CYBERSECURITY NEL POST-PANDEMIA

MAG ne parla con Stefano Mele, socio dello studio Gianni & Origoni. «La cybersecurity è sempre più un tema all'attenzione dei board e non solo un argomento relegato agli informatici»

di giuseppe salemme

Non bastavano di certo "coronavirus", "tampone", "lockdown" e "droplets". Tra le parole entrate nel nostro lessico quotidiano in questi mesi ci sono anche termini come "ransomware" e "data breach". Proprio a conferma del fatto che i mali (e gli inglesismi) non arrivano mai da soli.
Non che ognuna di queste parole non esistesse da ben prima dell'emergenza sanitaria. Ma, com'era forse inevitabile, l'improvviso digitalizzarsi delle nostre vite private e lavorative ha rappresentato per i criminali informatici il fatidico terno al lotto. Con tanto di premio in denaro. Arriverebbero addirittura a 5,2 miliardi di dollari i profitti (rigorosamente in bitcoin) da attacchi ransomware nei primi sei mesi del 2021: lo sostiene un'analisi del Financial Crimes Enforcement Network statunitense.
Uno scenario inquietante, con un possibile, piccolo, lato positivo: ogni persona, azienda e amministrazione ha dovuto infine fare i conti con il tema della cyber-sicurezza in maniera seria.
L'avvocato **Stefano Mele**, partner e global head del dipartimento cybersecurity dello studio Gianni & Origoni, ironizza: «Ha fatto di più l'ondata di ransomware che anni e anni di convegni sulla sicurezza». L'avvocato è infatti da anni in prima linea non solo nell'assistenza a soggetti pubblici e privati in materia di diritto delle tecnologie e cybersecurity, ma anche in una difficile opera di divulgazione e awareness sull'importanza che questi temi diventino una priorità per aziende e istituzioni. In Gop dallo scorso aprile, Mele sta ora introducendo un approccio multidipartimentale al tema della sicurezza informatica, con un'offerta che mira ad assistere le aziende dalla prevenzione fino ai momenti "caldi" di un cyber-attacco. Ma andiamo con ordine.

L'avvocato Mele, dalla sua finestra Zoom, racconta a MAG i modi in cui la pandemia ha posto in evidenza le criticità di sicurezza dei nostri device: «L'esigenza di trasferire in un brevissimo lasso di tempo tutto il lavoro dagli uffici alle abitazioni dei lavoratori ha fatto emergere con forza tutta una serie di mancanze organizzative e di vulnerabilità. Quando siamo al lavoro ci sono protocolli e team di security che proteggono le reti e i sistemi informatici, che mancano, invece, se si lavora da remoto, connettendosi alle reti aziendali da dispositivi personali, non allineati agli standard di sicurezza e magari utilizzati da più soggetti all'interno dello stesso nucleo familiare».
Si possono innescare in questi casi situazioni molto pericolose, «perché la maggior parte delle misure di cybersecurity sono mirate a proteggere da attacchi provenienti dall'esterno. Tuttavia, quando viene infettato un PC o un dispositivo personale con accesso alla rete aziendale, questo può essere usato come base per attaccare dall'interno i dati di valore presenti nei sistemi informatici principali». Come spiega Mele, si parla in questi casi di «attacchi attraverso movimenti orizzontali».

Un piccolo segnale positivo, come testimonia l'avvocato, è dato dall'aumento nelle aziende della consapevolezza dell'importanza di proteggere le informazioni digitalizzate e di dotarsi di infrastrutture informatiche sempre più sicure: «La cybersecurity è sempre più un tema all'attenzione dei board e non più solo un argomento relegato agli informatici e agli esperti di sicurezza. Si comprende sempre di più – finalmente – che le informazioni hanno un preciso valore economico per il business e che la mancanza di politiche reali di cybersecurity può avere una ricaduta sull'operatività aziendale, sugli investimenti, sulla reputazione, sulle responsabilità normative dettate dal legislatore europeo e nazionale» spiega l'avvocato. Che però precisa: «Se le grandi aziende stanno investendo sempre di più in questo settore, anche a seguito degli obblighi discendenti da importantissimi impianti normativi come la direttiva NIS e il Perimetro di Sicurezza Nazionale Cibernetica (si veda il box), discorso diverso deve essere effettuato per le pmi, che mancano spesso di cultura e sensibilità ai temi della sicurezza, anche per una minore capacità di investimenti specifici nel settore». Il discorso, purtroppo, è il medesimo anche nel settore pubblico: «È un tema oramai noto: lo stesso ministro Vittorio Colao ha affermato che il 95% dei server della PA non è sicuro», ricorda Mele. Considerate queste percentuali, si salvano solo i sistemi informatici dei servizi segreti. O almeno questo è l'auspicio.
Parliamo, dunque, di un problema universale. Ma

esistono modi per tentare di risolverlo? Non resta che incrementare il più possibile la consapevolezza dello scenario, la cultura aziendale nel settore della cybersecurity e ovviamente le difese, organizzando la governance aziendale e le infrastrutture tecnologiche in modo da riuscire a rispondere prontamente a questo genere di criticità. «Tutto ciò, però, non sta ancora avvenendo come ci si aspetterebbe. Non è un caso che, durante i mesi estivi abbiamo registrato un'impennata nelle richieste di supporto legale da parte di numerosissimi clienti alle prese con cyber-attacchi, che sono aumentati non solo quantitativamente, ma soprattutto qualitativamente», racconta Mele. «Riceviamo mediamente un mandato ogni due giorni da aziende sotto attacco. I ransomware, in particolare, stanno creando vere e proprie situazioni di "crisi cibernetica" nelle nostre aziende, spesso bloccandone completamente l'operatività».
In questo scenario, diventa essenziale il fattore tempo, «non solo per bloccare l'attacco informatico, ma anche e soprattutto per la ripresa delle attività e per gestire tutti gli adempimenti legali conseguenti, che sono sempre di più e richiedono una vera e propria regia esterna a supporto del board, del legal e della security aziendale».

È questa, in sintesi, l'offerta di Gop in fatto di cybersecurity: un supporto interdipartimentale mirato a gestire queste situazioni di crisi e le questioni che pongono. Ad esempio, sul pagare o meno un riscatto, quali profili di responsabilità potrebbero emergere? Cosa dicono i contratti assicurativi? Ci sono obblighi informativi? E la 231? «Il nostro intervento ha ovviamente un approccio proattivo, strutturando in primis a disegnare o rafforzare i processi, le difese, a verificare quanto di buono è stato fatto nelle attività di compliance. Dobbiamo aiutare a fronteggiare delle vere e proprie organizzazioni criminali internazionali, non dei "ragazzini" che si improvvisano. Una volta si usava dire che il mondo è diviso in chi ha subito un attacco e chi lo subirà, ma oggi la situazione è ancora peggiore: ciò che vediamo, nei fatti, è che la distinzione è tra chi ha subito l'attacco e se n'è accorto e chi l'ha subito e ancora non lo sa», avverte Mele. Ciò spiega anche il modus operandi che da sempre orienta il suo lavoro: «Credo che per questo settore la chiave sia quella di essere equamente vicini sia al "cervello" che al "cuore" dell'azienda: parlare, quindi, sicuramente al general counsel e al legal, ma anche al board e alla security. La sicurezza è un lavoro di squadra, che impegna tutti conclude Mele.

CHE COSA SONO?

RANSOMWARE

Programma informatico malevolo che limita o blocca l'accesso a un dispositivo o a un insieme di dati richiedendo un riscatto (ransom) per rimuovere la limitazione. Tra gli attacchi di tipo ransomware figura anche quello che, all'inizio di agosto, ha bloccato l'infrastruttura informatica della campagna vaccinale della Regione Lazio, nonché quello subito dalla Siae pochi giorni fa.

DIRETTIVA NIS (NETWORK AND INFORMATION SECURITY)

Direttiva UE 2016/1148 sulla sicurezza delle reti e dei sistemi informativi, recepita nel nostro ordinamento attraverso il decreto legislativo 18 maggio 2018, n. 65, in vigore dal 24 giugno 2018.

PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

Quadro normativo di sicurezza nazionale mirato a consentire di monitorare e gestire il rischio di cyberattacchi in Italia. Coinvolge tutti i soggetti che esercitano una funzione essenziale dello Stato o che prestano servizi essenziali la cui compromissione creerebbe un serio problema per la sicurezza nazionale. È stato definito sulla base del d.l. 105/2019, a cui è stata data attuazione per mezzo di cinque Dpcm attuativi, tra l'ottobre 2020 e il marzo 2021.