fornitori di servizi cloud, la ripercussione dell'accaduto sarebbe ancora più rovinosa. Per tornare al paragone precedente, la violazione delle cas-

18 Si veda Capra E., "Imprese italiane e cyber security: ecco come proteggersi", su Cybersecurity360, *19/04/2022*

sette di sicurezza di una banca ne mettono a dura prova la reputazione. È la capacità di essere inviolabile a costituire il principale asset della banca, ma anche qualora dovesse accadere l'irreparabile, gli istituti finanziari possono contare sul supporto delle cospicue polizze assicurative contro i furti. Gli strumenti di difesa a disposizione dei grandi fornitori di servizi cloud sono senza dubbio più sviluppati delle dotazioni di sicurezza di una qualunque azienda. A questo si deve aggiungere l'affidabilità dei server che certificati a livelli prossimi a zero rischi (i server TIER IV hanno un'affidabilità pari al 99,995%).
Gartner, una delle principali società di ricerca e consulenza in ambito digitale, stima che la sicurezza del cloud è la categoria che potrà registrare la crescita più forte tra i servizi di cybersecurity nei prossimi due anni (+22% nel 2022 e +27% nel 2023)[19]. Non solo le grandi organizzazioni sono interessate da questa dinamica, ma anche le aziende di media dimensione per le quali Gartner prevede che la migrazione ai sistemi cloud rappresenti uno dei principali driver di crescita del mercato IT[20].

2.3 Il ruolo del cloud per minimizzare i rischi, contrastare gli attacchi e rafforzare la conformità[21]

I grandi cloud service providers come AWS aiutano le aziende, che spostano in cloud i propri *workload*, a sfruttare le tecnologie cloud per proteggere dati, sistemi e risorse in modo da migliorare il livello di sicurezza generale.
Nel cloud, ci sono una serie di principi che possono aiutare le aziende a rafforzare la sicurezza dei loro *workload*. I principi di sicurezza più importanti sono i seguenti.
Implementare solidi meccanismi basati sulla identità: implementa il principio del privilegio minimo e applica la separazione dei compiti con l'autorizzazione appropriata per ogni interazione con le risorse AWS. Centralizza la gestione delle identità e mira a eliminare la dipendenza da credenziali statiche a lungo termine.
Abilitare la tracciabilità: monitora, avvisa e verifica le azioni e le modifiche all'ambiente in tempo reale. Integra la raccolta di registri e metriche con i sistemi per analizzare e agire automaticamente.

- Applicare la sicurezza a tutti i livelli: applica un approccio di difesa approfondito con più controlli di sicurezza. Applicabile a tutti i livelli (ad esempio, edge of network, VPC, load balancing, ogni istanza e servizio di elaborazione, sistema operativo, applicazione e codice).
- Automatizzare le *best practices* di sicurezza: i meccanismi di sicurezza automatizzati basati su software migliorano la tua capacità di scalare in modo sicuro in modo più rapido ed economico. Crea architetture sicure, inclusa l'implementazione di controlli definiti e gestiti come codice in modelli controllati dalla versione.

19 https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i
20 https://www.gartner.com/en/newsroom/press-releases/2022-09-26-gartner-says-cybersecurity-application-and-integration-strategies-and-cloud-are-top-technology-priorities-for-midsize-enterprises
21 Contenuto a cura di AWS

- Proteggere i dati in transito e a riposo: classifica i tuoi dati in base a livelli di sensibilità e utilizza meccanismi, come la crittografia, la tokenizzazione e il controllo degli accessi, se del caso.
- Tenere le persone lontane dai dati: utilizza meccanismi e strumenti per ridurre o eliminare la necessità di accesso diretto o di elaborazione manuale dei dati. Ciò riduce il rischio di cattiva gestione o modifica e di errore umano durante la gestione di dati sensibili.
- Prepararsi per gli eventi di sicurezza: preparati a un incidente adottando politiche e processi di gestione degli incidenti e di indagine in linea con i requisiti aziendali. Esegui simulazioni di risposta agli incidenti e utilizza strumenti automatizzati per aumentare la velocità di rilevamento, indagine e ripristino.

Il cloud per contrastare attacchi DDoS[22]

Un attacco Denial of Service (DoS) è un tentativo dannoso di interferire con la disponibilità di un determinato sistema, come un sito web o un'applicazione, per conto degli utenti legittimi. In genere, gli attacker generano grandi volumi di pacchetti o richieste travolgendo il sistema di destinazione. Nel caso di un attacco Distributed Denial of Service (DDoS), per generare l'attacco l'attacker utilizza più origini controllate o compromesse.

In generale, gli attacchi DDoS possono essere isolati dallo strato del modello Open Systems Interconnection (OSI) che attaccano. Gli attacchi sono più comuni sui livelli di rete (layer 3), trasferimento (layer 4), presentazione (layer 6) e applicazione (layer 7). Gli attacchi ai livelli 3 e 4 si possono classificare come attacchi alle infrastrutture. Gli attacchi ai livelli 6 e 7 come attacchi alle applicazioni.

Per proteggersi da attacchi DDoS occorre ridurre la superficie di attacco, avere a disposizione un piano per la scalabilità (sia di traffico sia di server), avere la capacità di riconoscere il traffico normale e quello anomalo, dislocare opportunamente firewall per gli attacchi sofisticati alle applicazioni.

È importante proteggere la propria azienda dall'impatto degli attacchi DDoS e di altri attacchi informatici. AWS fornisce sia linee guida prescrittive sugli attacchi DDoS, per migliorare la resilienza delle applicazioni in esecuzione su AWS, sia servizi cloud gestiti che aiutano i clienti a proteggersi da questa tipologia di attacchi. Ciò include un'architettura di riferimento resiliente agli attacchi DDoS che può essere utilizzata come guida per proteggere la disponibilità delle applicazioni.

In particolare, AWS Shield è un servizio di sicurezza gestito che protegge le applicazioni web dei clienti contro gli attacchi DDoS, che potrebbero influire sulla disponibilità delle applicazioni o consumano risorse eccessive. AWS Shield protegge dai più grandi attacchi volumetrici (layer 3/4) e attacchi a livello di applicazione (layer 7) senza complessità

22 Contenuto a cura AWS

e impatto sulle prestazioni o costo tradizionalmente associati alle tecnologie di protezione dagli attacchi DDoS. Fornisce inoltre visibilità sul traffico di attacco, l'accesso a un team di risposta DDoS (DRT) attivo 24 ore su 24, 7 giorni su 7 e una protezione economica per prevenire gli attacchi che produrrebbero un aumento nei costi della fattura mensile. AWS Shield rende i servizi AWS intrinsecamente resilienti agli attacchi DDoS e rimuove l'onere di predisporre una architettura *ad hoc* per la protezione dagli attacchi DDoS. Il livello standard di AWS Shield è disponibile per tutti i clienti AWS senza costi aggiuntivi. AWS Shield Standard Tier protegge automaticamente dagli attacchi più comuni al mondo, sfruttando la scalabilità della rete AWS.
AWS Shield è disponibile sugli stessi servizi AWS che i clienti utilizzano per eseguire le proprie applicazioni web. I clienti non devono apportare modifiche alla propria architettura, aggiungere un nuovo livello davanti all'applicazione o cercare un fornitore esterno per abilitare la protezione dagli attacchi DDoS. AWS Shield esiste in modo trasparente davanti alle risorse AWS. I clienti devono semplicemente "punta e clicca" per abilitare la protezione dagli attacchi DDoS
Il servizio AWS Shield fornisce un monitoraggio attivo del flusso di traffico di rete, ispezionando il traffico in entrata nell'infrastruttura del cliente. I sistemi di rilevamento sempre attivi rilevano gli attacchi utilizzando diverse tecniche fondate su rilevamenti basati su anomalie o euristiche. Per gran parte degli attacchi, le misure di mitigazione degli attacchi vengono attivate automaticamente quando gli attacchi vengono rilevati, garantendo ai clienti un "tempo di mitigazione" molto ridotto. Per altri attacchi di livello 3 e 4, il DDoS Response Team è automaticamente impegnato a intraprendere azioni manuali e mitigazioni quando necessario.

Il cloud per proteggere i dati e mantenere la conformità[23]

Una parte essenziale della gestione di un'azienda fiorente è mitigare le minacce alla sicurezza esistenti ed emergenti. Identificando e affrontando potenziali lacune nella sicurezza dei dati, le aziende di tutte le dimensioni possono adottare misure per proteggere i dati dei clienti, salvaguardare la proprietà intellettuale (IP) e mantenere la conformità. Le violazioni dei dati aziendali sono aumentate di quasi il 20% nel 2021, quindi concentrarsi sulla sicurezza dei dati è un imperativo per ogni azienda.
Amazon Web Services mette in luce che l'adozione di strumenti basati sul cloud offre alle aziende soluzioni integrate e automatizzate per la sicurezza della rete e dei dati, la gestione della configurazione, il controllo degli accessi, il monitoraggio e la visibilità. Inoltre, il cloud è progettato per essere sicuro senza l'esborso di capitale e il sovraccarico operativo di un data center tradizionale. Via via che l'azienda cresce, cloud come quello di AWS, può fornire sempre una scalabilità sicura[24]. La capacità si può aumentare quando se ne ha bisogno e diminuire quando non se ne ha bisogno. Una azienda che

23 Contenuto a cura AWS
24Non rientrano le aziende facenti parte del Perimetro di Sicurezza Nazionale Cibernetica (PSNC) e gli enti della PA

sfrutta il cloud paga solo per quello che viene usato e ne eredita tutti i controlli di sicurezza.
Avevamo già accennato al concetto che un'azienda, indipendentemente dalla sua dimensione, che porta i suoi *workload* in cloud eredita i controlli di sicurezza messi in campo dal cloud provider a protezione della infrastruttura globale. Tali controlli costituiscono la base sulla quale i cloud service provider costruiscono i loro programmi di conformità che sono verificati da auditor di terze parti. Nel caso specifico, il cloud di AWS è progettato per essere l'ambiente di cloud computing tra i più flessibili e sicuri disponibili oggi. La sua infrastruttura principale è progettata per soddisfare i requisiti di sicurezza per il settore militare, delle banche globali e di altre organizzazioni ad alta sensibilità[25]. Questo è supportato da una serie completa di strumenti di sicurezza cloud, con oltre 300 servizi e funzionalità di sicurezza, conformità e governance. Inoltre, AWS supporta 98 standard di sicurezza e certificazioni di conformità, tra cui: ISO/IEC, PCI-DSS, HI¬PAA/HITECH, FedRAMP, GDPR, FIPS 140-2 e NIST 800-171, che aiutano a soddisfare i requisiti di conformità delle agenzie di regolamentazione.

2.4 Gestire il rischio: le coperture assicurative

La parte residuale di rischio, vale a dire una certa frazione dei costi legati a un attacco cyber, può essere trasferita al mercato assicurativo. Per farlo, tuttavia, è necessario che l'impresa si sia già dotata di difese informatiche solide: le compagnie assicurative, per tutelarsi dal rischio di offrire copertura ad aziende carenti sul lato tecnologico, prendono infatti in considerazione solo le richieste provenienti da soggetti dotati di certi requisiti minimi; requisiti, peraltro, che si fanno via via più stringenti parallelamente all'evoluzione delle minacce. A livello generale, comunque, è ancora basso il numero delle imprese – specie se si parla di piccole e medie – che decidono di sottoscrivere una polizza *cyber risk*, vista la limitata attenzione al tema.
Le polizze di copertura dai rischi informatici assicurano dai danni diretti (la perdita di dati, ad esempio), da quelli indiretti (come le perdite di profitto e le spese di recupero) e dalle responsabilità civili verso quelle terze parti (clienti o fornitori) di cui il soggetto assicurato detiene informazioni sensibili, come dati personali o proprietà intellettuali. Polizze più ampie possono includere opzioni per la protezione dagli attacchi di *social engineering* (falsificazione d'identità o dirottamento di pagamento) e dai furti di denaro tramite operazioni informatiche illecite, o anche estensioni per il risarcimento in caso di arresto volontario dei sistemi per motivi ragionevoli (*voluntary shutdown*).
Nelle trattative con le imprese, le compagnie assicurative chiedono di compilare dei questionari per valutare la sicurezza dei sistemi informatici aziendali. Tra i prerequisiti richiesti per la stipula di una polizza figurano l'utilizzo di meccanismi di autenticazione a più fattori; la presenza di backup sicuri, offline o in cloud; l'esecuzione di *vulnerability assessment* (test di identificazione e quantificazione delle debolezze informatiche) con

25 Il mercato di riferimento è principalmente quello degli USA

cadenze regolari; la formazione dei dipendenti in materia di cybersicurezza; la disponibilità di procedure per la gestione degli attacchi e la ripresa.
Non sono molte le aziende che soddisfanno questi requisiti minimi; di conseguenza, il mercato assicurativo italiano del rischio cyber è "ristretto", dato il basso numero di compagnie disposte ad assumersi i rischi, e "duro". Si parla di *hard market* perché i premi assicurativi sono in aumento, la capacità assuntiva è ridotta, i tempi di quotazione si allungano e ci sono maggiori difficoltà ad assicurare tutti i rischi. Una rilevazione di Assiteca[26] ha riscontrato, nell'ultimo trimestre del 2021, degli aumenti medi dei costi assicurativi delle polizze cyber pari al 20 per cento. In alcuni casi – in presenza di sistemi informatici poco strutturati, o di settori ad elevato rischio come la finanza e la sanità, per esempio – si arriva anche al raddoppio. Le realtà che hanno necessità di assicurare massimali ampi, intorno ai 20-30 milioni di euro, devono frazionare il rischio su più assicuratori, nell'ordine di 5-7 milioni di euro l'uno.
Dal rapporto di Deloitte *Il futuro delle assicurazioni per le PMI dopo la pandemia* si evince come la pandemia di coronavirus abbia modificato la percezione dei rischi tra le PMI italiane. Tra le cinque principali categorie di rischio (rischio cibernetico, rischio pandemico, rischio sistemico, rischio climatico e rischio catastrofale), queste aziende identificano quello cibernetico come il primo rischio aggiuntivo da cui ritengono necessario proteggersi, e che non sia già previsto dalla loro copertura assicurativa: il dato è del 33 per cento, contro una media internazionale del 25 per cento. Un'importanza sostanzialmente pari (32 per cento, contro una media del 27) viene attribuita al rischio pandemico. Questa crescita dell'attenzione alle minacce provenienti dal dominio cyber è una tendenza mondiale, con il rischio cibernetico che si sostituisce, per grado di urgenza, ad altri più tradizionali come il rischio sistemico economico-finanziario o il rischio catastrofale.
Come fa notare Deloitte, questo aumento della percezione non corrisponde necessariamente a una maggiore volontà di spesa in cybersicurezza: le PMI, anzi, dicono di essere più propense a spendere in misure di prevenzione e contenimento dei rischi sistemico e catastrofale. Alla domanda "Quanto saresti disposto a spendere all'anno per aggiungere una copertura assicurativa che copra queste categorie di rischio?", nelle fasce di spesa 11.600-23.499 euro e 23.500-34.999 euro il rischio cyber occupa la posizione più bassa, rispettivamente del 6 e del 4 per cento.
Nel nuovo contesto creato dalla pandemia, le PMI italiane dichiarano di avere un livello elevato di copertura assicurativa: solo il 4 per cento di queste non ne possiede affatto (la media del campione internazionale è del 2 per cento). In termini di tipologie di coperture assicurative, quelle più diffuse tra le aziende di ridotte e medie dimensioni sono quelle per la protezione della flotta aziendale (48 per cento in Italia, contro una media internazionale del 34 per cento); per la protezione dei danni diretti ai fabbricati e al loro contenuto (37 contro 46 per cento); per la protezione dalle responsabilità civili verso dipendenti, clienti e fornitori (29 contro 31 per cento); per la protezione dal rischio cyber, infine (25 contro 26 per cento).

26 Si veda Veronesi V., "Cyber risk e cyber security: tra prevenzione e protezione", su AziendaBanca*, marzo 2022*

3.1 PNRR, digitalizzazione e PMI

PNRR dispone 620 milioni di euro per stimolare la cybersicurezza della pubblica amministrazione, ma stanzia anche risorse per l'aggiornamento informatico dei processi aziendali e la digitalizzazione[27]. L'Italian Digital SME Alliance, raggruppamento di associazioni e PMI, pensa che il piano debba essere guidato in un modo sì strategico ma anche "capillare, perché deve riuscire a coinvolgere un vasto tessuto socioeconomico fatto di piccole e medie imprese, che spesso non hanno la cultura e le risorse per uscire dalla comfort zone e attivare il cambiamento". L'associazione ha sviluppato allora un documento[28] contenente tre macro-proposte per favorire la crescita digitale e culturale delle PMI italiane.

L'Italian Digital SME Alliance chiede innanzitutto di creare le condizioni per la partecipazione di queste aziende al processo di trasformazione digitale della pubblica amministrazione. Ad esempio si potrebbe introdurre, nei grandi lotti Consip, la suddivisione in lotti più piccoli, con una percentuale minima del 30 per cento da dedicare in modo esclusivo alle PMI. È inoltre necessario, secondo l'associazione, garantire la libera concorrenza nel mercato ICT.

Come seconda proposta, l'associazione propone di favorire la trasformazione digitale delle PMI attraverso bandi e incentivi fiscali, che vanno pensati e stilati tenendo in considerazione le aziende di ridotte dimensioni. In questo senso si possono definire, per esempio, dei bandi a fondo perduto che coprano almeno il 60 per cento dell'investimento, con una rendicontazione semplificata e veloce (trenta giorni) su progetti almeno di 10.000 euro e dalla durata massima di un anno. Può essere utile attuare dei finanziamenti *ex ante* perché molte PMI, nonostante la vincita di un bando, spesso non hanno la disponibilità per anticipare l'investimento. Per agevolare il processo, l'Italian Digital SME Alliance avanza una proposta di armonizzazione del credito d'imposta alla dimensione dell'impresa in maniera inversamente proporzionale: si partirebbe dal 20 per cento per le aziende con un fatturato superiore ai 5 milioni di euro, per arrivare ad una quota del 50 per cento per quelle con fatturato inferiore ai 2 milioni.

Il terzo e ultimo punto insiste sulla promozione della ricerca e sviluppo nelle aziende ICT e digitali, prevedendo per queste dei bandi a fondo perduto relativi ad attività di ricerca e sviluppo. Dovrebbe essere prevista – anche in questi casi – la possibilità di accesso immediato a un finanziamento bancario che anticipi la cifra vinta nel bando, fissando

27In particolare, per la digitalizzazione della PA, sono previsti circa 30 miliardi di euro. Considerando l'intera Missione 1 del Piano Nazionale di Ripresa e Resilienza, che si pone l'obiettivo di dare un impulso decisivo al rilancio della competitività e della produttività del Sistema Paese, è possibile una stima complessiva di circa 45 miliardi di euro.

28Il documento, intitolato "Massimizzare le potenzialità del PNRR per la crescita digital e culturale delle PMI" e datato 8 febbraio 2022, è disponibile all'indirizzo digitalsme.eu/digital/uploads/Italian-Digital-SME-Alliance_PNRR.pdf

un tetto minimo di investimento di 20.000 euro. Per favorire la visibilità di aziende e progetti innovativi, può essere utile includere nei bandi una voce a sostegno della loro promozione sul web. Infine, si potrebbe formare una cabina di regia con le associazioni di categoria, le università e gli enti di ricerca per la condivisione di un piano per la razionalizzazione di queste iniziative, facendole convergere verso uno "schema di rete di ecosistemi dell'innovazione".

3.2 Le *best practices* per le PMI

Nel giugno del 2021 l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) ha pubblicato un rapporto (*Cybersecurity for SMEs. Challenges and Recommendations*) dedicato alla sicurezza informatica per le piccole e medie imprese, cruciali per l'economia non solo italiana ma europea: la Commissione le definisce infatti "la spina dorsale dell'economia dell'Ue. Rappresentano il 99% di tutte le imprese dell'Ue e danno lavoro a circa 100 milioni di persone. Rappresentano inoltre più della metà del PIL europeo e svolgono un ruolo fondamentale nel creare valore aggiunto in tutti i settori dell'economia dell'Ue". L'ENISA, tuttavia, registra come le PMI «non sembrano rendersi conto che la sicurezza informatica non è qualcosa che riguarda solo le organizzazioni più grandi»: la sottovalutano, e finiscono così per l'esporsi a rischi che possono degenerare nella bancarotta. Eppure "la crisi COVID-19 ha messo in evidenza l'importanza di internet e dei computer in generale per le piccole e medie imprese", le quali, per proseguire l'attività durante i *lockdown*, "hanno dovuto adottare misure di continuità operativa, quali il ricorso a servizi cloud, il miglioramento dei propri servizi Internet, il potenziamento dei siti web e il lavoro a distanza per i dipendenti".

L'agenzia ha allora stilato un evento di dodici linee guida[29] che le aziende possono seguire per cominciare a migliorare i sistemi informatici e proteggere il business dalla cybercriminalità; le indicazioni, estremamente pratiche, tengono conto delle necessità delle PMI di ottimizzare le spese, del loro scarso tempo disponibile per aggiornarsi su una materia in continua evoluzione e della carenza di risorse umane impiegabili, visto il difficile contesto economico.

La prima regola consiste nello «sviluppare una solida cultura della cybersicurezza» attra-verso l'attribuzione di responsabilità e il coinvolgimento del personale. L'ENISA consiglia alle PMI di assegnare le responsabilità di cybersicurezza a una persona, che avrà così il compito – specifico, e non secondario rispetto ad altre mansioni – di verificare e garantire che vengano destinate a questo scopo delle risorse appropriate: vale a dire impegno in termini di tempo; acquisto di software e hardware; formazione del personale; sviluppo di politiche in materia di cybersicurezza. In secondo luogo, i quadri dirigenziali dell'azienda dovrebbero elaborare una comunicazione efficace sulla cybersicurezza in modo da coinvolgere i dipendenti, formarli e fornire loro regole chiare sulle pratiche da seguire – con tanto di conseguenze in caso di violazioni – quando accedono alle attrezzature e ai servizi informatici.

29 Consultabili, in italiano, all'indirizzo enisa.europa.eu/publications/report-files/smes-leaflet-translations/enisa-cybersecurity-guide-for-smes_it.pdf

L'ENISA invita poi a svolgere, con cadenza periodica, degli audit di cybersicurezza da far condurre a persone in possesso di conoscenze, competenze ed esperienze appropriate. I revisori dovranno essere delle figure indipendenti, cioè non coinvolti nelle quotidiane operazioni informatiche: dei contraenti esterni, ad esempio. I controlli dovranno servire ad accertare anche il rispetto del regolamento sulla protezione dei dati personali conservati dalla PMI e dagli eventuali soggetti terzi con cui lavora.
La seconda regola ha a che vedere con la formazione di tutti i dipendenti della PMI, a cui andrà garantita un'appropriata educazione alla cybersicurezza che – oltre a sensibilizzarli all'argomento – gli permetta di riconoscere e affrontare le varie minacce. L'ENISA scrive che i corsi di formazione cyber dovrebbero essere personalizzati per le PMI e concentrarsi su situazioni di vita reale, in modo da consentire una migliore ricezione delle informazioni trasmesse. Andranno definiti anche percorsi specialistici per gli informatici e gli stessi responsabili della cybersicurezza, per aggiornarli alle nuove tecnologie e ai nuovi rischi.
Come terza regola, l'ENISA invita le PMI ad assicurarsi che tutti i fornitori, e in particolare quelli che hanno accesso a dati o sistemi sensibili, soddisfino i livelli di cybersicurezza richiesti: andranno pertanto stipulati degli accordi contrattuali per definirli nello specifico. Essendo pienamente inseriti nella *supply chain* della PMI, la vulnerabilità informatica dei fornitori può ripercuotersi sull'azienda "committente" del prodotto o servizio.
È poi necessario (quarta regola) elaborare un piano di risposta agli incidenti informatici che definisca con chiarezza orientamenti, ruoli e responsabilità, in modo da permettere una risposta appropriata, professionale e tempestiva: oltre a mitigare il danno, un piano di questo tipo. «Per rispondere prontamente alle minacce per la sicurezza", scrive l'agenzia, bisogna "studiare gli strumenti che potrebbero monitorare e creare allerta in caso di attività sospette o di violazioni della sicurezza".
La fase di autenticazione ai servizi o ai sistemi operativi è cruciale, e la quinta regola dice proprio di "rendere sicuro l'accesso ai sistemi". L'ENISA incoraggia tutti i dipendenti dell'impresa a utilizzare una frase d'accesso (*passphrase*) che sia composta da almeno tre parole scelte a caso che forniscano una combinazione facilmente ricordabile ma anche sicura, per via della lunghezza. Se invece si decide di optare per una più tradizionale password, questa deve essere lunga e composta da caratteri minuscoli e maiuscoli, più numeri e caratteri speciali ("?", "!" o "$"). Bisogna, al contrario, evitare ovvietà come «password», «abc» o «123», ma anche informazioni personali che possono essere reperite online (la data di nascita, il nome del partner o dell'animale domestico). Sia nel caso di *passphrase* che di password, queste non devono essere utilizzate per accedere a servizi o sistemi diversi e non devono essere condivise con i colleghi. Per aumentare ulteriormente il livello di sicurezza, l'agenzia raccomanda di attivare l'autenticazione a più fattori e di utilizzare software di *password manager* (gestore di password).
La sesta regola dice di "rendere sicuri i dispositivi» a disposizione del personale, siano

essi computer, laptop, smartphone o tablet. Tutti i loro software andranno mantenuti aggiornati: per ottimizzare il processo, l'ENISA raccomanda l'utilizzo di una piattaforma centralizzata. Essendo aggiornamenti e *patch* cruciali per la cybersicurezza, l'agenzia ci tiene a raccomandare alle PMI di aggiornare i software con regolarità, di procedere agli aggiornamenti automatici ogniqualvolta è possibile, di tenere traccia di software e hardware che richiedono aggiornamenti manuali, di non trascurare i dispositivi mobili e IoT (da *Internet of Things*, o Internet delle cose). Quanto agli antivirus, per ENISA la soluzione migliore è quella a gestione centralizzata su tutti i tipi di dispositivi, evitando l'installazione di software pirata che potrebbero contenere *malware*. È fondamentale anche adottare soluzioni di blocco delle e-mail indesiderate (*spam*), quelle contenenti allegati dannosi (*virus*) e dei messaggi di *phishing*. Un ulteriore strumento utile alla protezione dei dati è la crittografia: andranno criptati non solo i dati conservati su laptop e smartphone, ma anche quelli trasferiti su reti pubbliche (ad esempio le reti Wi-Fi degli aeroporti o degli alberghi) grazie all'utilizzo di reti private virtuali (VPN) e del protocollo SSL/TLS per l'accesso sicuro ai siti web. Anche il sito web aziendale dovrà disporre di protocolli di cifratura aggiornati, in modo da proteggere i dati dei dipendenti, dei fornitori e dei clienti. Nel caso in cui i dipendenti lavorino a distanza, permettere loro di utilizzare i propri smartphone o laptop può rivelarsi rischioso sotto il profilo della sicurezza dei dati gestiti da quei dispositivi. Il rischio, tuttavia, può essere tenuto sotto controllo utilizzando un software di gestione dei dispositivi mobili (*mobile device management*) che permetta all'impresa di monitorare quali dispositivi dispongano dell'autorizzazione ad accedere ai propri sistemi; di assicurarsi che nel dispositivo sia installato un antivirus aggiornato; di stabilire se il dispositivo debba venire criptato; di assicurarsi che il dispositivo utilizzi un software aggiornato e sia protetto da PIN o password; di eliminare da remoto, se necessario (ad esempio in caso di furto o di smarrimento da parte del proprietario, o di termine del rapporto lavorativo), i dati aziendali presenti.

Per rendere sicura la rete (settima regola), l'ENISA raccomanda alla PMI di utilizzare un firewall e di analizzare le soluzioni di accesso remoto. Nel primo caso – un firewall è un componente hardware/software che gestisce il traffico in entrata e in uscita da una rete –, si invita l'azienda ad utilizzare dei firewall per proteggere tutti i propri sistemi i critici, e in particolare la propria rete interna da Internet. Nel secondo caso, procedere all'analisi periodica di tutti gli strumenti di accesso remoto permetterà di garantire la loro sicurezza: oltre a verificare il loro aggiornamento, si potrà limitare l'accesso da luoghi o indirizzi IP di natura sospetta, limitare l'accesso dei dipendenti ai soli strumenti davvero necessari per lavorare, monitorare i meccanismi di allerta in caso di attività sospette o attacchi.

L'ottava regola dell'ENISA parla di come migliorare la sicurezza informatica a partire dalla sicurezza fisica dei luoghi e dei dispositivi in cui sono presenti informazioni importanti. Laptop e smartphone non devono essere lasciati incustoditi, ad esempio sul sedi-

le di un'automobile. I computer andrebbero bloccati (è possibile predisporre funzioni di blocco automatico) ogniqualvolta ci si allontana dalla postazione di lavoro. I documenti sensibili stampati, quelli dai quali è possibile ottenere informazioni utili alla sottrazione di dati informatici, vanno archiviati in locali sicuri e sorvegliati, a cui può accedere solo il personale autorizzato.

In caso di attacco informatico come un *ransomware*, un backup può rivelarsi cruciale ai fini della mitigazione del danno. La ridondanza del dato è un aspetto fondamentale delle politiche di cybersicurezza e il backup, in quest'ottica, rappresenta un modo efficace per recuperare informazioni preziose e garantire continuità al business; a patto però che venga predisposto e gestito bene. Il backup – raccomanda l'ENISA nella sua nona regola – deve svolgersi in automatico e ogniqualvolta possibile; deve essere tenuto separato dai sistemi informatici del ciclo produttivo della PMI; deve essere criptato; deve esserne testata la capacità di ripristino regolare e completo dei dati, effettuando simulazioni periodiche.

Anche il cloud computing, protagonista della decima regola, è fondamentale per irrobustire le difese informatiche, ma può presentare anche dei rischi. "Quando scelgono un provider di servizi cloud", avverte l'ENISA, "le PMI dovrebbero fare in modo di non violare leggi o regolamenti in caso di conservazione di dati, specialmente dati personali, al di fuori dell'Ue/del SEE. Ad esempio, il regolamento generale dell'Ue sulla protezione dei dati richiede che i dati personali di residenti Ue/SEE non siano conservati o trasmessi al di fuori dell'Ue/del SEE, salvo in casi molto specifici". In aggiunta alle valutazioni di rispetto delle norme del GDPR sul trasferimento dei dati, le aziende dovrebbero analizzare anche le specifiche sulla cifratura dei dati e sui processi di backup del cloud stesso.

L'undicesima regola è dedicata alla sicurezza dei siti web aziendali, che vanno configurati e gestiti in maniera tale da assicurare la protezione dei dati personali e/o finanziari presenti (numeri delle carte di credito, storici degli acquisti e simili). Anche in questo caso, è buona abitudine realizzare dei test periodici della sicurezza, che simulino degli attacchi informatici e consentano di individuare le eventuali carenze e vulnerabilità. I *penetration test* possono avere un costo notevole per le PMI, ma sono fondamentali e previsti dall'articolo 32 del GDPR[30].

Nella dodicesima e ultima regola l'ENISA si sofferma sulla condivisione di informazioni legate alla criminalità informatica, utile perché aiuta le PMI a comprendere meglio la "concretezza" dei rischi cibernetici, a valutare con maggiore cognizione le attività sospette e a non trascurare il loro grado di esposizione alle minacce. "È più probabile che le imprese adotteranno misure per rendere sicuri i loro sistemi se sentono parlare

30 "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: […] una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento*"

dai loro omologhi delle sfide della cibersicurezza e di come sono state superate", nota l'agenzia, "piuttosto che se ne vengono a conoscenza attraverso relazioni del settore o indagini sulla cibersicurezza".

3.3 La conformità al GDPR

Small Business Standards, associazione che rappresenta gli interessi delle PMI a livello internazionale, ed European DIGITAL SME Alliance, la maggiore rete europea di PMI digitali, hanno redatto una guida[31] per aiutare le aziende di ridotte dimensioni ad aumentare le proprie difese informatiche in maniera economicamente efficiente. Le due associazioni suggeriscono alle PMI una serie di controlli minimi indispensabili a proteggere le proprie informazioni e a conformarsi al GDPR.

La guida parte da una definizione: "Le informazioni sono un insieme di dati interpretabili che, all'interno di un dato contesto, hanno un significato e un valore. Per garantire e migliorare questi dati di valore, l'interpretabilità e il contesto devono essere preservati e tutelati". Le informazioni servono ad aumentare conoscenze e competenze, ad adottare decisioni efficaci, ad agire per realizzare degli obiettivi e a misurare i risultati raggiunti. Un'azienda che non sia in possesso di informazioni affidabili, dunque, è di fatto paralizzata: pertanto, dovrebbe prestare massima attenzione alla riservatezza dei dati (per impedire che finiscano in mano a soggetti malevoli), alla loro integrità (per evitare che vengano alterati, compromettendone l'affidabilità) e alla loro disponibilità (per assicurarsi che siano disponibili e raggiungibili in caso di necessità). "Riservatezza, integrità e disponibilità vengono da molto tempo considerate come i tre principali criteri per garantire la sicurezza delle informazioni", si legge. Il rispetto delle regole sul trattamento dei dati è dunque una priorità per le PMI, anche considerando le sanzioni previste in caso contrario.

Il GDPR, in particolare, impone una gestione controllata delle Informazioni di identificazione personale – quelle che riguardano il personale della PMI, i suoi clienti e i suoi fornitori – a partire dal momento in cui il nome di una persona viene associato a qualcos'altro. In quest'ambito sono applicabili i due standard di riferimento sulla sicurezza delle informazioni, l'ISO/IEC 27001 (Sistema di gestione della sicurezza delle informazioni) e l'ISO/IEC 27002 (Codice di pratica per la gestione della sicurezza delle informazioni), integrati dall'ISO/IEC 27701, che è dedicato espressamente alle Informazioni di identificazione personale. Ciascuna PMI europea, dovendo trattare dati personali per funzionare, deve porsi il problema della conformità al GDPR.

Al di là del rischio sanzionatorio, però, per una PMI l'adozione di tecnologie dell'informazione per innovare e ottimizzare i processi produttivi o la fornitura di servizi è strategica ai fini dell'allineamento alla rivoluzione industriale digitale. In questo senso, la cybersicurezza diventa un asset cruciale ai fini della continuità e della sopravvivenza stessa dell'azienda. Proteggere la riservatezza, l'integrità e la disponibilità delle infor-

31 La Guida ai controlli di sicurezza delle informazioni per le piccole e medie imprese, pubblicata ad aprile 2022, è consultabile all'indirizzo digitalsme.eu*/digital/uploads/SME-ISC-Guide_IT_revFINALE.pdf*

mazioni in possesso, dunque, non garantisce solo il rispetto dei livelli di sicurezza previsti dal GDPR, ma tutela anche lo sviluppo e la competitività nel futuro.
D'altra parte, anche Small Business Standards ed European DIGITAL SME Alliance riconoscono che l'implementazione dei centoquattordici controlli per la conformità di cybersicurezza previsti dallo standard ISO/IEC 27002 potrebbe rivelarsi complesso e costoso da implementare per molte PMI. La guida, pertanto, si concentra su sedici controlli ritenuti essenziali per una politica minima in materia di protezione dei dati che sia efficace. I controlli selezionati – simili, nella sostanza, alle linee guida dell'ENISA già viste – sono i seguenti[32]: consapevolezza in materia di sicurezza delle informazioni; gestione degli asset (compresa la procedura di classificazione); politiche, standard e linee guida; gestione degli incidenti; aspetti di sicurezza delle informazioni in relazione ai fornitori; organizzazione della sicurezza delle informazioni; ulteriori controlli sulla privacy; gestione del controllo degli accessi; sicurezza di rete e scambi di dati; gestione delle vulnerabilità; protezione contro i *malware*; gestione dei backup; gestione delle misure di salvaguardia; prontezza ICT per la continuità operativa; lavoro a distanza; monitoraggio delle minacce informatiche.
La guida stessa riconosce tuttavia che un'implementazione efficace del controllo della sicurezza è impossibile senza una strategia solida alla base e senza obiettivi chiari in materia di sicurezza. Gli standard, infatti, si concentrano su ciò che un'azienda deve fare, ma non sul come debba farlo. Sono necessarie, dunque, conoscenze specialistiche che permettano l'attuazione della strategia, seguendo procedure misurabili attraverso il modello COBIT. Il COBIT (sigla che sta per "Obiettivi di controllo per le informazioni e le tecnologie correlate") è un modello per la governance e la gestione delle informazioni e delle tecnologie aziendali, comprese le problematiche di sicurezza, rivolto all'intera impresa. Stabilisce una netta distinzione tra governance e gestione: la prima è quella che garantisce, ad esempio, che le direttive aziendali vengano stabilite attraverso la definizione di priorità, e che le prestazioni vengano poi monitorate sulla base degli obiettivi concordati; la gestione, invece, pianifica e gestisce le attività. Applicare una metodologia COBIT alla sicurezza informatica permette di raggiungere una maggiore efficienza di costo attraverso l'integrazione degli standard di sicurezza, delle buone pratiche e delle linee guida specifiche.

3.4 Il ruolo del cloud per il rispetto del GDPR[33]

Il Regolamento generale sulla protezione dei dati (GDPR) dell'Unione europea tutela il diritto fondamentale alla privacy e alla protezione dei dati personali di ogni individuo. Il GDPR include i rigorosi requisiti che definiscono e armonizzano gli standard in materia di protezione, sicurezza e conformità dei dati.
Un cloud provider come AWS copre il ruolo di *responsabile del trattamento dei dati* quando i clienti utilizzano i servizi AWS per elaborare i dati personali nei contenuti che

32 Ibidem, pp. 20-55
33 Il contenuto del paragrafo, a cura di AWS, riguarda esclusivamente AWS e non è attribuibile ad altri soggetti.

caricano sui servizi AWS. I clienti potranno utilizzare i controlli resi disponibili dai servizi AWS, ad esempio i controlli di configurazione della sicurezza, per la gestione dei dati personali. In tali circostanze, il cliente potrà ricoprire il ruolo di *titolare* o *responsabile del trattamento dei dati*, mentre AWS sarà il responsabile o il sub-responsabile del trattamento. AWS offre un "Addendum AWS sul trattamento dei dati del GDPR (DPA)" che incorpora gli impegni di AWS in qualità di responsabile del trattamento dei dati. Il DPA del GDPR di AWS, che include Clausole contrattuali standard, fa parte dei Termini di servizio AWS ed è automaticamente disponibile per tutti i clienti che ne hanno bisogno per essere conformi al GDPR.

Quando AWS raccoglie dati personali e determina le finalità e le modalità per il loro trattamento – ad esempio, quando AWS archivia le informazioni dell'account (es. indirizzi e-mail forniti durante la registrazione dell'account) necessarie per la registrazione e l'amministrazione di un account, l'accesso ai servizi o le informazioni di contatto per l'account AWS per fornire assistenza tramite il servizio clienti – agisce da titolare del trattamento dei dati. In tutti i casi viene resa disponibile l'Informativa sulla Privacy di AWS per ulteriori dettagli sul modo in cui AWS tratta i dati personali in qualità di Titolare del trattamento.

È importante sottolineare che i clienti che utilizzano il cloud di AWS hanno il pieno controllo dei propri dati, in quanto essi possono: stabilire dove archiviare i propri dati, selezionando anche il tipo di archiviazione e la loro regione geografica di residenza (dalla quale regione non saranno spostati); scegliere l'opportuno livello di sicurezza dei dati, ad esempio utilizzando una solida crittografia per i dati sia in transito sia inattivi e avendo la possibilità di gestire le proprie chiavi di crittografia personali; gestire l'accesso ai propri dati e ai servizi e risorse di AWS mediante utenti, gruppi, autorizzazioni e credenziali sotto il loro pieno controllo.

Ancora in questo ambito, AWS ha pubblicato il white paper *Navigazione nella conformità ai requisiti di trasferimento dei dati dell'UE*[34], dove fornisce informazioni sui servizi e le risorse che AWS offre ai clienti per aiutarli a effettuare valutazioni sul trasferimento dei dati alla luce della decisione Schrems II e alle seguenti Raccomandazioni[35] del Comitato europeo per la protezione dei dati (EDPB). Il white paper descrive anche le misure supplementari principali adottate e rese disponibili da AWS per proteggere i dati dei clienti.

Infine, la partecipazione attiva di AWS a un Codice di condotta come il CISPE garantisce alle organizzazioni che i loro fornitori di servizi infrastrutturali cloud soddisfino i requisiti applicabili ai dati personali processati nell'ambito del GDPR. Questo fornisce ai clienti del cloud un'ulteriore sicurezza di poter scegliere servizi che sono stati verificati in modo indipendente per la loro conformità con il GDPR.

In questo ambito, a novembre 2022, AWS ha portato a cento il numero dei suoi servizi cloud che sono conformi al Codice di condotta CISPE per la protezione dei dati. CI-

34 Cfr: https://d1.awsstatic.com/whitepapers/Security/navigating-compliance-with-eu-data-transfer-requirements.pdf

35 Cfr: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

SPE[36] (Cloud Infrastructure Services Providers in Europe) è l'associazione dei principali fornitori di servizi di cloud computing che serve milioni di clienti in Europa. Il Codice[37] di condotta CISPE per la protezione dei dati (Codice CISPE) è il primo codice di condotta pan-europeo per la protezione dei dati incentrato sui fornitori di servizi infrastrutturali cloud. Il Codice CISPE è stato approvato Comitato[38] europeo per la protezione dei dati, che agisce per conto di 27 autorità per la protezione dei dati in tutta Europa ed è stato adottato formalmente dall'Autorità francese per la protezione dai dati (CNIL), che opera in qualità di principale autorità di vigilanza. Nel 2017 AWS ha annunciato la sua conformità con una versione precedente del Codice CISPE.
Il Codice CISPE aiuta i clienti a garantire che il proprio fornitore di servizi infrastrutturali cloud offra adeguate garanzie operative per dimostrare la conformità al GDPR e proteggere i dati dei clienti. Alcuni vantaggi chiave del codice CISPE includono:

- Incentrato sull'infrastruttura cloud: chiarisce il ruolo del fornitore di servizi infrastrutturali cloud ai sensi del GDPR per quanto riguarda il trattamento dei dati del cliente, ovvero qualsiasi dato personale elaborato per conto del cliente utilizzando il servizio di infrastruttura cloud.
- Dati in Europa: richiede ai fornitori di servizi infrastrutturali cloud di offrire ai clienti la possibilità di utilizzare servizi per archiviare ed elaborare i dati dei clienti esclusivamente all'interno dello Spazio economico europeo (SEE).
- Privacy dei dati: il Codice CISPE garantisce alle organizzazioni che i loro fornitori di servizi infrastrutturali cloud soddisfino i requisiti applicabili ai dati personali processati per conto loro (dati dei clienti) nell'ambito del GDPR.

Oltre alla conformità al codice di condotta CISPE per la protezione dei dati, AWS offre ai clienti informazioni utili quali report di conformità provenienti da enti di controllo di terza parte, che hanno verificato lo stato di conformità secondo diversi standard e normative di sicurezza informatica, per documentare gli elevati livelli di conformità mantenuti da AWS per la propria infrastruttura. Questi report mostrano ai clienti che vengono protetti i dati personali che scelgono di elaborare in AWS. Ne sono esempio la conformità di AWS alle norme ISO 27001, 27017, 27018 e 27701. In particolare, la conformità di AWS alla norma ISO 27018 evidenzia che AWS dispone di un sistema di controlli rivolto specificatamente a proteggere la privacy dei contenuti affidati dai clienti. Invece, la norma ISO/IEC 27701 specifica i requisiti e le linee guida per stabilire e migliorare continuamente il sistema di gestione delle informazioni sulla privacy (PIMS), incluso il trattamento delle informazioni di identificazione personale (PII). È un'estensione degli standard ISO/IEC 27001 e ISO/IEC 27002 per la gestione della sicurezza delle informazioni che fornisce una serie di controlli aggiuntivi e linee guida associate destinati a

36 Cfr: https://cispe.cloud/
37 Cfr: https://www.codeofconduct.cloud/
38 Cfr: https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-172021-draft-decision-french-supervisory_en

soddisfare i requisiti di gestione dei PIMS e delle PII del cloud pubblico per processori e controller, non risolti dal set di controllo ISO/IEC 27002 esistente. La conformità di AWS a questo codice di condotta riconosciuto a livello internazionale, comprovata da una valutazione indipendente di terze parti, dimostra l'impegno di AWS nei confronti della privacy e della protezione dei contenuti dei clienti.
L'allineamento a norme quali ISO 27018 e ISO 27701 dimostra ai clienti che AWS dispone di un efficace sistema di gestione delle informazioni sulla privacy (PIMS) per supportare la conformità al Regolamento generale europeo sulla protezione dei dati (GDPR) e ad altre normative sulla privacy dei dati. L'allineamento di AWS a questi standard, in aggiunta alla valutazione indipendente da parte di terzi di questi codici di condotta riconosciuto a livello internazionale, dimostra l'impegno di AWS per la privacy e la protezione dei contenuti dei clienti e garantisce la conformità alle legislazioni internazionali e locali sulla privacy.

3.5 Il Cyber Resilience Act

Il 15 settembre la Commissione europea ha proposto una serie di regole per assicurarsi che tutti i cosiddetti "dispositivi intelligenti" connessi a Internet (computer, smartphone, televisori, frigoriferi) presenti sul mercato europeo vengano valutati per i loro standard di sicurezza informatica. "In un ambiente connesso", spiega la Commissione[39], "un incidente di cybersecurity in un prodotto può ripercuotersi su un'intera organizzazione o un'intera catena di fornitura, spesso propagandosi attraverso i confini del mercato interno nel giro di pochi minuti. Questo può portare a gravi interruzioni delle attività economiche e sociali o addirittura a rischi per la vita".
Stando alla proposta ancora in discussione al Parlamento UE, nota come Cyber Resilience Act, le società che producono *smart devices* dovranno tenere in considerazione i rischi cyber dei loro prodotti e adottare misure appropriate per risolverne le falle di sicurezza per un periodo di cinque anni; in caso di attacchi, poi, dovranno notificarli all'ENISA entro ventiquattr'ore dalla scoperta. Le imprese che importano e distribuiscono i dispositivi nel territorio dell'Unione, invece, dovranno accertarsi della loro conformità alle regole europee.
Le aziende che non rispetteranno il Cyber Resilience Act rischiano multe fino a 15 milioni di euro, oltre all'imposizione di restrizioni alla vendita – fino al divieto totale – dei loro prodotti nei singoli Paesi membri. Secondo la Commissione, però, le regole permetteranno alle società di risparmiare fino a 290 miliardi di euro all'anno di danni per incidenti informatici, a fronte di costi di adeguamento per 29 miliardi.
"Esistono numerosi esempi di cyberattacchi degni di nota derivanti da una sicurezza non ottimale dei prodotti", spiega la Commissione, "come il worm *ransomware WannaCry*, che ha sfruttato una vulnerabilità di Windows e che nel 2017 ha colpito 200.000 computer in 150 paesi, causando un danno per miliardi di dollari; l'attacco alla

39 Si veda all'indirizzo digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

catena di fornitura Kaseya VSA, che ha utilizzato il software di amministrazione di rete di Kaseya per attaccare oltre 1.000 aziende e costringere una catena di supermercati a chiudere tutti i suoi 500 negozi in Svezia; o i numerosi incidenti in cui le applicazioni bancarie vengono violate per rubare denaro a consumatori ignari".

3.6 Le soluzioni del Gruppo TIM per la sicurezza aziendale

Il Gruppo TIM, leader della digitalizzazione, pone da sempre grande attenzione al tema della cybersecurity avvalendosi di competenze e professionalità specializzate per offrire le soluzioni con il più elevato livello di sicurezza a tutti i propri clienti. Con TIM Enterprise – la nuova business unit dedicata alle imprese, alla Pubblica Amministrazione e ai grandi clienti – offre soluzioni che spaziano dalla connettività ai servizi digitali avanzati come cloud, 5G, Internet delle cose e cybersicurezza presidiati delle aziende del Gruppo, ovvero Noovle, Olivetti e Telsy. La business unit vuole rispondere alle esigenze dei clienti grazie alla propria leadership nei servizi digitali. L'obiettivo è posizionarsi al centro del mercato, sfruttando un approccio sempre più integrato per un'offerta che valorizzerà pienamente l'unicità delle competenze e degli asset del Gruppo, cogliendo anche le opportunità del PNRR, tra cui la realizzazione del Polo Strategico Nazionale.
Nell'ambito della cybersecurity TIM Enterprise sviluppa servizi per proteggere efficacemente l'infrastruttura IT e i dati aziendali e garantire processi operativi aziendali, nel rispetto delle normative in materia di sicurezza delle informazioni, avvalendosi delle competenze dei Security Operation Center (SOC), sempre operativi per la rilevazione di eventi malevoli, la pronta gestione degli incidenti di sicurezza, l'analisi forense post evento.

PSN - Polo Strategico Nazionale

TIM, alla guida di una compagine costituita da Leonardo, Cassa Depositi e Prestiti (CDP, attraverso la controllata CDP Equity) e Sogei, si è aggiudicata la gara per la progettazione, realizzazione e gestione dell'infrastruttura Polo Strategico Nazionale (PSN) per l'erogazione di servizi cloud per la Pubblica Amministrazione. L'iniziativa si inserisce nel piano complessivo di accelerazione della trasformazione digitale dell'Italia, a garanzia della sicurezza e dell'affidabilità dei dati e per fornire servizi innovativi a cittadini e imprese, come previsto dal PNRR (Piano Nazionale di Ripresa e Resilienza) e dagli interventi normativi in materia di infrastrutture digitali.

I servizi

Tra i Managed Security Services, TIM Enterprise mette a disposizione dei clienti personale qualificato per supportarli lungo l'intera esperienza d'uso, a partire dall'assessment del rischio informatico, dalla definizione dei piani di sicurezza e delle attività di Security Compliance fino a quelle periodiche di Security Audit, mirati al monitoraggio continuo

del mantenimento di adeguati livelli di sicurezza per la protezione del business aziendale. Con le Network Security Solutions offre, invece, tecnologie in grado di prevenire e gestire rischi informatici.
In particolare, le soluzioni DDoS Protection bloccano, direttamente a monte della rete cliente, attacchi hacker massivi; i Next Generation Firewall impediscono tentativi di intrusione implementando policy di sicurezza; il DNS Sicuro inibisce la navigazione su siti malevoli ai dipendenti dell'azienda; i dispositivi di Network Detection & Response (NDR) monitorano flussi di traffico anomalo e tentativi di esfiltrazione di dati coadiuvati da algoritmi di intelligenza artificiale e, infine, le soluzioni di protezione delle reti aziendali consentono di interagire principalmente con le macchine (Operational Technology, OT) per impedire attacchi ai dispositivi industriali e ai sensori dispiegati dal cliente (Internet of Things). La digitalizzazione delle imprese ha favorito la crescente adozione delle applicazioni cloud basate su architetture ibride, collocate in cloud privati e pubblici, come nel caso di dipendenti che accedono alla rete aziendale in smart working o in mobilità con personal computer e smartphone. Scenari in cui TIM Enterprise garantisce il più elevato livello di sicurezza combinando soluzioni avanzate di networking che consentono di verificare l'identità digitale con strumenti di autenticazione multi-fattore e analisi del contesto e del comportamento dell'utente oppure di proteggere le applicazioni in cloud.
TIM Enterprise rende inoltre disponibili protocolli di sicurezza tra reti, inoltre protocolli di sicurezza tra reti, provider di servizi cloud e utenti finali (Cloud Access Service Broker), servizi di Remote Browser per abilitare le sessioni di navigazione web degli utenti su server remoto, oltre a soluzioni che impediscono di fornire informazioni sensibili al di fuori della rete aziendale (Data Loss Prevention), o che proteggono le applicazioni web dai rischi legati al traffico Internet indesiderato (Web Application Firewall). Sono inclusi servizi che consentono di eseguire il backup dei dati e dell'infrastruttura IT in ambiente cloud (Cloud Disaster recovery) e di Endpoint Protection per la gestione della sicurezza degli apparati di rete o singoli device da cui si accede alla rete.
Con la soluzione TIM myBroker infine, le aziende possono dotarsi di un'assicurazione sui rischi cyber grazie ad una polizza contro i danni subiti in caso di attacco.

Soluzioni di TIM per la sicurezza informatica delle PMI e delle partite IVA
TIM offre a tutte le partite IVA e piccole e medie imprese della propria clientela soluzioni di connettività fissa e mobile che vengono arricchite anche da un servizio di navigazione sicura che, attraverso funzionalità di anti-phishing e di *malware containment* direttamente integrate nella rete TIM, non necessita di alcuna installazione software sui dispositivi degli utenti. Sono disponibili inoltre soluzioni antivirus pronte all'uso e facili da installare, per difendere computer, laptop e server con i diversi sistemi operativi che completano l'offerta base.

Completa il quadro delle soluzioni pensate per le realtà più piccole anche un utile servizio di supporto professionale che in caso di incidente informatico, garantisce entro 4 ore il supporto telefonico da remoto a cura di un esperto informatico per affrontare il problema con la massima efficacia.
Una protezione più sofisticata di sicurezza perimetrale si attua con i firewall di nuova generazione di TIM nonché attraverso le soluzioni di Security Information and Event Management, che offrono una console centralizzata per la gestione dei dati di log e degli eventi di sicurezza delle diverse piattaforme impiegate all'interno dell'azienda, gestibile in autonomia dal cliente o con il supporto esterno di uno Smart SOC.
Le soluzioni di sicurezza informatica di TIM per le medie imprese comprendono inoltre servizi professionali di rilevazione e analisi delle vulnerabilità dei sistemi (penetration test e vulnerability), realizzati attraverso simulazioni di hacking e metodologie riconosciute a livello internazionale applicate dal personale specializzato dei Security Operation Center di TIM. Tali servizi proteggono i clienti dai potenziali attacchi, grazie a criteri sofisticati di controllo e filtraggio dati che si avvalgono di Big Data Analytics e delle tecniche di Data Science, oltre che di una consulenza specialistica finalizzata a mettere a punto un adeguato modello di governance.
A queste si aggiungono le soluzioni di disaster recovery e business continuity, che garantiscono la conservazione delle copie dei dati aziendali sul cloud di TIM in conformità alle policy di backup dell'azienda, oltre al ripristino immediato di dati e infrastrutture informatiche in caso di problemi. In questo modo è possibile continuare a erogare i servizi nel rispetto dei requisiti richiesti (Service Level Agreement), ricorrendo anche a siti alternativi dove poter trasferire temporaneamente il proprio ambiente operativo e per minimizzare i disagi in caso di fermi applicativi.

Telsy

Telsy – società del Gruppo TIM che opera nell'ambito della nuova Business Unit TIM Enterprise – è attiva da oltre cinquant'anni nel settore della sicurezza delle comunicazioni e della cybersecurity, con soluzioni rivolte alle amministrazioni governative e alle realtà private in Italia ed all'estero. Fornisce sistemi di sicurezza basate su tecnologie proprietarie di crittografia, capacità e competenze di system integration, oltre all'analisi del rischio cyber, all'implementazione e governance di soluzioni di protezione, al monitoraggio di infrastrutture e capacità di risposta agli attacchi.
Dispone di un Security Operation Center, di un gruppo dedicato alla Cyber Threat Intelligence e di un Incident Response Team. È attiva, inoltre, nei settori della Decision Intelligence e della Quantum Security con team di ricerca e sviluppo, piattaforme e soluzioni proprietarie, e con partecipazione nell'azienda QTI srl, specializzata nella Quantum Key Distribution (QKD).

Le soluzioni crittografiche

Queste soluzioni proteggono comunicazioni e dati da minacce in continua evoluzione attraverso tecnologie, algoritmi e protocolli sviluppate in-house. In particolare, il portfolio Crypto comprende i prodotti Crypto Voice per mettere in sicurezza il traffico telefonico VoIP, Encryptors (cifranti) per il trasferimento sicuro di dati critici, applicativi di videoconferenze sicure che utilizzano protocolli di crittografia asimmetrica per autenticare i partecipanti nelle riunioni virtuali di lavoro e dispositivi ultrasonici in grado di inibire registrazioni audio involontarie da parte di app dannose installate nei dispositivi mobili.

Le soluzioni di cybersecurity

Nell'ambito dei Managed Detection and Response Services, Telsy offre software, sistemi e servizi integrati per gestire direttamente e nelle sedi aziendali il proprio perimetro di sicurezza cyber.

I Cyber Professional Services sono invece soluzioni per la difesa preventiva che includono le attività di Vulnerability Assessment e Penetration Test e consentono di presidiare il perimetro di sicurezza cyber di aziende e organizzazioni anche attraverso percorsi di formazione per la sensibilizzazione del personale sulle principali tematiche di sicurezza informatica.

Nell'ambito dei Managed Security Services, Telsy offre inoltre servizi di Network Security, Application Security ed Endpoint Security per la sicurezza di applicazioni cloud, dispositivi IoT, mobili e firmware.

TelsyOlimpo è, inoltre, la piattaforma di decision intelligence utilizzata dagli analisti Telsy per effettuare un continuo monitoraggio di big data e fornire report utili per i decision maker e per la sicurezza di personaggi (pubblici e privati) particolarmente esposti.

Infine, grazie all'investimento strategico nel capitale sociale di QTI, azienda leader nel campo delle comunicazioni quantistiche, Telsy opera in primo piano anche sul fronte della Quantum Security, con soluzioni di sicurezza che sfruttano i principi della meccanica quantistica e rendono impossibili gli attacchi da computer classici e quantistici, anche grazie a sofisticati algoritmi di cifratura post-quantum.

4.1 Il caso delle microimprese

Con "microimpresa" si definisce un'azienda con meno di dieci impiegati e un fatturato annuo non superiore ai 2 milioni di euro. Le microimprese ricevono solitamente molte meno attenzioni (e finanziamenti) rispetto alle PMI, specie in materia di cybersicurezza. Sprovviste spesso sia di competenze settoriali sia di linee guida specifiche a cui rifarsi, finiscono allora per trascurare del tutto il tema oppure per affidarsi (*outsourcing*) ad altre microimprese, che però potrebbero a loro volta non disporre delle soluzioni più aggiornate per contrastare i criminali informatici.

Le microimprese sono però particolarmente esposte al rischio cibernetico. Per i criminali informatici, specialmente se "micro" anch'essi (soggetti singoli, e non grosse organizzazioni internazionali), è infatti conveniente attaccare una microimpresa, per diverse ragioni[40]. Innanzitutto perché l'evoluzione tecnologica permette una maggiore automazione degli attacchi verso bersagli specifici (target): utilizzando strumenti di intelligenza artificiale, ad esempio, è possibile automatizzare le campagne di *social engineering* e di *spear phishing*. Queste offensive, poi, non incontrano difese solide, anzi: un sondaggio di PurpleSec ha rivelato che il 70 per cento delle microimprese è impreparato a rispondere a un attacco informatico. Tre microimprese su quattro non dispongono di personale dedicato alla cybersicurezza, e oltre la metà non assegna alcun budget alla sicurezza informatica.

Rispetto alle PMI, l'esposizione delle microimprese alle minacce cibernetiche è maggiore non soltanto per via delle minori risorse impiegabili nella difesa, ma anche per i loro stessi metodi lavorativi: esternalizzando alcune fasi del processo produttivo o gli interi processi di supporto a partner terzi, infatti, vedono aumentare il rischio di violazione dei dati. Dati peraltro di grande valore, come i brevetti. Le microimprese, infine, tendono a pagare i riscatti con relativa facilità per timore di essere costrette a chiudere le loro attività.

La vulnerabilità delle microimprese agli attacchi di *social engineering*, in particolare, è elevata perché il numero di dipendenti "chiave" – in possesso, cioè, di informazioni sensibili – è ridotto e la preparazione media sui pericoli informatici è spesso scarsa. Più complessi, per i cybercriminali, possono essere gli attacchi di *phishing*: una microimpresa si interfaccia con un pubblico ridotto di fornitori e clienti, e i messaggi-truffa devono dunque essere ben contestualizzati. Tuttavia, l'evoluzione delle tecniche di Open Source Intelligence (la ricerca di informazioni d'interesse da fonti aperte, ad esempio su Internet: si abbrevia in OSINT) e l'automazione delle offensive cyber avvantaggiano l'attaccante, riducendone l'impegno diretto. Il gran numero di informazioni reperibili in rete tramite OSINT permette infatti al criminale di impersonare, ad esempio, un for-

---

40 Frumento E., Cyber security nelle microimprese: perché è un problema e come mitigarlo, su Cybersecurity360, *28/07/2022*

nitore di una microimpresa, alla quale invierà una e-mail descrivendo un problema di consegna e chiedendo la conferma di informazioni riservate (indirizzi o dettagli bancari). Grazie all'automazione, questi processi possono essere facilmente replicati su larga scala.

Dall'altro lato dello schermo troviamo i dipendenti delle microimprese, che spesso lavorano con i propri dispositivi personali, un fatto che aumenta la loro esposizione a rischi come la perdita di dati e l'installazione di app malevole. Alle carenze tecniche si accompagna un'attenzione generalmente bassa alle minacce online: di norma le microimprese sottovalutano il rischio cibernetico perché si considerano troppo piccole per venire bersagliate, oppure perché pensano che i loro business non siano interessanti per i criminali informatici. Non è così, anche perché le microimprese costituiscono spesso il primo anello di una lunga catena di approvvigionamento (*supply chain*) che può portare fino a società di grandi dimensioni: attaccando una microimpresa, dunque, i cybercriminali potrebbero riuscire a risalire l'intera filiera.

Un attacco informatico può avere ripercussioni gravissime su una microimpresa: se colpita da un *ransomware* e forzata a interrompere le attività, per esempio, potrebbe andare incontro al fallimento, anche come conseguenza di un riscatto troppo alto. Una ditta che si vedesse sottratti i dati personali di clienti e collaboratori, poi, finirebbe col dover pagare pesanti sanzioni amministrative, oltre a subire un danno reputazionale potenzialmente devastante per i suoi affari. Un'altra conseguenza può essere la perdita di proprietà intellettuali.

5.1 La carenza di esperti

Secondo l'Agenzia per la cybersicurezza nazionale, in Italia mancano centomila esperti di sicurezza informatica. Il problema non è solo italiano, ma europeo e globale. In un rapporto pubblicato a novembre 2021[41], l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) scriveva infatti che "nel mercato del lavoro c'è carenza di personale qualificato per svolgere ruoli di sicurezza informatica e in grado di affrontare in maniera sufficiente la gamma di minacce informatiche poste. Nel corso degli anni, questo è diventato un problema ben documentato, che continua ad avere un impatto significativo sui Paesi in Europa e nel mondo. All'interno dei Paesi e dei settori specifici, questi problemi sono ancora più pronunciati a causa della forte concorrenza per i professionisti della sicurezza, il che spesso significa che alcuni settori (per esempio i governi e le banche centrali) hanno difficoltà ad attrarre professionisti della sicurezza di talento rispetto ad altri (come l'industria finanziaria) che possono offrire un lavoro più redditizio". Allargando ancora di più lo sguardo, il *2022 Cybersecurity Skills Gap – Global Research Report* di Fortinet ha messo in evidenza come, a livello mondiale, il 60 per cento delle aziende che cerca personale qualificato nel campo della cybersicurezza ha difficoltà a riempire le posizioni: i ruoli in questo senso più critici sono i Cloud Security Specialist e i Security Operations Analyst.

A giugno 2022 il sito *Guerre di Rete* ha pubblicato[42] i risultati di un'indagine sullo stato della sicurezza informatica nelle aziende medio-grandi d'Italia, intervistando cinquantuno professionisti del settore. Il 66 per cento di questi ha dichiarato che nella propria azienda la cybersecurity occupa un ruolo centrale ed è adeguatamente finanziata; il 24 per cento racconta invece dell'esistenza di solo un piccolo gruppo di esperti; il 10 per cento, infine, dice che non esiste alcun team interno dedicato al tema.

Il 40,5 per cento degli intervistati afferma che la propria azienda ha aperto nell'ultimo anno dalle due alle cinque posizioni per ruoli legati alla cybersicurezza; il 21,4 per cento parla di sei-dieci posizioni aperte e il 19 per cento di oltre dieci. L'88,1 per cento parla di difficoltà nella selezione dei candidati perché – nel 35,3 per cento dei casi – le candidature sono state troppo scarse. Per il 17,6 per cento degli intervistati, invece, i candidati non disponevano di sufficiente esperienza nel campo; per il 47 per cento i candidati non erano in possesso delle competenze richieste. L'88,1 per cento dei soggetti intervistati segnala che la propria azienda prevede dei corsi di potenziamento delle competenze di cybersecurity per i nuovi assunti.

Stando all'ENISA[43], ci sono 125 programmi di istruzione superiore in venticinque Paesi europei che rispondono ai requisiti dell'agenzia per la formazione sulla cybersicurezza. In Italia sono diciassette, principalmente master: ce ne sono al Politecnico di Milano

41 ENISA, Addressing Skills Shortage and Gap Through Higher Education, 24/11/2021
42 Stefanello V., Cybersicurezza in Italia: perché non si trovano candidati?, su Guerre di Rete, *16/06/2022*
43 Si veda all'indirizzo enisa.europa.eu/topics/cybersecurity-education/cyberhead#/

(*Computer Engineering*), all'Università Bocconi (*Cyber Risk Strategy and Governance*), all'Università di Torino (*Cybersecurity*), all'Università di Pisa (*Cybersecurity*), all'Università di Perugia (*Cybersecurity*), all'Università degli Studi di Bari Aldo Moro (*Sicurezza informatica*), all'Università di Cagliari (*Computer Engineering, Cybersecurity and Artificial Intelligence*) e alla Sapienza Università di Roma (*Cybersecurity*), tra gli altri. I corsi di laurea triennale sono invece due: quello in *Sicurezza dei sistemi e delle reti* all'Università degli Studi di Milano e quello in *Diplomatic, International and Global Security Studies* all'Università del Salento. Il Laboratorio nazionale di cybersicurezza del CINI (Consorzio interuniversitario nazionale per l'informatica) patrocina[44] otto master di primo livello, quattro master di secondo livello, tre dottorati di ricerca, venti lauree magistrali e due lauree triennali.

Tuttavia, solo il 30 per cento dei professionisti intervistati da *Guerre di Rete* ha detto che la propria azienda svolge attività di ricerca talenti (*scouting*) già negli istituti tecnici; il 60 per cento ha affermato però che la propria azienda dispone di uno o più atenei di riferimento per la ricerca di candidati.

5.2 La sfida nell'attrarre i talenti: il differenziale retributivo tra Italia e Paesi leader in cybersecurity

Accanto all'evidente carenza di talenti e al divario tra preparazione universitaria (formazione teorica) e necessità aziendali (competenze pratiche), le imprese d'Italia fanno fatica ad attirare, ma soprattutto a mantenere professionisti in cybersicurezza anche per via della remunerazione mediamente più bassa rispetto all'estero: gli esperti italiani, dunque, decidono spesso di trasferirsi altrove; quelli stranieri, invece, non considerano il nostro Paese una meta attraente.

Secondo Economic Research Institute[45], la retribuzione lorda media di un Cybersecurity Specialist in Italia si aggira attorno ai 66.000 euro nel 2021, un valore molto inferiore rispetto a quelli che si possono percepire nei Paesi che rappresentano degli attrattori di talenti in ambito cybersecurity: in Svizzera, Lussemburgo, Stati Uniti e Regno Unito, in particolare nella zona di Londra, lo stesso profilo professionale ottiene una remunerazione media che oscilla tra i 105 ed i 109mila euro.

Il Centro Studi TIM ha esaminato come varia il differenziale salariale comparando le retribuzioni nette adeguate al costo della vita. I due effetti vanno in una direzione opposta: mentre il cuneo fiscale (rapporto tra l'ammontare di tassi e contributi che gravano sulla retribuzione del lavoratore e il corrispondente costo totale sostenuto dal datore di lavoro) è mediamente più elevato in Italia rispetto agli altri Paesi, il costo della vita tende ad essere più basso nel nostro Paese. Tuttavia, nonostante tutto, si conferma un differenziale considerevole: in Italia un Cybersecurity Specialist percepisce intorno ai 40mila euro, ovvero una retribuzione netta che in termini reali risulta del 50% inferiore

44 Si veda all'indirizzo cybersecnatlab.it/formazione-in-cybersecurity/
45 https://www.erieri.com/

rispetto a quella dei 4 Paesi considerati come *benchmark*. Il costo sostenuto per la retribuzione di un singolo esperto di cybersecurity che un'impresa italiana dovrebbe affrontare per poter essere competitiva e pareggiare l'offerta, ad esempio, di una società inglese, dovrebbe aumentare di 1,5 volte.
Letto in un altro modo, quanto appena detto significa che, a parità di budget, se un'azienda italiana avesse bisogno di 150 Cybersecurity Specialist, al prezzo del Regno Unito potrebbe riuscirne ad assumerne solo 100.
Il problema non riguarda solo il settore privato. Anche l'Agenzia per la cybersicurezza nazionale ha problemi a trovare candidati: si è data l'obiettivo di assumere trecento persone entro la fine del 2023 e ottocento entro il 2028 – molte meno sia dell'ente equivalente francese (1100 persone) sia di quello tedesco (1200) –, ma il bando sta "andando deserto, tanto da costringere l'agenzia a rivolgersi a un apposito team di recruiting", scriveva *Wired*[46]. Alcune fonti hanno rivelato al giornale che tra i motivi della ridotta partecipazione c'è la bassa retribuzione offerta. Da bando, la retribuzione annua lorda prevista per i nuovi assunti è di 50.000 euro, ovvero la metà degli stipendi pagati dalle multinazionali dell'informatica per le stesse figure professionali, stando a un'indagine del Politecnico di Milano[47].

46 Cruciata G., Cosa ha fatto finora l'Agenzia per la cybersicurezza nazionale, su Wired*, 11/05/2022*
47 Si veda all'indirizzo thefutureofmanagement.mip.polimi.it/cybersecurity/responsabile-sicurezza-informatica-fino-a-quanto-guadagna-un-esperto/

innovative publishing

www.startmag.it
www.innovativepublishing.it