Tiratura: 10.000 Diffusione: 15.000

Harvard Business Review ITALIA

Mensile

Data 10-2017
Pagina 69/75
Foglio 1 / 7

TECNOLOGIA, IMPRESE E SOCIETÀ

Crimini informatici: la minaccia è in aumento

NON ESISTE IN PRATICA UN'AZIENDA CHE NON SUBISCA PRIMA O POI UN ATTACCO INFORMATICO, E LA TENDENZA È IN NETTO AUMENTO. PURTROPPO, NON C'È UNA SOLUZIONE DEFINITIVA PER RISOLVERE IL PROBLEMA, MA OCCORRE AFFIDARSI A UNA STRATEGIA GLOBALE DI CUI LA TECNOLOGIA È SOLO UNA PARTE DELLA SOLUZIONE, CHE SI BASA SOPRATTUTTO SULLA CONSAPEVOLEZZA E LA FORMAZIONE DELLE PERSONE.

DI ANDREW BECKETT E MARIANNA VINTIADIS

L'85% delle imprese che hanno risposto nell'ambito del Global Fraud & Risk Report 2017 (rapporto che Kroll redige annualmente sulla frode e altre fonti di rischio per le imprese), ha evidenziato di aver subito una perdita di dati negli ultimi 12 mesi (figura 1). Un livello simile di attacchi informatici viene segnalato anche da altre società di ricerca globali e dai Governi di tutto il mondo.

In parte, questa tendenza in aumento (del 7% rispetto al 2016) è guidata dalla crescente criminalità informatica economica che trae "sostentamento" dalle vite e attività sempre più connesse dei Governi, delle aziende e dei cittadini. Questo, associato a scarsi livelli di sicurezza informatica nei sistemi utilizzati, ha portato al proliferare dei criminali informatici. É così che alcuni Stati europei riportano un incremento nella frequenza di episodi di crimine informatico rispetto a quelli di crimine tradizionale. Come tutti gli altri Paesi, anche l'Italia è soggetta ad attacchi informatici anche se, purtroppo, vi è una minore consapevolezza rispetto ad altre economie più avanzate, anche a causa dalla scarsa copertura da parte dei media locali su casi di crimini informatici che hanno colpito aziende italiane. Inoltre, l'economia italiana è caratterizzata da piccole aziende dinamiche che da una parte hanno meno probabilità di destinare risorse alla difesa informatica, mentre dall'altra hanno maggiori possibilità di caderne vittima. Ora ci sono più criminali informatici che mai ad approfittare delle opportunità disponibili, tenendo in considerazione che:

- meno sono le persone coinvolte in un disegno criminale minori sono le possibilità di perdite o infiltrazioni.
- I reati tendono a essere perpetrati da Paesi terzi, fatto che rende costoso e molto difficile per le forze dell'ordine perseguire il crimine.
- Le probabilità di essere scoperti sono molto più basse.
- Le pene e le sanzioni sono molto minori rispetto ad altri delitti, in particolare rispetto a quelle legate ai crimini per droga.
- I costi per la preparazione di un attacco sono molto più bassi.
- I mercati per i dati rubati e la proprietà intellettuale fanno sì che i proventi siano facilmente monetizzabili.
- Il denaro rubato è in formato elettronico e quindi più facile da spostare rispetto ai contanti e considerazioni analoghe possono essere fatte anche sui dati.

Nell'indagare e trovare soluzioni al cyber-crimine in tutto il mondo, le tendenze che abbiamo potuto analizzare possono essere classificate nelle seguenti macro aree:

1. **Cyber-crime come servizio.** I criminali informatici non devono essere necessariamente esperti ingegneri informatici per mettere a punto i loro attacchi. Infatti, attacchi già pronti possono tranquillamente essere acquistati e scambiati su internet all'interno di appositi mercati, (nella maggior parte dei casi, gli attacchi acquistati sono corredati di aggiornamenti e supporto gratuiti); alternativamente, i committenti possono acquistare un servizio dando semplicemente i dettagli dell'obiettivo e lasciando al fornitore il compito di creare l'attacco. Fino ad oggi questa è stata un'attività molto redditizia per la criminalità organizzata e vi è il sospetto che alcune organizzazioni

terroristiche forniscano questi servizi come mezzo per finanziare le loro operazioni.

2. **Ransomware.** Durante il 2017 abbiamo già assistito a due dei più grandi attacchi di *ransomware* mai registrati. Il 2016 ha visto un aumento di quasi il 1500% nel numero di attacchi di questo tipo rispetto al 2015 e questa tendenza sembra destinata ad aumentare. *Ransomware* è una delle principali famiglie di *malware* acquistabili su internet, e molte nuove varianti vengono scoperte ogni mese.
3. **Manomissione della posta elettronica aziendale.** La presentazione di fatture false o la richiesta di modificare le coordinate bancarie del destinatario in caso di pagamento di fatture legittime è un altro trend in rapida crescita che sta costando ogni anno miliardi di dollari all'industria globale in tutti i settori. Anche in questo caso la tendenza è in crescita e non sembra destinata a rallentare.
4. **Vendita di dati.** I dati rimangono una merce chiave per i cyber-criminali in quanto facilmente scambiabili e monetizzabili. A volte, i criminali rubano i dati per le possibilità di guadagno finanziario immediato, ma stiamo rilevando sempre più frequentemente accessi tramite *back-door*, che vengono venduti a terzi per lo sfruttamento dei dati. L'ultimo gruppo che beneficia del furto di dati sono gli "aggregatori di dati" che raccolgono piccoli volumi (spesso dati di carte di credito o di conti bancari) che poi vendono in grandi volumi - spesso decine o centinaia di migliaia. Anche le vendite record di milioni di dati stanno diventando sempre più comuni.
5. **Pagamenti e frodi con carta di credito.** Il crescente utilizzo di *chip-and-pin* in tutto il mondo sta riducendo i casi di frode "*card present*", sono invece in aumento gli attacchi a carte di credito tramite reti ATM e NFC (*Near Field Communication* il c.d. "*contactless*") e altri dispositivi come Apple Pay attuati da bande di criminalità organizzata.
6. **Cyber-bullismo e abusi.** Abbiamo incluso il cyber-bullismo nella categoria, anche se i titoli dei giornali fanno generalmente riferimento a bande e piattaforme online create apposta per attaccare minorenni e individui vulnerabili e per lo scambio di immagini pornografiche e altri materiali illegali. Mentre le forze dell'ordine quest'anno hanno sgominato diverse bande internazionali che operano in questo tipo di mercati, altre ne hanno rapidamente preso il posto.
7. **Criptovalute.** Mentre Bitcoin sta rapidamente perdendo la propria posizione come valuta prescelta dalla criminalità organizzata, la crescita di criptovalute difficili da tracciare, grazie al crescente anonimato, continuano a sostenere l'economia sommersa e la criminalità organizzata.

Mentre la lista di cui sopra rappresenta le tendenze criminali più ampie, le tipologie di attacchi contro le imprese sono rimaste abbastanza costanti nel corso dell'ultimo anno. Nel complesso, come abbiamo visto, l'85% delle aziende che hanno partecipato alla nostra ricerca hanno dichiarato di essere state colpite da attacchi informatici. La perdita di informazioni commerciali confidenziali, il furto o l'attacco nel campo della ricerca e sviluppo e della proprietà intellettuale (IP) sono stati indicati come gli attacchi più frequenti da più di metà dei rispondenti, con picchi riguardanti l'attacco ai dati dei clienti (riportato dal 63% degli intervistati).

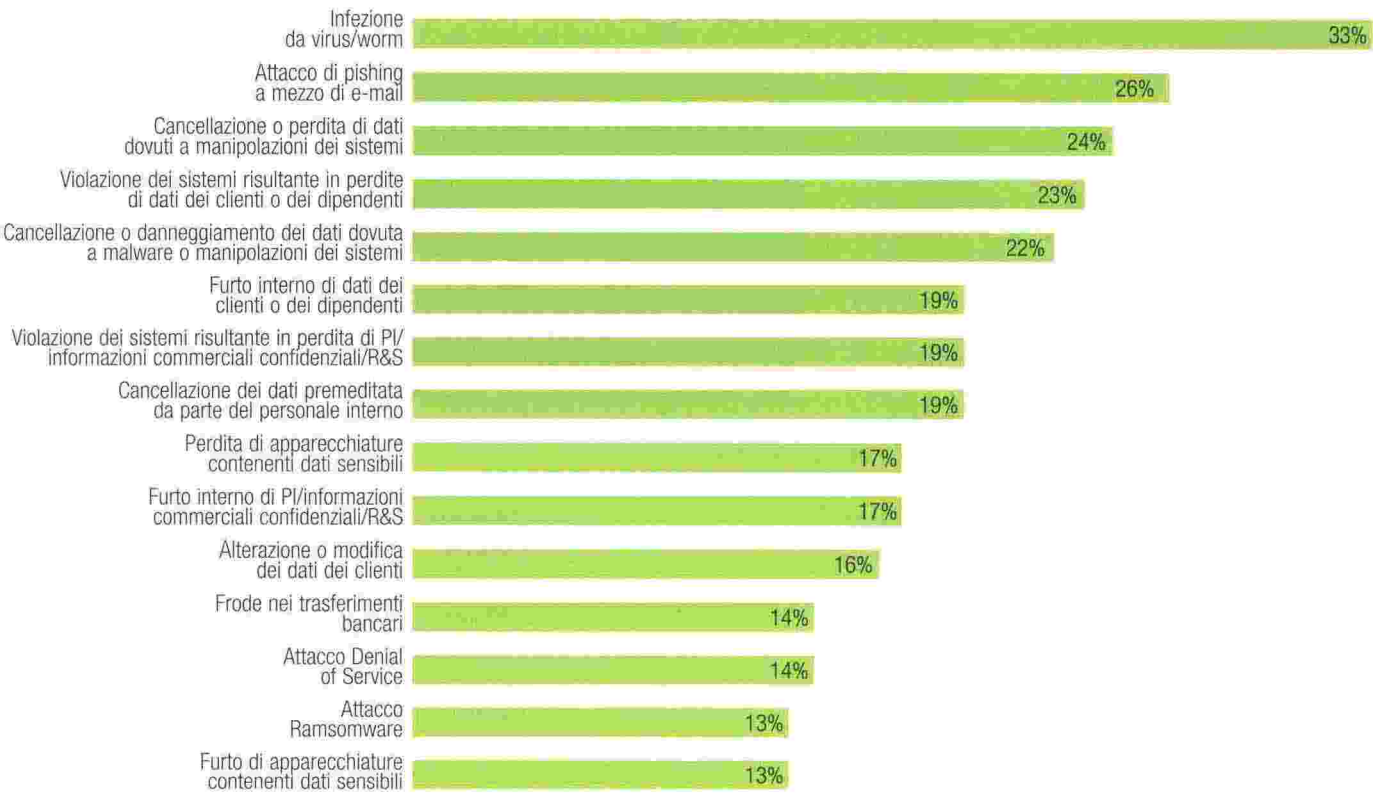
In Italia solo il 79% degli intervistati ha riportato un cyber-incidente negli ultimi 12 mesi, una cifra significativamente inferiore alla media globale. Una delle cause può essere ricondotta al basso livello di rilevamento, in quanto il resto delle informazioni riportate è in linea con le tendenze globali. Infatti, a quanto riportano le aziende italiane, i beni fisici e il denaro, i dati dei clienti e la proprietà intellettuale sono le tre aree più attaccate.

La più grande minaccia per dati e sistemi aziendali viene dall'interno. L'indagine Kroll ha rilevato che nel 44% dei casi la colpa è da attribuirsi a un *insider* - personale recentemente uscito dall'azienda (20%), personale temporaneo o a contratto (14%) o ancora personale attualmente impiegato (10%) - con una percentuale che sale fino all'80% per i casi di personale che viene coinvolto involontariamente (impiegati vittime di *social engineering*, attacchi di *phishing* etc.)

Per gli attacchi esterni, il *ransomware* rimane la minaccia singola più grande per le imprese, questo anche escludendo gli attacchi WannaCry e NotPetya di quest'anno. Tuttavia altre forme tradizionali di attacco rimangono ancora molto popolari:

- **Drive-By Downloads.** Il *malware* viene installato automaticamente sul computer di un utente quando accede a un sito compromesso.
- **Cross-site Scripting.** Un altro *malware* che sfrutta i siti legittimi per rubare le credenziali di accesso e le password memorizzate nel browser. La maggior parte degli utenti riutilizza le password per più siti e scopi.
- **Attacchi Watering Hole.** Una tipologia di attacco più mirata in cui il codice dannoso viene iniettato in un sito utilizzato spesso da un'azienda o un settore. Gli utenti di solito sono infettati con i download drive-by o "malware" dopo aver visitato il sito.
- **Wrappers.** In questo caso il *malware* è nascosto in un software legittimo che lo rende invisibile. Il *malware* viene inviato come documento PDF o Word

FIGURA 1.
Incidenti informatici subiti negli ultimi 12 mesi



che permette al file di non essere rilevato dalla maggior parte dei software antivirus.

L'aumento della criminalità informatica ha portato a una recente proliferazione di leggi e regolamentazioni in merito poiché i Governi e le aziende cercano di tutelarsi dalla crescente minaccia. In Europa, il Regolamento generale UE sulla protezione dei dati è entrato in vigore nel 2016 e si applicherà a partire da maggio 2018; questo introduce una serie di requisiti a cui dovranno sottostare le imprese che raccolgono, processano o memorizzano dati personali. Questo tipo di applicazioni non è una novità per l'Unione europea che annovera già regolamentazioni per la protezione dei dati personali. Tuttavia, i nuovi requisiti sono molto più stringenti e i livelli di multe per non conformità o in caso di perdita dei dati sono aumentati significativamente fino ad arrivare al 4% del fatturato globale dell'azienda, oppure 20 milioni di euro a seconda della gravità. Non è da trascurare il fatto che il calcolo della multa viene computato sul fatturato globale del gruppo di cui la società vittima della perdita di dati fa parte. Inoltre, molte altre giurisdizioni hanno creato regole analoghe, ma la mancanza di costanza nei requisiti ha portato almeno una rivista legale a chiedersi se l'aumento di una regolamentazione inconsistente non rappresenti essa stessa una minaccia ancora maggiore per le imprese internazionali rispetto ai criminali informatici. Alcuni settori specifici hanno inoltre introdotto le proprie normative e requisiti. È il caso del Dipartimento delle Finanze dello Stato di New York che ha introdotto controlli obbligatori per tutte le società finanziarie di servizi che operano nello Stato di New York, mentre il settore marittimo ha emesso nuove linee guida attraverso l'IMO, BIMCO e altri che si basano sui controlli in ISO27002 e gli standard NIST negli USA. Molti altri settori e giurisdizioni sono propensi a seguire l'esempio aggiungendo confusione al quadro già confuso per le imprese che desiderano operare a livello internazionale.

Misure di protezione dal cyber-crime

Cosa possono fare le aziende per proteggere se stesse e i loro dati? Di seguito le soluzioni che si possono adottare.

Formazione e consapevolezza del personale. Essendo il personale la più grande debolezza di ogni organizzazione, il primo luogo in cui migliorare le difese della propria azienda è proprio questo. Investire nella formazione di una coscienza informatica aiuterà il personale a individuare e combattere gli attacchi di social engineering e di phishing. Insieme alla formazione, per segnalare sempre attività sospette, le aziende dovrebbero essere in grado di indagarle e identificarle in anticipo, prima che diventino un vero e proprio incidente. Dovrebbero, inoltre, formare e impiegare personale per l'attuazione di solide politiche di sicurezza. La ricerca ha dimostrato che controlli basilari di "igiene informatica" possono neutralizzare circa l'80% degli attacchi comunemente osservati. Ricordiamo che la formazione del personale in Italia è spesso guidata da teoria e regolamentazione. Corsi pratici, frequenti e brevi (ad esempio su base trimestrale) che insegnano al personale come identificare messaggi e-mail sospetti o altre trappole sono fondamentali per una risposta pronta ed efficace.

Policy e Procedure. Oltre alla formazione del personale e alle policy degli utenti, le aziende dovrebbero esaminare le loro politiche di sicurezza più ampie. Mantenere i sistemi aggiornati riduce notevolmente la possibilità di essere attaccati. La vulnerabilità di Eternal Blue è stata scoperta nel mese di novembre 2016. Nel mese di febbraio 2017 Microsoft ha rilasciato un patch per la protezione contro di esso e nonostante ciò a maggio 2017 centinaia di migliaia di computer sono stati infettati da *ransomware* WannaCry che ne sfruttava appunto la vulnerabilità.

Governance. Le aziende dovrebbero identificare una specifica persona e carica per la sicurezza informatica e permetterle di attuare misure di sicurezza in linea con le necessità dell'azienda. Gli amministratori dovrebbero guidare dall'alto nel richiedere che le politiche e le procedure di sicurezza informatica vengano osservate, mentre il consiglio direttivo dovrebbe esaminare regolarmente l'efficacia delle norme di sicurezza e monitorare regolarmente i KPI per misurarne i miglioramenti.

Tecnologia. Anche se il cyber-crime è prevalentemente una questione legata alle persone, tuttavia la tecnologia gioca un ruolo fondamentale. Comprendere i sistemi; i punti di accesso e di uscita alla rete e come questi processi vengono monitorati e gestiti sono tutti passi importanti per difendere la società dagli attacchi informatici. Gli apparecchi di sicurezza hanno un ruolo fondamentale nella difesa degli asset aziendali e dei dati ma raramente sono l'unica soluzione richiesta.

FIGURA 2.
Una strategia globale di difesa

Le relazioni. Uno dei modi più semplici per aiutare a difendere asset critici dell'azienda è quello di ricevere e agire tempestivamente informazioni su potenziali minacce (*threat intelligence*). Stabilire rapporti all'interno del settore di mercato, area geografica e con il mondo accademico e le forze dell'ordine per essere sicuri di ricevere informazioni sulle ultime minacce o le tendenze d'attacco e per prepararsi di conseguenza. Nell'eventualità di un attacco, avere stretto relazioni e avere pronto un piano di risposta coinvolgendo fornitori precedentemente contattati che possano assistere nelle indagini forensi, nel ripristino dei sistemi per garantire la continuità del lavoro e nella gestione della comunicazione con le autorità, le parti interessate e il personale è cruciale per minimizzare l'impatto della violazione informatica nel breve e nel lungo termine. Purtroppo, non esiste una soluzione definitiva per risolvere il crescente problema della criminalità e delle minacce informatiche, ma è necessario affidarsi ad una strategia globale, esemplificata nella figura 2, di cui la tecnologia è solo il 20% della soluzione.

ANDREW BECKETT è responsabile Kroll della divisione cyber EMEA. **MARIANNA VINTIADIS** è responsabile Kroll per il Sud Europa con sede a Milano.

TECNOLOGIA, IMPRESE E SOCIETÀ

Cybercrime: un futuro di maggiori rischi, ma anche di maggiori protezioni

GLI ATTACCHI CRIMINALI VIA WEB SONO DESTINATI AD AUMENTARE SIA PER LE IMPRESE CHE PER I SINGOLI INDIVIDUI, MA A FRONTE DI UNA CRESCENTE AGGRESSIVITÀ DEI CYBERCRIMINALI SI RAFFORZERANNO ANCHE LE CAPACITÀ DI DIFESA. OCCORRONO PERÒ UNA MAGGIORE CONSAPEVOLEZZA E UNA FERMA CONDANNA SOCIALE.

DI GUIDO TRAVAINI E CAROLINA VIGGIANI

L'esperienza – come criminologi di professione - ci ha insegnato che nulla è più dinamico del crimine; uno straordinario "camaleonte" capace di adeguarsi perfettamente ai cambiamenti sociali, normativi ed, evidentemente, tecnologici. Ed è proprio su quest'ultimo aspetto che si focalizzano le riflessioni che seguono.

Partiamo da un dato oggettivo, ossia il sempre maggiore utilizzo dei sistemi informatici e del web.

Secondo un recente studio condotto da Cisco[1], il traffico globale IP passerà dagli attuali 1,2 a 3,3 zettabyte nel 2021, anno in cui gli abitanti della Terra che useranno uno smartphone saranno 5,5 miliardi, più delle persone che avranno un conto in banca (5,4 miliardi), acqua corrente (5,3 miliardi) o linee telefoniche fisse (2,9 miliardi). In Italia i dispositivi *wearable* tra cinque anni saranno 21 milioni; ora sono "solo" 7 milioni con una crescita annua del 24%. L'utilizzo di internet per i sistemi di video sorveglianza cresce di circa il 40 % annuo e si prevede che per il 2021 sarà aumentato di sette volte.

Uno sviluppo tecnologico trasversale che interessa e ha interessato enti, aziende, professionisti e una vastissima fascia della popolazione di età, livello culturale e istruzione differente. E il mondo criminale, veloce come sempre, ha colto sin da subito le opportunità tecnologiche per ampliare e differenziare le proprie azioni illegali e renderne più complessa la loro identificazione.

Crimine antico con mezzi moderni

Il *cybercrime* non ha nulla di rivoluzionario nella sua essenza criminologica; si è, semmai, di fronte a una modernizzazione di crimini antichi quanto l'uomo, come ad esempio il furto, il danneggiamento, l'estorsione o lo spionaggio.

Un esempio può aiutare a meglio comprendere. Si pensi a un reato quale l'estorsione, un crimine tanto odioso quanto noto e diffuso. Necessita per la propria esecuzione di alcuni passaggi obbligati: individuare una vittima, contattarla, prospettarle un male ingiusto e, infine, pretendere denaro o altro per evitare che il male, astrattamente prospettato, diventi tremendamente concreto. Tutto questo necessita di tempo, ma qui interviene la tecnologia. Inviamo, ad esempio, una serie di mail che contengono un *malware* in grado di bloccare il computer dei destinatari, richiediamo del denaro per riportare le cose alla normalità, attendiamo il versamento e, a pagamento avvenuto, il computer tornerà a operare perfettamente. Con una sola azione criminale possiamo raggiungere un numero elevatissimo di persone e moltiplicare gli effetti e i profitti della nostra condotta, riducendo sensibilmente il rischio di essere scoperti. Si tratta sempre della solita odiosa estorsione, ma in versione 2.0.

Considerare il *cybercrime* come una mera evoluzione tecnologica di condotte criminali note ha quale vantaggio il poter utilizzare alcuni paradigmi interpretativi tipici della letteratura criminologica, anche al fine

di poter immaginare scenari futuri.
Quanto all'oggi, il quadro non è tranquillizzante. Secondo il rapporto del Clusit 2017[2] in tema di sicurezza informatica, negli ultimi anni vi è stata una sensibile crescita di cyberattacchi condotti mediante tecniche di *phishing/social engineering*, con l'obiettivo molto chiaro di acquisire dati e informazioni riservate.
Solo nel 2016 almeno 15,4 milioni di persone nel mondo sono state vittime di un furto di identità che ha fruttato agli autori un vantaggio economico complessivo calcolato intorno ai 16 miliardi di dollari[3]. Perché numeri così grandi ed effetti così negativi?
Nel web circolano moltissimi dei nostri dati sensibili e impadronirsene non è cosa così complessa. Una volta che il nostro cyber criminale avrà le informazioni si costruirà una nuova identità, si presenterà come il vero Mario Rossi, senza però esserlo, e inizierà a fare acquisti facendoli pagare all'ignota vittima oppure potrà frequentare siti illegali e fare affari nel *dark web*, la rete oscura, a cui si accede con una minima conoscenza informatica. Si tratta di un *marketplace* virtuale ideale per soddisfare quelle esigenze, dalle più alle meno lecite, per cui l'anonimato non solo è gradito ma talvolta indispensabile. Ad esempio nel 2015, il Federal Bureau of Investigation ha condotto un'indagine su un sito pedopornografico che operava esclusivamente sul *dark web* individuando 215.000 adepti, molti dei quali usavano identità di altri. È anche possibile trovare "virus" con cui infettare computer di "nemici", programmi per controllare a distanza computer o telefonini, ma anche documenti falsi, passaporti, tessere di riconoscimento di tutte le polizie del mondo. Un bazar anonimo in cui si può perfino trovare chi, per una modica cifra, si offre come killer.
E a questo punto cosa succederà al nostro vero signor Rossi? Vivrà un'esperienza non piacevole, a tratti kafkiana, e in ogni caso si dovrà armare di pazienza e di un buon legale per spiegare a polizia, banche e familiari la sua estraneità ai fatti.

Imprese nel mirino

Vi è poi un'altra grande famiglia di cyberattacchi destinati alle imprese. Sempre secondo l'ultimo rapporto Clusit, i comparti più attaccati sono quelli creditizio, della grande distribuzione, dei servizi e sanitari. Nessuno si senta escluso!
Facciamo nostra una vecchia barzelletta che circola nel mondo della sicurezza informatica in cui si dice che esistono solamente due tipi di aziende: quelle che sono state attaccate e quelle che non lo sono state... finora[4].
Ne è la prova quel che è successo nel mese di maggio 2017, quando siamo stati spettatori di un attacco informatico su larghissima scala: 300.000 i computer "infettati", colpiti grandi gruppi industriali e società pubbliche e private in moltissime Nazioni. Secondo Europol si è trattato della più grande *online extortion* sino ad ora mai commessa[5]. Il "virus" era in grado di intervenire sul sistema operativo del computer rendendolo inutilizzabile. Ripristinare il tutto era molto semplice: versare una somma a titolo di riscatto, ben accettati i *bitcoin*.
Chi ha diffuso il *malware* ha deciso di colpire su larga scala con obiettivi multipli dalle grandi alle piccole aziende, alle banche centrali e agli ospedali. I giornali hanno riportato i tanti disagi che si sono venuti a creare: dal blocco della produzione industriale, all'erogazione di energia elettrica, al garantire le cure ai pazienti con esami strumentali da rinviare e mezzi di emergenza bloccati. Qui il mero guadagno si è scontrato con il concreto rischio di poter causare danni tali da mettere in serio pericolo la vita di molte persone.

Insufficiente consapevolezza

Sino ad oggi il criminale informatico ha beneficiato di un grandissimo vantaggio competitivo; una vertiginosa diffusione della tecnologia e del web senza una parallela crescita della consapevolezza da parte di tutti noi dei possibili rischi connessi. Ci siamo tutti mossi, in questa autostrada informatica, come tanti autisti inesperti e, a volte, imprudenti. Quante volte creiamo le nostre password aggiungendo al nostro nome e cognome i numeri invertiti della nostra data di nascita o di quella di un parente prossimo? Quanti di noi utilizzano i wi-fi pubblici senza nemmeno chiedersi se siano o meno sicuri? Tutto questo nonostante sempre più persone, con età differenti e con pochissima cultura di sicurezza tecnologica, utilizzino servizi delicati quali l'home banking, l'e-commerce con pagamenti tramite carta di credito o prenotazioni di esami medici sul web. Di fronte a una sorta di analfabetismo diffuso è stato davvero facile colpirci.
È interessante applicare a questo quadro l'approccio economico razionale di Gary Becker il quale, in uno dei suoi più interessanti contributi in tema di scelta criminale, ci insegna che il crimine non è nella maggior parte dei casi una scelta d'impeto ma semmai ragionata e che segue un calcolo basato su costi e benefici[6]. Partiamo dalla semplice formula $Oj = Oj\ (pj, fj, uj)$ che può sembrare complessa ma in realtà è tanto semplice quanto valida: O indica il numero di reati commessi da un soggetto in un particolare periodo j, data la probabilità soggettiva di arresto per reato (pj), di condanna (fj), mentre uj rappresenta la variabile etica e ambientale. Orbene, commettere crimini informatici, secondo questa matrice, è conveniente. I costi intesi come investimenti sono più bassi rispetto all'organizzazione di un crimine tradizionale, il rischio di essere individuati rimane piuttosto scarso

nonostante i notevoli sforzi delle polizie di tutto il mondo, (compresa quella italiana che è ben preparata), mentre il rischio di essere condannati pare ancor più remoto.
Accanto ai vantaggi vi è un altro elemento da considerare; il cyber-delinquente ha sovente la sensazione di commettere azioni sì illegali, ma non così gravi e certamente non paragonabili a quelle del criminale tradizionale. La distanza anche fisica rispetto alla vittima rende più facile l'attivazione di quelle tecniche che la letteratura criminologica chiama di neutralizzazione, una sorta di "via d'uscita", di disimpegno morale rispetto ai gesti illegali che si compiono. Vi è anche da considerare che sino ad oggi la reazione sociale rispetto a questo tipo di criminalità è stata modesta, anche perché considerata, erroneamente, lontana da ognuno di noi.

Un quadro destinato a cambiare

L'insieme di tutti questi elementi ha creato una situazione ideale per il cyber-criminale. Crediamo, però, che questo quadro sia destinato a cambiare. Le ragioni sono semplici.
In primo luogo, il vantaggio iniziale della ridotta capacità di fronteggiare gli attacchi è destinato a ridursi. Si sta assistendo a una reazione; molti Stati e aziende stanno investendo ingenti quantità di denaro nella *cybersecurity*. Ciò significa che si creeranno realtà sicure e altre più vulnerabili; quest'ultimo aspetto riguarderà soprattutto quelle di dimensioni più modeste o non in grado di adeguare il proprio livello di sicurezza informatica.
La sicurezza diventerà sempre più uno strumento di marketing: le imprese venderanno ai loro clienti la loro minore vulnerabilità rispetto alla concorrenza e la sicurezza informatica diventerà elemento distintivo e qualitativo. Le grandi aziende, come stanno già in parte facendo, chiederanno certificazioni di sicurezza informatica tanto ai professionisti quanto ai fornitori con cui decideranno di lavorare per evitare di che si crei una pericolosa asimmetria nella protezione.
Vi sarà un incremento di quella campagna di alfabetizzazione alla *cybersecurity* che ad oggi è solo all'inizio. Formazione che non può essere limitata ad aziende ed enti, ma dev'essere capillare a tutti i livelli della popolazione, magari iniziando proprio dalle scuole. Senza falsi allarmi o visioni apocalittiche, occorre far comprendere a tutti il concetto di rischio informatico. In questo modo crescerà non solo il livello di attenzione, ma anche la riprovazione sociale nei confronti dei cyber-criminali.
Per quanto riguarda le organizzazioni criminali, esse saranno sempre più consapevoli del valore che hanno nel nostro tempo l'informazione e le informazioni. Riuscire a ottenerle, analizzarle e magari manipolarle per usarle o rivenderle sarà certamente uno dei loro obiettivi. Aspetto questo ancor più delicato, vista la tendenza a utilizzare sempre più il web per consultazioni elettorali o semplicemente all'interno dei singoli movimenti politici. Riuscire a "penetrare" in questi siti e modificare risultati e contenuti significa alterare la volontà popolare.
Il quadro che si prospetta non tranquillizza e a preoccupare maggiormente è il rischio di un abbassamento del livello etico delle organizzazioni di *cybercrime* e degli hacker che per queste lavorano. Colpire le infrastrutture critiche significa aver scelto la concreta possibilità di mettere in serio pericolo la vita di moltissime persone. Non si tratta più di un narcisistico sfoggio di competenze, ma di un atto criminale che dev'essere paragonato e sanzionato come quelli contro la vita e l'incolumità delle persone.
In sintesi, lo scenario sta cambiando e le condizioni iniziali di grande vantaggio per il cyber-criminale si stanno riducendo con uno spostamento di attacchi sempre più tecnicamente raffinati che forse andranno a colpire meno il singolo cittadino, ma che avranno quale obiettivo la collettività nel senso più ampio del termine. La sensazione è che quella variabile *Uj* della formula di Becker stia perdendo, in questo mondo criminale, sempre più di significato e valore.
È fondamentale ricordare che dietro a un computer vi è pur sempre un individuo che decide cosa fare e cosa non fare. Ecco dunque che per tutelarsi, se da un lato è necessario un aumento delle difese tecnologiche, è altrettanto importante un'educazione comportamentale per diffondere la consapevolezza del danno e dei rischi che dal *cyber* possono derivare; in altri termini, investire sull'aumento della variabile etica, fino a creare una sorta di "deontologia tecnologica" alla portata di tutti.

GUIDO TRAVAINI insegna Criminologia all'Università Vita e Salute San Raffaele Milano ed è Visiting Professor alla Franklin University, Switzerland. **CAROLINA VIGGIANI**, criminologa, attualmente lavora per una multinazionale francese.

NOTE.
1. www.cisco.com/c/it_it/about/news/2017-archive/20170207.html.
2. https://clusit.it/rapporto-clusit/.
3. www.javelingstrategy.com/coverage-area/2017-identy-fraud.
4. Tratta dalla presentazione del libro *Il nodo di seta*, di Marco Forneris, Sandro Teti editore.
5. www.europol.europa.eu/newsroom/news/wannacry-recent-cyber-attack.
6. Gary S. Becker and William M. Landes, eds, *Essays in the Economics of Crime and Punishment*, Volume Publisher: NBER, 1974.