CYBERVADEMECUM

VII parte

Raffaele Azzarone

Aspetti economici

È *innegabile come lo strumento informatico e il libero accesso alla rete siano, ormai, da ritenersi indispensabili non solo nei settori produttivi, di crescita e di governo ma anche nella quotidianità del privato cittadino. Purtroppo, ciò consente ai criminali cibernetici di porre in atto azioni fraudolente di arricchimento illecito, arrecando danni economici alle vittime perché, per prevenire tali attività criminose, è necessario sostenere nuove spese. Nel testo che segue, in un'ottica rivolta alla pluralità degli aspetti economici che caratterizzano il crime online, ci si sofferma non solo sui danni conseguenti agli attacchi e sugli investimenti necessari in cyber security, ma anche sul giro d'affari e sui prezzi di prodotti e servizi malevoli riscontrabili nell'underground cyber market.*

I sistemi informatici e la capacità di connettersi in rete sono ormai indispensabili in ogni settore e fondamentali per lo sviluppo economico-sociale di un Paese, oltre che un fattore strategico di progresso e modernizzazione.
La I*nformation Communication Technology* (Ict) costituisce una componente essenziale per garantire l'efficienza degli organismi della Pubblica Amministrazione e la funzionalità e la produttività sia di quelle Infrastrutture – definite Critiche – la cui mancata operatività può influire negativamente sul benessere e sulla sicurezza del cittadino, sia delle imprese private in genere.
La libertà di accesso alla rete costituisce uno strumento irrinunciabile tanto per lo svolgimento delle attività lavorative quotidiane quanto per la diffusione dell'informazione, oltre che per finalità d'intrattenimento. D'altra parte, tale libertà di accesso consente a malintenzionati e criminali di porre in atto, per loro esclusivo tornaconto, manovre fraudolente a scapito di organismi e aziende, se non addirittura azioni tese ad arrecare danni irreparabili. Attività malevoli che comportano pregiudizi economici per chi ha subìto gli attacchi e, comunque, sensibili investimenti per coloro che intendano prevenirli.
I rischi di riflessi negativi sugli aspetti economici che organismi, imprese e infrastrutture possono correre in rete sono, in linea di massima, inquadrabili nelle seguenti tipologie:

– perdita della proprietà intellettuale, per consentire, ad esempio, a una società concorrente di immettere sul mercato prodotti innovativi prima che la società vittima del furto possa introdurre la propria versione legittima;
– perdita di informazioni sensibili per il business aziendale, come quelle, ad esempio, necessarie per ottenere vantaggi nelle negoziazioni commerciali o per sviluppare strategie competitive di business, includendo in tale categoria, anche le fraudolente manipolazioni dei dati della Borsa;
– perdite di opportunità economico-finanziarie, ossia dei benefici potenzialmente fruibili dallo sfruttamento del ciberspazio per una scarsa fiducia riposta nel web. Ciò può generare una ridotta produttività e le conseguenti minori vendite da parte di soggetti che decidano di evitare l'uso di internet per le proprie attività di business;
– perdita di reputazione, che può indurre l'allontanamento dei clienti o la mancanza di fiducia ed eventualmente anche la discesa delle quotazioni dei titoli azionari, se quotati in Borsa;
– compromissione dei dati di clienti e/o di partner;
– interruzione dei servizi offerti mediante tecniche d'attacco di tipo Ddos;
– compromissione della riservatezza dei dati;
– danni materiali agli asset dell'impresa, rendendo inutilizzabili gli apparati informatici;
– danni materiali ai clienti, ad esempio nell'ambito sanitario, distruggendo o modificando le cartelle cliniche degli assistiti.

Le modalità con le quali opera il cyber crime sono molteplici e multiformi.
Se ne segnalano alcune tra le più ricorrenti:

– furto o compromissione di dati sensibili, fenomeno in costante crescita, perpetrato per varie finalità, quali l'appropriazione indebita di know how e lo spionaggio industriale, con quanto ne deriva in termini di concorrenza sleale, violazione dei diritti sui brevetti e contraffazioni ecc.;
– distruzione o corruzione di dati sensibili, allo scopo di arrecare danni irreversibili;
– frodi di *online banking*, conseguenti a furti d'identità e alle credenziali di clienti, ottenute in maniera fraudolenta (ad esempio, tramite tecniche di *social engineering*) per accedere al conto corrente e trasferire illegalmente somme di denaro;
– frodi con carte di credito e bancomat contraffatti, messe a punto mediante la cattura dei dati con terminali P*oint Of Sales* (Pos) manomessi;
– alterazione dei contenuti delle pagine di web server per far apparire sullo schermo del visitatore un pop-up con la segnalazione che il computer è stato infettato da un malware, invitando a installare un falso antivirus per disabilitare quelli preesistenti e bloccare il Pc, così da poter lanciare richieste di pagamento per sbloccarlo;
– vendita di prodotti contraffatti, tra i quali quelli farmaceutici, diffusamente pubblicizzati online che, oltre a provocare perdite economiche per le case produttrici, comportano potenziali rischi per la salute del cittadino in ragione della loro scadente qualità o per l'uso di sostanze non soggette a regolari controlli;
– vendita di Sw contraffatti con perdita degli introiti relativi alle licenze d'uso dei titolari del marchio, anche se con sensibili risparmi degli acquirenti, qualora non si verifichi la truffa;
– vendita di brani musicali e di video contraffatti con violazione dei diritti d'autore, fenomeno ampiamente diffuso con inevitabile calo di vendite e noleggi di Cd e Dvd;
– truffe di impostori che, fingendosi parenti o amici, utilizzano l'account di una webmail compromessa per inviare a conoscenti dell'inconsapevole titolare messaggi con la richiesta di denaro necessario per uscire da una situazione critica inventata ad arte, fornendo l'indirizzo di intermediari, e contando sul fatto che in alcuni Paesi, al di sotto di un certo importo, non sono richiesti documenti;
– frodi fiscali verso governi con false richieste di rimborsi fiscali o pensioni, compilando moduli elettronici online e sostituendosi agli aventi diritto dopo essere entrati in possesso delle loro credenziali;
– frodi creditizie attraverso il furto d'identità e la conseguente richiesta di credito, utilizzando illegalmente dati identificativi altrui e relativi conti correnti bancari;
– *ransomware*, consistente nella richiesta di un riscatto per sbloccare il sistema informatico vittima dopo aver fraudolentemente infettato, crittandolo, l'hard disk;
– negazione del servizio offerto, esaurendo le risorse informatiche di un sistema che lo offre per mezzo di un attacco condotto simultaneamente da una moltitudine di Pc, che inondano la vittima con un elevatissimo flusso di dati, provocando l'interruzione delle relative funzionalità.

I rischi scaturenti dalle attività malevole svolte in rete sono fronteggiabili con investimenti economici sulla 'sicurezza delle informazioni', che involgano gli aspetti sia organizzativi che tecnologici.
La minaccia cibernetica, a livello globale, sta crescendo con ritmi esponenziali che non consentono indugi nell'intraprendere le azioni necessarie a contrastarla. Il Top Management di un organismo o di un'azienda deve affrontare la cyber security in termini di gestione generale del rischio e non come un esclusivo problema di natura It. Diventa necessario predisporre un piano integrato di sicurezza che coinvolga tutte le componenti strutturali e includa tutte le aree di vulnerabilità, definendone ruoli e responsabilità, promuovendone la consapevolezza e la conoscenza nonché le iniziative tese alla cooperazione sia nel proprio settore sia in ambito istituzionale, quale il Cert (*Computer Emergency Reaction Team*) Nazionale, il Cert Pa o il Cert Difesa. Essi sono deputati al contrasto delle minacce cyber attraverso un monitoraggio costante della loro mutevolezza e delle tecniche poste in atto dagli aggressori, con l'adozione di un *Risk Management* dinamico.
È necessario evidenziare come a tutt'oggi, pur consapevoli dei rischi connessi all'utilizzo del web, la spesa per la sicurezza venga in genere percepita come un costo puro, assimilabile a una tassa da pagare, mentre meriterebbero un'adeguata valutazione i benefici che potrebbero derivarne.
Alcune fonti stimano i costi relativi all'implementazione della *Ict Security* pari al 2,5-3,5% delle spese complessivamente sostenute dalle grandi aziende e al 5-6% di quelle affrontate da aziende medio piccole (Pmi).
Il principale problema riscontrabile presso queste ultime è che, nel momento in cui si affacciano alla tematica della sicurezza cyber, spesso non sono in grado di stimare correttamente il costo della messa in sicurezza dei propri dispositivi, con il risultato di accantonarne l'esigenza.
Secondo una recente ricerca della Gartner Inc., i costi sostenuti negli Usa per proteggersi sono passati dai 55 miliardi di dollari del 2011 agli 86 stimati per il 2016. Tuttavia, tali sforzi economici potrebbero rivelarsi essenziali per prevenire azioni malevole in grado di procurare danni economici ben superiori.
Considerando sia i rischi ai quali un'organizzazione o un'azienda è esposta sia le attività da intraprendere per il conseguimento di un adeguato livello di sicurezza, i costi complessivi da sostenere possono intendersi ripartiti tra quelli:

– per la prevenzione/mitigazione dei danni da cyber attack, come quelli per l'acquisto di Sw antivirus, di firewall, di filtri anti-spam, di dispositivi per il rilievo d'intrusioni online, per la realizzazione di sistemi conformi ai requisiti di sicurezza sia fisica che informatica, per il back-up dei dati, per le assicurazioni (pur non essendo ancora maturo il settore dei rischi cyber in ambito assicurativo), per le consulenze esterne, per l'indottrinamento ecc.;
– diretti, conseguenti a un attacco, come la sottrazione di denaro e/o di dati sensibili e la necessità di ripristinare la funzionalità dei sistemi;

– indiretti, conseguenti a un attacco, dovuti, ad esempio, a perdita di fiducia nell'online banking, riduzione delle transazioni in forma elettronica, diminuzione della competitività di un'azienda a seguito della compromissione della proprietà intellettuale, diminuzione delle vendite, perdita di reputazione/immagine, perdita di clienti, inattività temporanea dei sistemi oltre alle eventuali perdite occupazionali ecc.

Tra i costi indiretti è possibile includere anche quelli a carico della società quali, ad esempio, i contributi di disoccupazione e quelli connessi all'intervento delle Forze di polizia e alle attività di cui si fanno carico i provider dei servizi in rete, quando coinvolti.
I danni provocati annualmente dal cyber crime sono di difficile valutazione, per varie ragioni: le aziende, per timore di danneggiare la propria immagine, sono spesso restie a condividere le informazioni e segnalare gli attacchi subìti, e non di rado non hanno l'immediata consapevolezza dell'attacco. In molti casi può risultare arduo stimarne l'effettiva consistenza, come nel caso delle perdite connesse al furto di proprietà intellettuale, valutabile solo dopo un lungo arco temporale poiché riconducibile non solo alla perdita del business e dei clienti, ma anche a quella dei posti di lavoro, con implicazioni anche a livello nazionale.
I numerosi report che periodicamente vengono pubblicati da società di consolidata esperienza nel settore della cyber security, scontano il limite di essere basati solo su interviste a campione e adattati su modelli di proiezione. Allo stesso tempo, forniscono un'indicazione sulla gravità del fenomeno e del suo preoccupante trend di crescita. Allo stato attuale, le stime riscontrate quantificano in centinaia di miliardi di dollari l'impatto complessivo della criminalità informatica sull'economia globale.
Scendendo nel particolare, negli ultimi anni si assiste a un preoccupante incremento di reati verso organismi e aziende riconducibili al furto di dati (*Data Breach*). Da uno studio del Ponemon Institute emerge che nel 2013, il 43% dei danni totali stimati per il cyber crime sono attribuibili al furto dei dati, percentuale che ha continuato a crescere negli anni successivi.
Nel documento 2015 *Data Breach Investigation Report*, la Società Verizon stima in 400 milioni di dollari la perdita finanziaria conseguente alla compromissione di 700 milioni di record, quale risultato di un'indagine svolta su un campione di 70 organizzazioni nel mondo. Il settore maggiormente colpito si conferma quello pubblico, seguito da quelli dell'informazione e dei servizi finanziari.
Stime percentuali sui costi associati al *Data Breach*, tuttavia, non sono semplici da effettuare, pur se necessarie per quantificare i risarcimenti delle società assicurative alle vittime del furto. Nel 2014 il Ponemon Institute ha valutato un costo di 201 dollari per ciascun record compromesso, sulla base di dati acquisiti nell'anno (eseguendo semplicemente il rapporto tra perdita economica totale e numero dei record compromessi).

Stime della Società Verizon nel Report 2015 – adottando un modello più complesso e sulla base degli elementi dell'indagine effettuata – portano a una valutazione decrescente del costo per ciascun record compromesso all'aumentare della quantità, e la spesa in media può variare dai 254 dollari, per una perdita di 100 record, a 67 dollari, qualora il numero salga a 1.000, a 4,7 dollari, nel caso di 100.000 ecc.
Per l'Italia, alcune stime riportano che le aziende nazionali hanno subìto nel 2014 – a seguito del furto di dati sensibili – una perdita valutabile in 9 miliardi di dollari, cifra che sale a 14,1 miliardi se a queste si sommano le conseguenze derivanti dalle interruzioni operative dei sistemi informatici.
Passando agli aspetti relativi all'attività criminale in rete, il volume di affari scaturente dal cyber crime è stato recentemente stimato in circa 12 miliardi di dollari annui, pur se la cifra sembra decisamente sottostimata.
Nel mercato nero del cyber crime è facile reperire veri e propri pacchetti, Sw malevoli pronti all'uso e personalizzati sulla base del crimine che s'intende perpetrare, comprensivi di manuali d'istruzione e servizi di assistenza.
A titolo esemplificativo, si riportano alcuni dati aggiornati sulla compravendita di servizi di criminalità informatica.
Nel 2013 un fornitore di servizi 'underground' offriva l'accesso a cospicui gruppi di computer già infettati a prezzi che variavano da 25 dollari per 1.000 pc – dislocati in più parti del globo – a 50 dollari per lo stesso numero di pc localizzati in ambito Ue, fino a raggiungere i 120 dollari per lo stesso quantitativo di apparati, dislocati in territorio americano.
Nel 2015, il mercato dei cosiddetti *Zero Day Exploit*[1] offriva prodotti malevoli a prezzi variabili tra 5.000 dollari e mezzo milione di dollari, in relazione al grado di sofisticazione e della resistenza alla loro identificazione. Nel settembre 2015 sono stati offerti 'premi' da un milione di dollari per sviluppare prodotti capaci di violare la sicurezza dell'innovativo sistema operativo iOS9 per apparecchi mobili della Apple, lanciato nello stesso mese. Ovviamente il valore di uno Zero Day Exploit viene annullato nel momento stesso in cui viene scoperto e vengono implementate le *patche* appositamente sviluppate. Tra gli acquirenti di Zero Day Exploit figurano anche governi e organismi istituzionali per finalità di sicurezza nazionale.
Il prezzo degli account email rubati è crollato significativamente nel corso degli ultimi anni, passando da una somma compresa tra 4 e 30 dollari, nel 2007, a una tra 0,5 e 10 dollari per ben 1.000 account, nel 2015. Diversa è la situazione per i dati relativi alle credit card e alle carte bancomat, i cui prezzi unitari sono rimasti pressoché invariati negli anni, attestandosi tra 0,1 dollari e 20 dollari. A questo proposito, è da evidenziare la grande risonanza prodotta dall'utilizzo fraudolento del malware *BlackPos*, acquistabile nel mercato 'underground' per 1.800 dollari, in grado di catturare i dati delle carte di credito e dei bancomat quando utilizzati per acquisti nei Pos infettati. L'uso malevolo del BlackPos ha determinato, nel 2014, la compromissione di 40 milioni di carte negli Usa, a scapito dei clienti di una nota catena di supermarket.
La qualità dei dati riferiti alle carte di credito e ai bancomat offerti è tuttavia dubbia, in quanto alcuni venditori tentano di smerciare dati obsoleti o rivendere gli stessi più volte. Ciò ha portato alla creazione di veri e propri servizi accessori da commercializzare, come, ad esempio, la garanzia sulla validità delle carte, preventivamente verificata. Alcuni venditori forniscono anche assicurazioni sulla 'freschezza' dei dati e si rendono disponibili a sostituire, in tempi brevissimi, quelli relativi alle carte che dovessero risultare bloccate.
Nel deep web (ovvero la parte sommersa del web in cui sono svolte molte attività, tra cui quelle illegali, cui si accede attraverso reti di anonimizzazione, ad esempio, la diffusissima rete *The Onion Router* – Tor) è possibile reperire anche le offerte seguenti, secondo dati riportati nel Report della Trend Micro del secondo trimestre 2015:

- affitto per sei mesi di *on line banking malware* a prezzi tra 150 e 1.250 dollari;
- attacchi di Ddos a prezzi giornalieri compresi tra 10 e 1.000 dollari;
- carte di credito clonate, da 90 a 210 dollari;
- account rubati per *gaming*, da 10 a 15 dollari;
- malware customizzati, da 12 a 3.500 dollari;
- followers sui social network, da 1 a 12 dollari;
- account rubati per accesso ai cloud, da 5 a 8 dollari;
- servizio di spam a 1 milione di indirizzi e-mail, da 70 a 150 dollari.

Dall'esame delle offerte per attività malevole in rete emerge l'allarmante dato relativo alla generale, rapida diminuzione del livello dei prezzi che, purtroppo, rende i servizi offerti dal cyber crime sempre più facilmente accessibili e alla portata anche di malintenzionati non particolarmente esperti, non in possesso di attrezzature tecniche sofisticate.
Tale fenomeno ha determinato una rapida trasformazione del cyber crime in un'industria con produttori, mercati e fornitori di servizi con vere e proprie soluzioni di *Cyber crime as a Service* (Caas), di *Hacking as a Service* (Haas) o di *Malware as a Service* (Maas). Il malware, così preconfezionato e disponibile a prezzi vantaggiosi, ha contribuito negli ultimi anni all'incremento del numero di attacchi informatici registrati.
La crescente affermazione, inoltre, delle reti di anonimizzazione (in particolare la rete Tor) e delle valute virtuali (in primis, Bitcoin) è divenuta determinante per consentire ai criminali informatici di operare impunemente nei cyber market, sottraendosi alla vigilanza e al controllo delle Forze dell'ordine

1. Con il termine *exploit* s'intende un codice che, sfruttando un bug o una vulnerabilità presente in un programma, porta all'acquisizione di privilegi, con finalità illecite, sul sistema su cui esso è operante. Con la dizione *Zero Day* se ne indica, invece, una appena scoperta o, comunque, non pubblicamente nota, per la quale non sono ancora state sviluppate le relative *patche* o adottate idonee contromisure. Uno *Zero Day Exploit* è in grado di sfruttare tale vulnerabilità prima che la falla nel programma venga riparata.