Corso di
SICUREZZA NEL TRASPORTO E NELLE INFRASTRUTTURE STRATEGICHE

Lezione 5 –Infrastrutture Strategiche ICT

Ivan Rizzolo, Ph.D.
ivan.rizzolo@unipd.it

Gli attacchi informatici indirizzati a enti e imprese stanno diventando sempre più estesi, complessi e frequenti e determinano spesso, oltre a un danno d'immagine dei soggetti colpiti, anche significative ripercussioni economiche. La diffusione di social network, dispositivi mobili, tecnologie wireless e servizi cloud in contesti privati e aziendali ha generato un aumento delle vulnerabilità.

La minaccia informatica costituisce un rischio per l'economia delle aziende che devono adottare iniziative tecniche e organizzative per assicurare la propria operatività in caso di attacchi.

Secondo il rapporto Clusit 20162, cyber crime e spionaggio sono in crescita – in confronto al 2014 – rispettivamente del 30% e del 40%, con predilezione per i settori dei servizi online (+80%), news (+79%), ricerca/educazione (+50%) e infrastrutture strategiche (+150%), con riferimento ad aziende operanti nei settori dell'energia, trasporti, principali fornitori di servizi di Ict e pubbliche amministrazioni.

Per calcolare l'impatto del fenomeno occorre incrociare i dati assoluti con i costi dei danni economici stimati. Una ricerca dell'European Network and Information Security Agency rivela che il costo medio delle violazione cibernetiche subite nel periodo 2005-2010 da un campione di aziende statunitensi è di 2,4 milioni di dollari. Nel 2013, un report del «Wall Street Journal» ha quantificato il costo della criminalità informatica negli Stati Uniti in circa 100 miliardi di dollari, valore che veniva contestato da altre relazioni che lo attestavano su cifre 10 volte superiori

Nel 2015, la compagnia di assicurazione britannica Lloyd ha stimato che gli attacchi informatici, in termini di danni diretti e costi connessi alle attività post-attacco, costano alle imprese fino a 400 miliardi di dollari all'anno.

Secondo diversi studi le principali cause di incidenti informatici alla base dei danni economici subìti dalle imprese sono riconducibili a diversi seguenti aspetti che vanno attentamente studiati e monitorati.

Tali aspetti sono:

- negligenza o errori che hanno portato a una perdita di dati economici confidenziali;
- interruzione dell'attività delle aziende;
- uso improprio o furto di segreti aziendali;
- furto d'informazioni confidenziali di clienti;
- guasti nei sistemi o nei processi che hanno causato una perdita d'informazioni confidenziali;
- danni a infrastrutture ICT

L'analisi dei rapporti e degli studi che a varie latitudini sono pubblicati regolarmente sul tema evidenzia la difficoltà di disporre di un vero e proprio modello che permetta di tracciare un grafico dell'evoluzione del danno economico determinato dagli attacchi cibernetici. A volte, solo spostando il focus dai dati aggregati ai casi specifici di attacchi cibernetici si è in grado di percepire la piena portata del fenomeno. Negli scorsi anni, società delle dimensioni di Target, colosso americano dei supermercati, e di eBay, forse la più diffusa piattaforma mondiale di e-commerce, sono state vittime di attacchi definiti data breach, intrusioni informatiche volte ad acquisire dati sensibili dei rispettivi clienti.

Tali eventi hanno reso evidente che la sottrazione di dataset di informazioni 'immateriali' può determinare drammatiche ricadute negative sul bilancio di imprese multinazionali. Nel caso di Target, per ammissione della società stessa, la sottrazione di dati avvenuta nel 2014 ha determinato perdite complessivamente stimate in un miliardo di dollari. In quello di eBay, il furto di dati di propri utenti ha portato a una riduzione degli obiettivi di vendite annuali per un valore di 200 milioni di dollari. I casi avvenuti illustrano, ove sia necessario, che quello cibernetico è un rischio che può riguardare tutte le imprese, e non solo quelle che operano nel settore Ict. Ogni mercato, anche quello più fisico e materiale, connesso a beni tangibili, è sempre più dipendente da strumenti informatici di elaborazione, conservazione e comunicazione.

L'imprescindibile esigenza di relazioni elettroniche tra i vari attori del mercato proietta ogni impresa oltre il proprio perimetro aziendale, in uno spazio cibernetico e condiviso non sottoposto, per costruzione, a nessuna politica di controllo da parte di un qualche ente supervisore. Ogni entità che opera in tale spazio deve affrontare il tema della difesa dei propri interessi economici, applicando strategie di risk management in tema di cyber security.

Possiamo avere due approcci in tema di difesa delle infrastrutture ICT:

TRADIZIONALE, 'reazione ai tentativi di attacchi noti'. Partendo da una raccolta di 'firme' note, firewall e gateway di posta elettronica analizzano il traffico in entrata, per identificare e bloccare le potenziali minacce; controlli software cercano di individuare elementi malevoli sulle piattaforme interne, mentre gli strumenti di monitoraggio tentano di rilevare e bloccare le minacce in uscita;

PROATTIVO, 'individuazione di comportamenti a rischio'. Utilizzando algoritmi matematici applicati a una grande quantità di dati, è possibile classificare e identificare alcune minacce, prima che queste si trasformino in un attacco, introducendo la possibilità di una difesa proattiva.

Tuttavia, l'impossibilità di annullare completamente i rischi informatici e la crescente difficoltà di dotarsi di strumenti e competenze interne in grado di garantire un costante monitoraggio delle dinamiche evolutive dei diversi piani di attacco, inducono a una riflessione in merito ad altri strumenti per la gestione e il trasferimento del rischio cibernetico. In particolare, le organizzazioni stanno definendo, come ulteriore strategia di risk management, innovativi strumenti di copertura assicurativa per gestire e ridurre alcuni degli effetti derivanti dagli attacchi informatici.

Uno studio della società di riassicurazione Swiss Re prevede che entro il 2025 la copertura del rischio informatico sarà presente in ogni polizza assicurativa nei settori retail, commerciale e industriale.

Tali strumenti, oltre a garantire il trasferimento del rischio cibernetico e la gestione, anche economica, dei danni arrecati da attacchi informatici, determinano ricadute positive, incentivando le organizzazioni ad aumentare gli investimenti verso strumenti di protezione cibernetica al fine di sottoscrivere un'assicurazione o per ridurre il premio, accrescendo il livello complessivo di sicurezza informatica e fornendo, attraverso i premi, un indicatore sulla qualità della protezione cibernetica delle società che sottoscrivono l'assicurazione. Il mercato delle assicurazioni cibernetiche, nato nel 1998 dell'International Computer Security Association, è cresciuto negli anni, anche a seguito dei numerosi attacchi informatici avvenuti in danno di numerose aziende e all'accresciuta consapevolezza che la sottrazione di dati sensibili di un'azienda possa scatenare richieste di risarcimento da parte dei propri clienti

Ad esempio, nel 2003, è stata approvata in California la prima legge che obbliga le società a informare il mercato riguardo a qualunque tipo di attacco informatico subìto con conseguente sottrazione di dati sensibili e, a seguito di tali perdite, a risarcire gli eventuali danni. Successivamente, anche gli altri Stati hanno seguito questo modello, inducendo le aziende americane a ricorrere a forme di cyber insurance in grado di coprire i danni dovuti a: perdita o danneggiamento di risorse digitali aziendali, interruzione di servizi, estorsione cyber, furto di denaro o risorse digitali, violazione della privacy, danno reputazionale e terrorismo cyber.

CYBER INSURANCE E PROCESSI AZIENDALI

Nei contesti nei quali si assiste a una crescente affermazione delle assicurazioni cibernetiche è possibile registrare una serie di ricadute sui processi aziendali come ad esempio all'aumento della consapevolezza da parte del top management aziendale. Rispetto alla percezione che azioni fisiche di manomissione e sabotaggio possano arrecare danni agli interessi di un'azienda, gli attacchi cibernetici sono scarsamente associati al concetto di rischio aziendale. Un mercato dinamico può favorire, tramite processi di formazione e trasferimento di esperienza, la crescita della consapevolezza dell'effettivo rischio cibernetico; crescita del livello di sicurezza interna. Come ogni altra forma di assicurazione, anche quella cibernetica richiede che siano verificate, da parte dell'ente assicuratore, una serie di condizioni di base, che consentano di stimare l'effettivo costo della copertura in atto.

Tale processo virtuoso può essere visto come un percorso circolare, in cui si susseguano le seguenti attività:

- valutazione: l'impresa deve verificare puntualmente le modalità organizzative, logiche e fisiche di difesa del proprio patrimonio informatico, rispetto a possibili attacchi esterni e interni;
- pianificazione: studio delle vulnerabilità identificate al fine di individuare idonee iniziative di annullamento e contrasto delle stesse;
- implementazione: attuazione delle iniziative di contrasto individuate, dal punto di vista organizzativo, di processo e tecnologico;
- manutenzione: dopo ogni iterazione del percorso ciclico, il sistema deve essere mantenuto in efficienza tramite la definizione di policies di comportamento e sistemi automatici di audit.

Ove l'erogatore del servizio assicurativo riesca a definire con l'assicurando un modello simile e vincoli la copertura assicurativa al rispetto di codificate regole di gestione del rischio cibernetico, s'innescherebbe un processo virtuoso che potrebbe condurre alla significativa riduzione degli effetti degli attacchi.

- adozione di standard misurabili e regole di condotta. L'interoperabilità e l'interdipendenza tra le varie realtà che si affacciano sulla rete rendano fondamentale la definizione di standard e regole di condotta di riferimento per tutti gli attori del mercato. In tal senso, anche ai fini dell'effettiva e omogenea valutazione del rischio, gli operatori del settore assicurativo cibernetico potrebbero favorire la convergenza verso pratiche comuni di misura, protezione e controllo;

- definizione di modalità di aggregazione degli incidenti cibernetici. Per la definizione di modelli attuariali impiegabili da parte degli erogatori di servizi assicurativi è fortemente avvertita l'esigenza di disporre di un'ampia e dettagliata casistica d'incidenti informatici. In tal senso, lo sviluppo della specifica linea del mercato assicurativo da rischio cyber potrebbe stimolare la definizione di modalità di raccolta e di analisi, anche aggregata, di ogni elemento utile per migliorare i processi di difesa e le tecniche di valutazione del rischio.

Occorre, comunque, rilevare che esiste ancora una serie di fattori che favorisce lo scetticismo di una parte di aziende nei confronti di questi strumenti di trasferimento del rischio.

In particolare, lo studio citato del Ponemon Institute evidenzia i seguenti elementi percepiti come critici da parte delle imprese intervistate:

- premi assicurativi troppo alti; clausole con esclusioni, restrizioni e rischi difficilmente assicurabili;
- convinzione che i propri sistemi di difesa aziendali siano sufficienti a garantire un'adeguata sicurezza per l'azienda;
- profilo di rischio aziendale troppo elevato;
- valutazione della copertura assicurativa inadeguata sulla base dell'esposizione percepita;
- scarsa percezione del vantaggio di un'assicurazione cyber da parte del management.

CONVERGENZA DEL MERCATO ASSICURATIVO CON ALTRE INIZIATIVE

Come visto, il mercato assicurativo sta muovendo i propri passi e, secondo le regole della domanda e dell'offerta, potrebbe concorrere a un'importante evoluzione del quadro connesso alla gestione del rischio cibernetico, con auspicabili positive ricadute in termini di tutela globale dei mercati digitali. Tale sviluppo sarebbe favorito dalla convergenza tra le esigenze del mercato e le iniziative istituzionali. In tal senso, l'analisi del contesto internazionale evidenzia un'accresciuta consapevolezza da parte delle istituzioni in merito all'esigenza di definire procedure e standard condivisi che, adottati in via mandatoria o volontaria, favoriscano la sottoscrizione, tra i diversi attori pubblici e privati, di un 'contratto sociale' alla base di un fronte unico di difesa dagli attacchi cibernetici.

Negli Stati Uniti, nel febbraio 2015, con l'ordine esecutivo 13691, il presidente Obama ha incaricato il Department of Homeland Security di coordinare lo sviluppo di un sistema volontario di condivisione d'informazioni relative al rischio cibernetico tra attori del settore privato, i quali «must be able to share information related to Cybersecurity risks and incidents and collaborate to respond in as close to real time as possible». Si tratta di un vero e proprio patto sociale che, coinvolgendo un crescente numero di operatori economici, ha l'obiettivo di diffondere la consapevolezza dei rischi connessi agli attacchi in esame. Quest'ultima iniziativa si inserisce nell'ambito di una più ampia strategia che ha i suoi precedenti nell'ordine esecutivo 13636 e nella Presidential Policy Directive-21 del febbraio 2013, relativi al tema della difesa cibernetica delle infrastrutture critiche *(Improving Critical Infrastructure Cybersecurity e Critical Infrastructure Security and Resilience).*

Un elemento innovativo, introdotto dalla citata regolamentazione, è la costituzione di un repository comune per la raccolta dei dati relativi agli incidenti cyber. Tale soluzione potrebbe essere percepita dalle aziende come possibile rischio reputazionale, ove i dati forniti relativi ai propri incidenti informatici non siano opportunamente tutelati. L'orientamento attuale dello scenario americano è quello della costituzione di uno spazio digitale comune, sicuro e anonimizzato, che possa essere condiviso anche con i professionisti di risk management, attuando così la convergenza tra iniziative istituzionali e mercato assicurativo.

Analizzando la situazione europea emerge, in particolare, la proposta di direttiva in merito alla definizione delle misure di sicurezza delle reti e dell'informazione (Network and Information Security) per quello che è stato definito il Mercato Unico Digitale6. La proposta, originariamente presentata dalla commissione Ue all'inizio del 2013 e revisionata nel febbraio 2016, ha l'obiettivo di costituire un ambiente digitale caratterizzato da politiche di sicurezza minime per tutti gli Stati membri dell'Unione allo scopo di garantire uno spazio sicuro per gli scambi digitali. La nuova direttiva, oltre a imporre agli Stati membri l'adozione di misure minime di sicurezza comuni, introduce, nel quadro generale della difesa cibernetica, l'obbligo della notifica degli incidenti a un'Autorità nazionale appositamente istituita.

La notifica degli eventi critici non è un aspetto secondario alla luce dei timori che, come già accennato, le aziende potrebbero nutrire in merito a una possibile sfiducia da parte dei consumatori nel caso in cui i propri incidenti informatici venissero resi pubblici.Fino al 2017 non era ancora evidente il contesto di applicazione della direttiva, in quanto non erano ancora individuate le realtà economiche, definite 'servizi essenziali', che dovrebbero essere sottoposte alle suddette norme. Oggi sono stati definiti tali contesti.

Nel quadro italiano, il Dpcm del 24 gennaio 2013 recante 'indirizzi per la protezione cibernetica e la sicurezza informatica nazionale' pone le basi per un sistema organico di tutela della sicurezza cibernetica nazionale e di protezione delle infrastrutture critiche, promuovendo la collaborazione tra aziende private e pubblica amministrazione, incentivando la condivisione d'informazioni sensibili riguardo agli attacchi subìti.

In ambito accademico, emergono le meritevoli iniziative del Cyber Intelligence and Information Security Center dell'Università 'Sapienza' di Roma e del Cyber Security National Lab del Cini che, nel febbraio 2016, con la collaborazione di un team nazionale di esperti di settore, hanno presentato il Framework nazionale per la Cyber security. Si tratta di uno strumento che, pur mutuando diversi elementi del Framework di cyber security degli Usa, è stato organizzato pensando allo specifico sistema economico italiano, basato soprattutto su piccole e medie imprese: snello e dinamico, utile per inquadrare standard e norme di settore e favorire l'incontro tra il nascente mercato assicurativo cyber e le imprese che, aderendo a tale approccio, possono essere aiutate a misurare il proprio livello di maturità, sia in termini di processi organizzativi che di adeguamenti tecnologici.

CONCLUDENDO

In ultima analisi, anche in presenza di interventi normativi volti a definire il perimetro di un settore così dinamico e in continua evoluzione, resta da verificare se le leggi del mercato svolgeranno una funzione autoregolatrice, in grado di determinare una virtuosa convergenza con le iniziative istituzionali. Tale auspicabile tendenza potrà concorrere ad accrescere la consapevolezza del rischio cibernetico e favorire l'adozione di processi e di metodologie che, amplificando la portata degli interventi dei singoli operatori, nello spirito del principio «aliena pericula cautiones nostrae», accrescano il livello collettivo di difesa, in modo che da un 'patto sociale' siano poste le basi per la sicurezza e la stabilità del cyberspace

domande?

ivan.rizzolo@unipd.it