Sicurezza informatica, che cos'è

Come sempre, è utile partire dalle definizioni. La prima è quella relativa alla **sicurezza delle informazioni** che è caratterizzata *"dalla salvaguardia della riservatezza, integrità e disponibilità delle informazioni gestite da un'organizzazione".* Una salvaguardia non solo da attacchi diretti, ma anche ad esempio da fenomeni come calamità naturali oppure da problemi accidentali e che non riguarda certo soltanto la difesa degli apparati informatici, dal momento che l'attenzione alla sicurezza delle informazioni esiste ben da prima dell'ICT. Più specificatamente rivolta alla protezione degli apparati informatici da azioni di attacco volontarie è la **sicurezza informatica,** che è un sottoinsieme della sicurezza delle informazioni, e che può essere definita come *l'insieme di prodotti, servizi, regole organizzative e comportamenti individuali che proteggono i sistemi informatici di un'azienda.*

Sicurezza informatica: tante aree diverse

Come è facile da capire, la sicurezza informatica riguarda in realtà tante attività distinte: si può avere sicurezza a livello applicativo, dei dati, a livello di rete (nel momento in cui si scambiano dati attraverso la rete Internet occorre garantire la sicurezza della rete, affinchè questi non vengano intercettati) e così via. Tanto che **secondo una recentissima analisi Gartner,** nel 2018 si spenderanno a livello globale circa 114 miliardi di dollari nella sicurezza informatica: oltre la metà, vale a dire quasi 59 miliardi di dollari sono appannaggio dei servizi collegati. La seconda voce di spesa è rappresentata dai prodotti che si occupano della protezione delle infrastrutture, che assorbono poco più di 14 miliardi. La protezione delle reti, invece, incide per quasi 12,5 miliardi. Meno importante di quello che si potrebbe pensare è il mondo consumer: i software acquistati dai comuni utenti producono un giro d'affari di poco meno di 6,5 miliardi, destinato a crescere leggermente nel 2019. Decisamente maggiore è il fatturato di un segmento poco sotto i riflettori come l'Identity and Access management, pure cruciale in ambito aziendale: da un valore di 8,8 miliardi nel 2017 si passerà a 9,7 miliardi nel 2018, che diventeranno 10,6 nel 2019. Ancora minoritarie, ma in crescita a doppia cifra, sono aree come l'Application security e la Data Security.

Sicurezza informatica: in Italia si spende di più

E in Italia? L'aspetto positivo, rispetto al recente passato, come evidenziato dall**'Osservatorio Information Security e Privacy del Politecnico di Milano,** è il trend di sviluppo: nel 2017 il mercato delle soluzioni di information security in Italia ha raggiunto un valore di 1,09 miliardi di euro, in crescita del 12% rispetto al 2016. Un passo in avanti nettamente superiore rispetto a quanto osservato negli anni scorsi, quando il mercato nazionale viaggiava a ritmi inferiori (4-6%). Di questo oltre miliardo di euro destinato alla sicurezza la gran parte (78%) è appannaggio delle grandi imprese e non potrebbe essere altrimenti, data la difficoltà delle Pmi nazionali a effettuare investimenti di questo tipo. A spingere le grandi aziende, più che i grandi attacchi citati in precedenza, è soprattutto la necessità di essere conformi alla nuova normativa europea sulla privacy, il **GDPR,** che da solo pesa per circa la metà dell'aumento di spesa individuato dalla ricerca.

Un po' di storia degli attacchi informatici

Ma da cosa ci si difende? Occorre premettere che la sicurezza informatica ha una storia trentennale: il primo virus informatico della storia, **Brain A,** è arrivato nel 1986 direttamente dal Pakistan. Successivamente è stata la volta nel 1989 di **AIDS,** un malware che presentava delle analogie fortissime con gli attuali ransomware. Da lì in poi ogni anno ha avuto i suoi virus particolari: il 1992 ha visto l'arrivo di **Michelangelo**, il 1995 di Concept, mentre il millennio si è chiuso con Happy 99 (che può essere definito come il primo malware dell'era web). Il nuovo millennio si è aperto con **Melissa e Loveletter**, mentre il 2003 è stato l'anno sia del primo attacco riuscito contro un'infrastruttura critica, la compagnia di trasporto Usa Csx, che del primo virus mobile della storia. Andando avanti negli anni si arriva a nomi più recenti come **Zeus e Stuxnet:** quest'ultimo può essere considerato come un vero e proprio spartiacque nella storia del malware, perché si è dimostrato capace di colpire non solo l'ambiente Windows ma anche i sistemi di automazione.

Il malware è sempre più il re degli attacchi IT

Attualmente, invece, la maggioranza degli attacchi sono compiuti utilizzando metodi ormai nominati milioni di volte da operatori del settore. Secondo **l'ultimo rapporto del Clusit nel 2017** gli attacchi gravi sono stati compiuti nella maggioranza dei casi (68%) con tecniche banali, come SQLi, DDoS, Vulnerabilità note, Phishing, malware "semplice": si tratta di un trend è in crescita di 12 punti percentuali rispetto al 2016. A testimonianza che gli attaccanti realizzano attacchi di successo contro le loro vittime con relativa semplicità, a costi sempre minori. Il malware, prodotto industrialmente e a costi sempre decrescenti, resta il principale vettore di attacco nel 2017, in crescita del 95% rispetto al 2016 (quando già si era registrato un incremento del 116% rispetto all'anno precedente). È soprattutto **Android** a essere nel mirino dei cybercriminali, in particolare per effetto delle protezioni scarse o nulle approntate dagli utenti, anche se iOS non può certo ritenersi immune dal rischio. I costi di questo complesso di attività, come è facile da immaginare, sono considerevoli: la stima del Clusit è che il solo cybercrime abbia provocato danni per 500 miliardi di dollari nel 2017. Truffe, estorsioni, furti di denaro e dati personali hanno colpito quasi un miliardo di persone nel mondo, causando ai soli privati cittadini una perdita stimata in 180 miliardi di dollari. Per quanto riguarda l'Italia il conto (anche se riferito al 2016) è ugualmente salato: si ipotizzano per quasi 10 miliardi di euro, ossia un valore dieci volte superiore a quello degli attuali investimenti nazionali in sicurezza informatica che, come detto in precedenza, ammontano a circa un miliardo di euro.

Ransomware, che cos'è e come ci si difende

Tra le minacce alla sicurezza informatica che hanno più interessato in questi ultimi anni le aziende di tutte le dimensioni e settori, comprese quelle italiane, c'è sicuramente il **ransomware**: si tratta di una tipologia di malware (o virus del computer) che non permette di eseguire alcune funzionalità del computer infettato e prevede la presenza di un riscatto (dal termine "ransom", in inglese riscatto, e "ware", diminutivo di malware) che gli hacker richiedono come compenso da pagare per poter rimuovere il blocco. La variante più nota della vasta famiglia dei ransomware è stata quella dei **cryptolocker,** che abbiamo già avuto modo di raccontare in diversi articoli. **Qui abbiamo anche rivelato alcune modalità per recuperare i file dei device infettati.** Ci sono poi alcune regole base che permettono di limitare la possibilità di cadere nelle trappole del ransomware che, sostanzialmente, si traducono nella necessità di mantenere alta la guardia. Innanzitutto occorre aggiornare frequentemente le applicazioni e i software (i malware come i ransomware, infatti,

sfruttano le falle di sicurezza presenti nei software obsoleti), oltre naturalmente utilizzare un buon antivirus. Grande attenzione dovrebbe essere impiegata quando si usa la posta elettronica (non aprendo allegati o link sospetti). Più in generale, eseguire regolari backup dovrebbe essere le prassi da adottare sempre e comunque, perché così si taglia alla radice l'arma di ricatto a disposizione dei cybercriminali.

Sicurezza informatica: i problemi arrivano dall'interno

Ma perché i cybercriminali riescono a concludere così spesso con successo i propri attacchi? Non è soltanto un problema di scarse difese approntate, ma anche delle brecce su cui gli attaccanti possono contare. Che molto spesso coincidono con i dipendenti aziendali: secondo una recente indagine di K**aspersky Lab e B2B International**, nelle aziende di tutto il mondo è ancora allarmante la carenza di consapevolezza relativa alla sicurezza IT. Lo studio, che ha coinvolto 7.993 impiegati, ha evidenziato che solo un dipendente su dieci (12%) è pienamente consapevole delle policy e delle regole di sicurezza IT stabilite dall'azienda per cui lavora. Non solo: ben il 24% dei crede che la propria azienda non abbia stabilito alcuna policy. Eppure, secondo un'altra ricerca di Kaspersky, il personale disattento ha contribuito agli incidenti di cyber sicurezza nel 46% dei casi avvenuti nel corso dell'ultimo anno. È però interessante notare come l'ignoranza delle regole non venga considerata una scusante: quasi la metà degli intervistati (49%) pensa, infatti, che tutti i dipendenti – se stessi inclusi – dovrebbero assumersi la responsabilità della protezione delle risorse IT aziendali dalle minacce informatiche. Date queste premesse, i dipendenti non corrono solamente il rischio di diventare in prima persona vittime dei cyber criminali ma rischiano di rendere vittime la propria azienda dalle minacce informatiche. La priorità delle organizzazioni dovrebbe essere dunque quella di impegnarsi nell'educazione dello staff e nell'installazione di soluzioni potenti ma anche semplici da usare e gestire, che permettano di migliorare la protezione dell'azienda anche a chi è meno esperto di sicurezza IT. Anche le aziende di piccole e medie dimensioni dovrebbero avvalersi di regolari training di formazione sull'importanza della sicurezza IT per lo staff e di soluzioni personalizzate.

Sicurezza informatica, protezione dati e privacy: cosa cambia con il GDPR

Come abbiamo accennato in precedenza, negli ultimi anni molti investimenti aziendali in sicurezza sono stati spinti dall'entrata in vigore del GDPR. In che modo il GDPR influenza la sicurezza informatica? Innanzitutto c'è da osservare che la nuova normativa europea pone un focus specifico sulla sicurezza delle informazioni, tanto che c'è un articolo dedicato, il numero 32, che assicura delle indicazioni chiare e prescrittive. Occorre poi considerare che se l'obiettivo del GDPR è tutelare i diritti dei cittadini in materia di privacy, è chiaro che questo diritto non possa prescindere da trattamenti che presentino misure di sicurezza adeguate. Tutto questo cambia la prospettiva della sicurezza: con il GDPR il titolare viene responsabilizzato (la cosiddetta accountability), chiedendogli di valutare nel suo contesto e in relazione ai suoi rischi quali siano le misure di sicurezza più adeguate per garantire la tutela dei dati. In questo senso un altro elemento fondamentale introdotto è la richiesta di effettuare una valutazione dei rischi a cui le informazioni sono soggette, con gradi di complessità differenti a seconda delle organizzazioni. In buona sostanza il GDPR costringe tutti quelli che hanno a che fare con i dati di cittadini europei a occuparsi di sicurezza e a pensare in una prospettiva di gestione del rischio, ossia un atteggiamento che sinora era appannaggio soltanto delle grandi aziende (e neanche tutte in realtà).

Sicurezza informatica, come farla in azienda

Se da un lato è indubbio che la gestione della sicurezza informatica sia diversa a seconda della dimensione aziendale, è possibile comunque tracciare alcuni principi base che aiutano a capire come ci si può difendere in maniera efficace. Una buona politica di sicurezza si compone perlomeno di cinque fasi successive: l'identificazione (bisogna capire quali sono asset da proteggere e da quali minacce), l'approntamento di misure di protezione in maniera adeguata (controlli e contromisure di sicurezza, ad esempio installando i firewall), la rilevazione dell'evento negativo (detect), la response – cioè scatenare le difese per limitare i danni prodotti dall'attacco – e, infine, la capacità di recover, per ristabilire le condizioni originarie (ad esempio grazie al disaster recovery). Più in generale, una delle prime cose da mettere in atto è sviluppare una cultura interna: è inutile installare delle misure di sicurezza roboanti se poi il proprio personale continua a fare click su qualunque cosa riceva per email. In secondo luogo, visto che lo chiede il GDPR e non solo, serve un approccio orientato ai rischi, che serva a calibrare le scelte, in funzione anche dei budget presenti. Con un buon sistema di prevenzione attiva e scansioni regolari è poi possibile ridurre al minimo la minaccia di una perdita di dati per mano dei criminali informatici. Vitale è poi eseguire un backup regolare, che permette una continuità di accesso alle informazioni, che rappresenta una dimensione fondamentale della sicurezza IT.

Sicurezza informatica: il ruolo del canale IT e dei System integrator

In che modo il canale IT può affrontare il mondo della sicurezza? Occorre partire dalle basi: la cybersecurity è sempre più una priorità strategica per ogni azienda e organizzazione al mondo, indipendentemente da dove risiedono i dati. Quello che davvero è cambiato è il modello di business con cui le aziende operano, che rende inevitabile un salto di qualità da parte degli specialisti della sicurezza, che devono essere capaci di garantire il supporto necessario ai propri clienti e creare un valore aggiunto per i propri clienti, mixandolo con il giusto grado di innovazione. Anche perché, oltre agli attacchi degli hacker, le aziende devono guardarsi dall'eccessivo affollamento del mondo della security, che conta circa 2000 società presenti sul mercato. Ai consulenti della sicurezza, dunque, spetta l'arduo compito di selezionare quelle più adatta per ogni specifica esigenza aziendale, rendendo più semplice possibile la necessaria integrazione delle tecnologie e piattaforme.

Le materie da studiare per la sicurezza informatica

Come si acquisiscono le competenze necessarie per diventare **professionisti della sicurezza**? La prima questione da mettere in evidenza è che si tratta di un tema estremamente trasversale, che dà modo di affrontare problemi molto diversi tra loro: si va dalla gestione del rischio a quella dei sistemi, passando per la sicurezza software e i penetration test. Esistono dunque professionisti specializzati su alcune nicchie specifiche e altri che invece sono in grado di affrontare la protezione dei sistemi informativi a 360 gradi. In entrambi i casi, però, per acquisire le competenze necessarie è possibile seguire due tipi di percorsi: il primo prevede un cammino istituzionalizzato, che passa innanzitutto dall'acquisizione di una laurea triennale o magistrale in informatica. Successivamente è possibile iscriversi a uno dei tanti master o corsi di specializzazione ormai presenti in diverse università italiane, come ad esempio la Cyber Academy dell'Ateneo di Modena Reggio Emilia. Accanto a questo percorso istituzionalizzato c'è sempre la possibilità di imparare il mestiere in modo tradizionale: il caso classico è quello di una figura professionale che già lavora nell'IT e decide di dedicarsi di sua iniziativa – o su indicazione della propria azienda – all'approfondimento

di queste tematiche, magari frequentando uno dei tanti corsi di formazione disponibili, fuori dai canonici circuiti universitari.

Al di là però della formazione in aula e in laboratorio, un professionista della sicurezza deve avere una prospettiva soprattutto pratica sui problemi. Quel che è certo è che, negli ultimi anni la richiesta di professionisti della sicurezza è in evidente aumento. Anzi, la domanda è maggiore della disponibilità di queste figure, complice anche la maggiore cultura favorita da casi come quello di **Wannacry** e da normative come quella del GDPR. Inoltre l'accresciuta dipendenza delle aziende dai sistemi informativi rende di per sé il tema più critico. Tutto questo sta rendendo appetibile anche da un punto di vista economico questa professione, anche se di rado gli esperti di sicurezza IT sono assunti in maniera continuativa dalle aziende, trovandosi perlopiù a lavorare come free lance. Un modo efficace per distinguersi sul mercato dei professionisti della sicurezza è quello di investire su una certificazione internazionale. Il semplice svolgimento di un esame costa qualche centinaio di euro, mentre la frequentazione di un corso propedeutico è più dispendiosa (in genere qualche migliaio di euro). In materia di competenze sull'organizzazione della sicurezza delle informazioni il punto di riferimento è la Lead auditor ISO/IEC 27001, che è spesso richiesta per la partecipazione a numerosi bandi di gara. In ambito di competenze organizzative e tecnologiche c'è la CISSP – Certified Information Systems Security Professional, che attesta la conoscenza ad ampio spettro dei principi di progettazione e gestione dei sistemi di sicurezza informatica. Una terza certificazione spendibile sul mercato è la CIFI (Certified Information Forensics Investigator), che è stata sviluppata per esperti nel campo dell'information forensic con esperienza pratica nello svolgimento di indagini in supporto alle forze dell'ordine o nella partecipazione a un team aziendale. I**n questo articolo è possibile trovare un elenco completo delle certificazioni più utilizzate in materia di sicurezza informatica.**

Come si evolvono gli attacchi DDos

Tra le minacce più insidiose nel campo della sicurezza informatica ci sono sicuramente gli attacchi DDoS (distributed Denial of services), con cui gli hacker rendono un server, un servizio o un'infrastruttura indisponibile sovraccaricando la banda passante del server, utilizzando le risorse fino all'esaurimento. **In questa intervista,** un esperto di Netscout Arbor racconta l'evoluzione degli attacchi DDos, che si stanno progressivamente facendo meno frequenti ma più intensi relativamente alla portata dell'attacco, anche nel nostro Paese.

Primo semestre 2018 negativo per la sicurezza informatica

Nonostante la maggiore attenzione complessiva relativamente al tema della sicurezza informatica, gli attacchi del cybercrime non accennano a diminuire, anzi. Lo mette in evidenza **uno studio rilasciato dal Clusit, relativo al primo semestre del 2018 (qui è possibile leggere il servizio completo)**: in questo periodo sono stati registrati ben 730 attacchi gravi registrati a livello globale, che corrispondono a una crescita del 31% rispetto al semestre precedente. Numeri che fanno del primo semestre 2018 il peggiore di sempre: in particolare, in questo periodo si è registrata una media di 122 attacchi gravi al mese (rispetto a una media di 94 al mese nel 2017). Buona parte di queste incursioni del cybercrime non sono particolarmente elaborate e sofisticate: il "Malware semplice" – prodotto industrialmente a costi sempre decrescenti – si conferma infatti il vettore di attacco più utilizzato (40% del totale degli attacchi).

Fonte: digital4trade

Erik Dalla Valle