In Tendenza Popolari

Orrick e L&B Partners con Sonnedix e ICS per la compravendita di 4MW di fotovoltaico
AMBIENTALE, SOCIETARIO, SUITS, ULTIM'ORA

Ecco chi sono i migliori avvocati d'affari del 2020
PENALE, SUITS, ULTIM'ORA

Impresa: la classifica dei 100 manager selezionati da Forbes
IMPRESA, ULTIM'ORA

Imprese, Rapporto CERVED PMI 2020: "A rischio 2 milioni di posti di lavoro"
LAVORO, SOCIETARIO, ULTIM'ORA

Legance e Cappelli Rccd nel finanziamento Solution Bank ad Adl Milano
BANCARIO, SUITS

Indorama Netherlands B.V. acquisisce IMO Polowat SP. Z O.O.
INTERNAZIONALE, IP, SUITS

RIFLESSIONI ULTIM'ORA

Pandemia e digitalizzazione, aziende sempre più colpite dal Cybercrime

Redazione • Dicembre 7, 2020

L'**informatizzazione** e digitalizzazione forzata portata dal periodo pandemico ha decisamente giovato alle aziende che, per sopravvivere e proseguire nelle attività, hanno fatto un balzo in avanti in conoscenza e capacità d'uso dei sistemi informatici.

Va da sè però che la tecnologia, insieme agli ovvi vantaggi, porti anche inediti problemi per le aziende, che si trovano a far fronte al mondo del **Cybercrime** (crimini informatici), cresciuto esponenzialmente negli ultimi mesi.

Antonio Ranalli, firma di **Italia Oggi**, in un articolo pubblicato il 6 dicembre, ha analizzato le difficoltà incontrate dalle imprese nell'affrontare i numerosi attacchi informatici subiti in questo periodo, soprattutto negli ambiti del **Finance** e del **Food Products**, intervistando alcuni degli avvocati italiani, tra i massimi esperti del settore.

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 2014 e 2018. Il rapporto Clusit riporta che nel corso dell'ultimo anno sono stati effettuati 1.670 accessi illeciti. Emerge chiaramente come Cybercrime e Cyber espionage siano in netta crescita, segnando un aumento rispettivamente del 12.3% e dello 0.5%.

«Gli strumenti maggiormente usati dagli hacker – ha affermato il senior associate **Ivan Rotunno** di **Orrick** – hanno riguardato le campagne di malware a tema Covid-19 e l'ultilizzo di spam e phishing. In periodo di smartworking, gli hacker hanno puntato per lo più sui lavoratori e sull'assenza di presidi tecnici adeguati ad arginare violazioni ai sistemi It delle imprese. La necessità di costituire un reparto ad hoc, che controlli questi ambiti e sappia come muoversi in caso di attacco, è fondamentale, indipendentemente dalla crisi sanitaria».

Barbara Pontecorvo di **Tonucci & Partners** spiega: «La sfida del Paese è aumentare la digitalizzazione, ma anche di investire contemporaneamente in sicurezza. Oggi è quantomai necessario, per aziende che richiedono assistenza, anche preventiva, avvalersi di servizi di consulenza su tutti gli aspetti in materia di protezione dei dati e sistemi di sicurezza. Il servizio che offriamo contempla una serie di questioni complesse relative alla protezione dei Dati e Cybersecurity, come ad esempio formazione e aggiornamento delle politiche relative alla Privacy in ogni ambito delle dinamiche aziendali».

Ranalli riporta anche i dati della **Polizia Postale**, che mostrano un netto incremento di questi fenomeni di violazione. «La Direzione della Postale – afferma **Andrea Puccio**, managing partner di **Puccio Penalisti Associati** – mostra che la pandemia ha allargato la superficie d'attacco, visto che molte cose che prima svolgevamo fisicamente ora si fanno online, dal lavoro agli acquisti, passando per la sanità».

Nel periodo preso come riferimento dalle forze dell'ordine, 28 grandi società sono state vittime di frodi informatiche, per un totale di circa 25 milioni di euro di danni. Altro fenomeno in repentino aumento sono le mail **«fake ceo»**, finte comunicazioni di posta elettronica che sembrano provenire dai vertici dell'azienda, che registrano un +378%.

Un'altra ricerca ha inoltre riscontrato un aumento del 30% dei cyber attacchi nel **Finance** e nel **Food Products**. «Osserviamo che le aziende si stanno orientando sempre più nel cercare di prevenire gli attacchi informatici sviluppando un'infrastruttura It solida», 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". 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».

I settori di riferimento nella gestione dei rischi cyber sono Security Strategy, Governance e Compliance. **Iacopo Destri**, partner dello studio legale internazionale **C-Lex** di Milano, ha commentato ha riguardo: «Sopratutto negli ambiti dei servizi della gestione lavoratori e nel delivery questo periodo crea potenziali falle di sicurezza poiché, soprattutto nella prima fase, lo smartworking era effettuato con strumenti propri degli impiegati, non dotati dei giusti sistemi di protezione. Gli investimenti a riguardo sono e devono essere ingenti e mirati, per assicurare a chi opera da remoto workflow sicuro e produttivo».

«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. Le app in cloud spesso 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, che guadagnano l'accesso a un account autorizzato per craccare dati criptati e rubare informazioni a scopi di frode. Rischi giungono anche dall'intercettazione delle conversazioni e dalla contraffazione della voce delle persone, utilizzata dai sistemi delle banche online per autenticare gli utenti. Visto ciò 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 velocissime», ribadisce **Francesco Sciaudone**, managing partner di **Grimaldi Studio Legale**.

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», dice **Giacomo Moleri**, partner **Spheriens**. «Casi come quello molto recente di Campari dimostrano l'attualità di questo rischio e i danni che attacchi di questo genere 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».

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 di condivisione, comunicazione e conservazione di ingenti masse di dati, personali e non personali, fa notare Ranalli. «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».

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)»; continua **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 porta un altrettanto rapido mutamento delle condotte illecite nelle loro forme di manifestazione, a cui il legislatore deve adeguarsi. «Sotto il profilo penale, quindi repressivo», ribatte **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».

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».

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», sostiene **Nicolò Ghibellini**, associate di **Marazzi & Associati**, «A livello internazionale, uno dei principali riferimenti è rappresentato dal Manuale di Tallin (Tallin 1.0 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».

Tags: Cybercrime DirittoeAffari ItaliaOggi Ranalli sicurezza informatica

PREVIOUS ARTICLE
Orrick e MJH Alma per Prestiamoci con Banca Valsabbina nella seconda operazione in Italia nel settore del P2P Lending

NEXT ARTICLE
Premio Top Legal, Maisto e Associati premiati per Tax Contenzioso