ItaliaOggi Sette
diffusione:88589
tiratura:133263

La pandemia ha fatto crescere i reati informatici: a giugno 2020 aumentati di oltre il 250%

Cybercrime, allarme nelle aziende per gli attacchi degli hacker

Pagine a cura
DI ANTONIO RANALLI

Crescono gli attacchi informatici ai danni delle aziende. Aumentano malware e iniziative in grado di mettere in pericolo dati sensibili e la sicurezza informatica. Una crescita che si è registrata soprattutto in seguito al lockdown, che ha portato sempre più persone a lavorare in casa e le aziende ad attrezzarsi di conseguenza per avere maggiori servizi informatici. La necessità di percepire il rischio informatico come un pericolo concreto sul quale le aziende devono intervenire con urgenza primaria è stata messa in evidenza da un recente studio dell'Osservatorio del Politecnico di Milano. Secondo la ricerca condotta sui dati relativi all'anno 2019, le imprese italiane hanno subito una media di 139 violazioni informatiche al mese, registrando un aumento di quasi il 50% rispetto agli attacchi perpetrati tra il 2014 e il 2018. Secondo il rapporto Clusit, nel corso dell'ultimo anno, sono stati effettuati 1.670 attacchi informatici, il +7,6% in più rispetto al 2018 con un aumento del 91.2% in confronti ai dati del 2014. Dal rapporto emerge chiaramente come le attività di Cybercrime e di Cyber espionage siano in netta crescita, segnando un aumento pari a +12,3% e +0,5%.

Ivan Rotunno

«Dati già di per sé allarmanti che con l'arrivo della pandemia hanno subito una crescita esponenziale, indicando - nel mese di giugno 2020 - un aumento di oltre il 250% dei reati informatici ai danni delle imprese», dice **Ivan Rotunno** di ***Orrick***. «Gli strumenti maggiormente utilizzati dagli hacker hanno riguardato le campagne di malware a tema Covid-19 e l'utilizzo di spam e phishing sul Coronavirus. In periodo di smartworking, gli hacker hanno puntato per lo più sui lavoratori e sull'assenza di presidi tecnici adeguati ad arginare gli attacchi ai sistemi It delle imprese. La capacità di resistere a un attacco informatico – cyber resilienza – richiede che un'impresa adotti un approccio multidisciplinare che guardi alla sicurezza informatica, alla possibilità di garantire un sistema di business continuity e che tenga conto della preparazione delle funzioni e delle risorse interne, per rispondere positivamente in caso di violazioni».

Dati preoccupanti sono arrivati anche dal recente Salone della Giustizia, che si è tenuto a Roma dal 29 settembre al 1 ottobre, «La pandemia ha aumentato la superficie degli attacchi informatici, a causa del maggiore uso dell'online, che ha reso la vita reale tradotta in maniera esponenziale in dati digitali (onlife)», spiega **Barbara Pontecorvo**, partner di ***Tonucci & Partners***, «la sfida del Paese è di aumentare la digitalizzazione, ma anche di investire contemporaneamente in sicurezza. Oggi è quanto mai necessario per le aziende che rivolgono richieste di assistenza, anche in via preventiva e non solo dopo aver subito un attacco, avvalersi di servizi di consulenza su tutti gli aspetti in materia di protezione dei dati e sistemi di sicurezza. Gli ambiti nei quali si svolge l'attività legale in materia di sicurezza sono molteplici, partendo dall'elaborazione e attuazione del D.lgs. 231/2001, anche riguardo agli adempimenti normativi in tema di sicurezza informatica. La consulenza che offriamo contempla un'ampia gamma di questioni complesse relative alla protezione dei Dati e Cybersecurity, quali a titolo esemplificativo, la predisposizione, la formazione e l'aggiornamento delle politiche e delle procedure legate alla Privacy, in conformità al Gdpr, l'assistenza ed il supporto (anche ai responsabili interni alle aziende) alla protezione dei dati personali e alla gestione del rischio informatico, in tutti e più vari contesti aziendali e commerciali, inclusi i servizi resi via internet, su cloud, via social media e call center, con particolare attenzione alle peculiarità di ogni servizio sul quale si concentra la nostra consulenza».

Barbara Pontecorvo

Tra gli effetti dirompenti cagionati dal Covid-19, vi è stato anche il vertiginoso aumento degli episodi di Cybercrime. «Come è stato riferito dalla Direzione della Polizia Postale», afferma **Andrea Puccio**, managing partner di ***Puccio Penalisti Associati***, «la pandemia avrebbe allargato la superficie d'attacco, «visto che quello che non potevamo fare fisicamente lo facevamo online, dal lavoro, agli acquisti, alla sanità», con conseguente aumento esponenziale dei reati di natura informatica. Nel periodo di riferimento – ad esempio – 28 grandi società sono state vittime di frodi informatiche (per un totale di circa 25 milioni di euro), mentre le email «fake ceo» (finte comunicazioni di posta elettronica che sembrano provenire da soggetti apicali) sono aumentate del 378% come ha detto recentemente in un convegno a Roma Nunzia Ciardi, direttore della Polizia Postale e delle comunicazioni. Infatti, a differenza delle società straniere, le organizzazioni italiane, composte perlopiù da piccolemedio imprese restie all'innovazione tecnologica, hanno dovuto accelerare in poche settimane il percorso digitale, senza tuttavia gestire in modo adeguato i rischi connessi ai sistemi informatici. Negli ultimi mesi, in considerazione di quanto sopra, abbiamo supportato numerose imprese nella gestione di svariate condotte illecite in ambito Cybercrime, poste in essere ai propri danni da parte di organizzazioni criminali».

Andrea Puccio

Secondo un recente report dell'*European Cyber Security Organization* condotto su 340 stakeholders, il 34% degli intervistati percepisce «l'aumento delle frodi, dei cyber crimini e dei cyber attacchi» come la più grave minaccia aziendale derivante dal Covid-19. Un'altra ricerca ha inoltre riscontrato un aumento del 30% dei cyber attacchi in alcuni settori come nel Finance e Food Products. «Quello che osserviamo è che le aziende si stanno orientando sempre più nel cercare di prevenire gli attacchi informatici sviluppando non solo un'infrastruttura IT solida, ma anche dei processi e delle best practices comportamentali aziendali per la sicurezza informatica», prosegue **Daniele Caneva**, partner e responsabile del dipartimento Ip di ***EY***, «A livello europeo, il recente *Cybersecurity Act* (Reg. EU 2019/881) viene incontro alle imprese realizzando il principio della cosiddetta «security by design» (ovvero la sicurezza dei prodotti e servizi Ict sin dalla loro progettazione). In particolare, il Regolamento amplia i poteri dell'Enisa (*European Network Information Security Agency*) che fornirà consulenza tecnica agli Stati membri per elaborare politiche in materia di sicurezza informatica e per prevenire incidenti informatici. Inoltre, il Cybersecurity Act introduce un quadro di regole uniformi per la certificazione della sicurezza informatica di prodotti, servizi e processi. Lo schema di certificazione Ue sarà presto operativo e andrà a sostituire le attuali certificazioni nazionali».

Daniele Caneva

Security Strategy, Governance e Compliance, sono i settori di riferimento o nella gestione dei rischi cyber. «In questo momento le aziende hanno fatto un massiccio ricorso all'attività dello smart working», prosegue **Iacopo Destri**, partner dello studio legale internazionale ***C-Lex*** di Milano, «Soprattutto nel mondo dei servizi e nella gestione dei lavoratori e della delivery dei servizi tipici. In questo settore si apre una potenziale falla della sicurezza delle aziende. I lavoratori nella prima fase della pandemia si sono ritrovati a lavorare da casa con strumenti propri o con strumenti non del tutto pronti per questo tipo di lavoro da remoto. Per cui l'elemento di criticità che le aziende hanno cercato di affrontare è stato quello di comprare strumenti informatici. Dopodiché l'ulteriore elemento di criticità rilevante è l'utilizzo della rete. Quello che abbiamo notato è che molte aziende hanno adottato degli strumenti informativi, che hanno il vantaggio di andare a gestire la sicurezza rispetto a eventuali attacchi informatici».

Iacopo Destri

I maggiori rischi per la sicurezza informatica continuano ad essere gli attacchi dall'esterno, quindi email e app legate a internet. «I virus veicolati con email eludono sempre più frequentemente le misure di sicurezza tradizionali», afferma **Francesco Sciaudone**, managing partner di ***Grimaldi Studio Legale***, «anche le applicazioni SaaS (*Software as a service*), sono un rischio sempre maggiore che invitano i cybercriminal a veicolare i propri virus tramite le applicazioni web messe a disposizione dei clienti direttamente via Internet; Le app in cloud non risolvono il problema, anzi spesso la protezione del sistema di hosting in cloud non è adeguata al rischio e rimane vulnerabile anche ad attacchi c.d. di brute force, attacchi che guadagnano l'accesso a un account autorizzato per craccare dati criptati e rubare informazioni per scopi di frode; Rischi anche dalle Intercettazione delle conversazioni e contraffazione della voce delle persone i cui tool sono abbastanza utilizzati dal sistema di banche online per autenticare gli utenti e autorizzare funzioni dispositive. Anche la distribuzione di malware e ransomware è sempre frequente e il rischio di perdita di dati in detti casi è molto elevato. In ogni caso contrastare le minacce interne (del personale interno) è ancora una delle maggiori sfide. A fronte di detti rischi, è importante che i responsabili della security si concentrino sul modo di integrare la sicurezza nella cultura aziendale anche perché ogni anno gli ambienti tecnologici si complicano, si diffonde la rete 5g che permetterà connessioni rapidissime».

Francesco Sciaudone

La digitalizzazione pone difficili sfide in tema di sicurezza, sotto molteplici profili. «Le imprese devono prestare particolare attenzione affinché la nuova apertura al mondo digitale non esponga a rischi i propri asset immateriali quali segreti aziendali e know-how nonché i dati sensibili di cui sono responsabili», prosegue **Giacomo Moleri**, partner ***Spheriens***. «Casi come quello molto recente di Campari dimostrano l'attualità di questo rischio e i danni che attacchi di questo ge-

Supplemento a cura di ROBERTO MILIACCA
rmiliacca@italiaoggi.it
e GIANNI MACHEDA
gmacheda@italiaoggi.it

La proprietà intellettuale è riconducibile alla fonte specificata in testa alla pagina. Il ritaglio stampa è da intendersi per uso privato

ItaliaOggi Sette

diffusione:88589
tiratura:133263

Sotto attacco settori come il Finance e Food Products

nere possono causare. Sempre più spesso, inoltre, si violano le reti aziendali per carpire informazioni utili a mettere in atto truffe ai danni delle società o dei partner di queste ultime. Cyber criminali, dopo essersi infiltrati nelle reti aziendali, si inseriscono in scambi di email con i fornitori e i clienti utilizzando indirizzi email che riproducono in maniera quasi identica quelle del personale interno per richiedere pagamenti verso conti che poi spariscono prima ancora che ci si avveda della truffa».

Licia Garotti

Il 2020 rappresenta l'anno di svolta della sicurezza informatica aziendale. Ne sono convinti **Licia Garotti**, **Lorenzo Cairo** e **Marco Galli** dello studio ***Gattai, Minoli, Agostinelli & Partners*** in quanto «da un lato, lo scenario attuale unito al nuovo approccio normativo hanno contribuito ad aumentare il livello di consapevolezza nei confronti di rischi connessi ad una gestione errata o deficitaria della cybersecurity. Il Gdpr ha rappresentato un momento di svolta: la normativa sulla protezione dei dati personali ha infatti istituzionalizzato il principio di accountability e ha imposto l'adozione di modelli basati sulla valutazione del rischio in relazione alle scelte strategiche in materia di sicurezza informatica aziendale. Dall'altro lato, la pandemia e la maturata centralità del lavoro da remoto hanno contribuito -o necessariamente obbligato- a innalzare la soglia di attenzione delle imprese, che si sono trovate a fare i conti con l'aumento esponenziale di incidenti di sicurezza (spesso di tipo ransomeware) e tentativi di truffa, specie di natura man-in-the-middle».

Ci troviamo in un momento in cui c'è un aumento notevole dell'utilizzo, della condivisione, della comunicazione e della conservazione di ingenti masse di dati, personali e non personali. «Le aziende debbono quindi proteggere i propri dati, che costituiscono degli asset in senso economico, da difendere dai sempre più frequenti e sofisticati attacchi informatici, furti di dati e data breach», spiega **Roberto Jacchia**, senior partner di ***De Berti Jacchia***, «tutte le imprese, con maggiore o minore dedicazione di risorse, tendono a introdurre delle precise procedure e protocolli, in cui convergono la prospettiva tecnica dell'IT officer, quella del Data Protection Officer e quella del responsabile legale e della compliance. Le aziende sono interessate a gestire gli oneri e le complessità che conseguono ad un data breach, sia come obblighi di segnalazione sia come misure tecniche d'emergenza. La preoccupazione è legata alla perdita di reputazione e di fiducia da parte dei terzi che affidano i loro dati all'azienda, con esposizione a richieste di danni. Inoltre, è quasi sempre necessario supporto legale per presentare denunce ed esposti, richiedere indennizzi assicurativi, valutare la posizione dell'azienda sotto il profilo della compliance in materia di dati personali, o gestire situazioni di crisi al confine della materia penale. Infine occorre gestire, anche dal punto di vista legale, i provvedimenti delle autorità regolatorie (e le eventuali sanzioni) a carico di chi ha mostrato lacune nella difesa da attacchi informatici». Gli autori degli attacchi informatici spesso si nascondono all'estero «in luoghi protetti, e quasi mai agevolmente identificabili. In pochi casi di grande dimensione o rilievo mediatico, possono essere mobilitate le risorse della giustizia penale, ma molto più frequentemente i crimini informatici restano di fatto impuniti».

Gianluigi Marino

Molte norme sono di matrice europea pertanto il quadro normativo italiano non è così distante da quello degli altri Stati membri. «La difficoltà principale è che in molti casi si tratta di fattispecie che richiedono indagini complesse (anche dal punto di vista tecnico)»; spiega **Gianluigi Marino** partner di ***Osborne Clarke***, «e coordinamento a livello internazionale. Inoltre, il rischio per le aziende è non solo quello di subire i danni derivanti da una azione illecita di terzi ignoti ma anche quelli derivanti dall'eventuale accertamento della carenza di misure tecniche e organizzative adeguate (talvolta, anche a fronte di investimenti significativi)».

La rapida evoluzione delle tecnologie importa un altrettanto rapido mutamento delle condotte illecite nelle loro forme di manifestazione, a cui il legislatore deve adeguarsi. «Sotto il profilo penale, quindi repressivo», spiega **Pietro Montella**, founding partner di ***Montella Law***, «le fattispecie previste (frode informatica, accesso abusivo, diffusione di hardware diretti a danneggiare sistemi ecc..) sono capaci di fungere da contenitore delle azioni illecite, al fine del perseguimento dell'agente e dell'accertamento del reato. In tema di tutela e difesa della parte lesa, sarebbe di certo, invece, auspicabile una disciplina organica della materia. Organizzazioni criminali transnazionali e piccoli truffatori del commercio in line rappresentano gli estremi della delinquenza informatica, autori, in molti casi, di difficile individuazione ed economicamente incapaci di risarcire il danno».

Gli strumenti normativi sovranazionali faticano a rivelarsi efficaci per colpire queste realtà. Per questo è fondamentale la prevenzione. «La predisposizione di una procedura Cyber security rappresenta la pianificazione di un insieme di criteri, e risorse, capaci di rilevare il prima possibile attacchi, rimuoverne le cause, contenere gli effetti e ripristinare i sistemi allo stato originale, al fine di minimizzare l'impatto della minaccia sugli asset societari, sia dal punto di vista economico, che dal punto di vista reputazionale, sia per quanto riguarda i diritti e le libertà delle persone interessate alla violazione, rispondendo alle esigenze ed agli obblighi dell'art. 33 del Gdpr 679/2016», prosegue **Alessandro Rubino**, partner di ***Rubino Avvocati*** e specialista in cybersicurity, «La consulenza Cyber ha come scopo principale il raggiungimento del target ottimale. A tal proposito, si parte con la configurazione degli asset societari e della regola degli *Ottostep*. Con il processo di business process re-engineering si arriva alla redazione di una dettagliata policy sull'uso corretto delle postazioni di lavoro, integrate con un piano scelto, definito dalla procedure esistenti, in materia di smart working, al fine di procedere alla stesura ed alla progettazione del framework di riferimento, e quindi al raggiungimento di un profilo target per conferire all'organizzazione standard di compliance in materia di trattamento dati e cybersecurity».

Pietro Montella

Alessandro Rubino

Per **Antonio Bana**, partner dello ***Studio Bana,*** in Italia «manca una cultura della minaccia informatica, ma il phishing delle password, le altre problematiche legate all'accesso e all'identità, nonché i malware basati sull'ingegneria sociale, sono molto più diffusi di quanto pensiamo. È necessario dunque non solo adeguare le tecnologie, ma anche formare e rendere più consapevoli i propri dipendenti. L'emergenza Covid-19 ha fatto emergere in modo ancora più evidente la situazione di «disordine digitale», ovvero un aumento esponenziale dei dati e della condivisione senza controllo dei file aziendali e dei documenti conservati all'interno degli spazi di storage, senza misure di sicurezza idonee. Il ricorso allo smart working ha poi moltiplicato i punti d'accesso, lasciando via libera ai criminali informatici di fare breccia nelle nostre difese».

Secondo **Enrico Di Fiorino**, partner di ***Fornari e Associati*** «l'attività di impresa interessa fisiologicamente il trattamento di un gran numero di dati, comuni e sensibili, non solo dei propri dipendenti, ma anche di terzi. La prevenzione dei reati informatici appare porsi, dunque, in rapporto di complementarietà con il tema della sicurezza dei dati e più in generale della privacy. Occorre oggi un ripensamento nell'approccio alla cybersecurity sia dal punto di vista tecnologico che culturale, che passa da due grandi consapevolezze: la prima, che tutti possiamo essere vittima di un attacco; la seconda, che bisogna dare valore (anche economico) alla propria sicurezza e a quella dei propri dati. Ai fini di una miglior tutela risulta quindi necessario affidarsi alle giuste competenze e investire in materia di prevenzione, che rappresenta l'unica strada per la gestione efficace dei rischi. Si consideri, peraltro, che l'impresa non è solo una potenziale vittima: vi è anche la possibilità che questa venga chiamata a rispondere dei delitti cibernetici, in qualità di responsabile».

Luca Tufarelli

Il tema degli attacchi informatici è di importanza vitale per il corretto andamento sia dell'attività d'impresa che per il corretto funzionamento di tutti i meccanismi della nostra organizzazione sociale. «La prima legge che si è occupata di regolamentare il tema fu il regolamento sulle misure minime di sicurezza emanata in attuazione della prima legge sulla privacy con il dpr 318/1999», ricorda **Luca Tufarelli**, founding e naming partner di ***Ristuccia & Tufarelli***, «per troppo tempo si è confuso il tema della sicurezza dei sistemi con gli obblighi in materia di privacy. Il dlgs 18 maggio 2018, n. 65 ha dato attuazione nel nostro ordinamento alla direttiva comunitaria 2016/1148 (c.d. Direttiva Nis) che in maniera chiara spezza questa convinzione e distingue l'esigenza di garantire la sicurezza e resilienza dei sistemi in settori vitali. L'obbligo di notifica degli incidenti di sicurezza da parte del gestore dei sistemi agli organi di controllo governativi a ciò preposti (Csirt e Agid ove occorra) prescinde dal tema del coinvolgimento dei dati personali (la cui notifica al Garante dei dati personali semmai ai aggiunge) e a nostro avviso costituisce un valido sistema per obbligare chi opera in settori vitali a garantire la sicurezza e resilienza dei sistemi non foss'altro per le pesanti sanzioni che la legge commina qualora l'incidente risulti poi dovuto a carenze sull'adeguatezza delle misure di cyber security adottate».

Con il Dpcm n. 131 pubblicato in *Gazzetta Ufficiale* lo scorso 21 ottobre, la normativa italiana ha compiuto un altro importante passo nella regolamentazione della cyber security, ovvero in quello specifico settore del diritto che disciplina gli strumenti e le tecnologie predisposti per proteggere i sistemi informatici dagli attacchi e dalle minacce provenienti dall'esterno e, quindi, le misure per la difesa della confidenzialità, integrità e disponibilità di un sistema informatico. «Il panorama normativo è complesso e articolato», spiega **Nicolò Ghibellini**, associate di ***Marazzi & Associati***, «A livello internazionale, uno dei principali riferimenti è rappresentato dal Manuale di Tallin (Tallin 1 del 2013 e Tallin 2.0 del 2017) con il quale si è cercato di individuare le regole di diritto internazionale applicabile alla guerra cybernetica e alle operazioni cyber in tempo di pace. A livello europeo, deve essere citata la direttiva Ue 2016/1148, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. Direttiva Nis), recepita dal nostro ordinamento con il D.lgs. 65/2018. In tale contesto, ad ulteriore definizione di un quadro nazionale di cyber law, si inserisce il recentissimo Dpcm 131/20, ovvero il Regolamento in materia di perimetro di sicurezza nazionale cibernetica, emanato in attuazione di quanto previsto dal DL 105/19 (convertito nella L. n. 133719)».

Negli ultimi anni le imprese stanno prestando un'attenzione sempre maggiore alle tematiche concernenti il Cyber Crime e la Cyber Security. «Per questo sempre più aziende stanno adottando specifiche misure volte a prevenire e gestire il fenomeno», conclude **Giulia Stefanini**, associate di ***Picchi, Angelini & Associati***, «prima tra tutte, la formazione interna e continua del personale su temi ricorrenti (come il phishing). Gli sforzi delle imprese trovano oggi un fattivo riscontro anche sul piano normativo; l'evoluzione tecnologica, infatti, ha reso necessaria l'introduzione - sia a livello nazionale che a livello internazionale - di nuove fattispecie di reato volte a contrastare condotte che mettono in pericolo l'integrità dei dati, dei programmi e dei sistemi informatici delle imprese».

© Riproduzione riservata

La proprietà intellettuale è riconducibile alla fonte specificata in testa alla pagina. Il ritaglio stampa è da intendersi per uso privato