CRIPPA PISTOCHINI
STUDIO LEGALE

Kroll | A Division of DUFF & PHELPS

Cyber Crime e Cyber Security.

Gli Strumenti a Disposizione delle Aziende per Prevenire e Gestire gli Attacchi Informatici

Media Partner

4CLEGAL

GIURISPRUDENZA PENALE

Indice

Introduzione p. 2

Reati informatici e protezione dell'azienda, di Simone Fraschini p. 3

Il ruolo dei cda nella cyber sicurezza delle aziende, di Marianna Vintiadis p. 4

La nuova geopolitica della cybersecurity, di Giulia Pastorella p. 5

Cyber crime: il ruolo dell'avvocato penalista, di Alessandro Pistochini p. 6

L'attività di indagine a seguito di un cyber attacco, di Cristian Battisello p. 7

Riassunto dell'intervento del Dott. Ciro Santoriello p. 8

Riassunto dell'intervento del Dott. Eugenio Fusco p. 9

Riassunto dell'intervento del Dott. Franco Ghiringhelli p. 10

Conclusione p. 11

Contatti p. 12

Introduzione

Le tematiche del cyber crime e della cyber security sono ormai affare quotidiano per le aziende e, più latamente ancora, per la società. Quasi non passa giorno senza che sulle testate nazionali appaiano notizie relative alle ultime minacce alla sicurezza di chi opera attraverso il Web – ovvero la totalità della business community. E molto spesso le minacce vanno a segno: per chi ne è vittima si tratta solo di minimizzare i danni. In questo contesto, il convegno "Cyber crime e cyber security. Gli strumenti a disposizione delle aziende per prevenire e gestire gli attacchi informatici", organizzato a Milano da Kroll e Studio Legale Crippa Pistochini, giunge con puntualità: il 26 settembre 2019 aziende e avvocati si sono incontrati per fare il punto su alcune delle questioni più urgenti.

Otto relatori si sono avvicendati in due panel di discussione, uno con focus sulla normativa e l'altro su pratiche e strumenti di prevenzione e gestione. Le sintesi di alcuni degli interventi sono raccolte in questo E-book. Alcuni dei concetti espressi prima e durante il Congegno risultano particolarmente efficaci come "istantanee" della situazione: per Alessandro Pistochini, founder dello Studio Legale Crippa-Pistochini, non è in discussione che l'ambiente digitale oggi sia tendenzialmente meno sicuro che nel recente passato, perché le strategie di attacco informatico si evolvono più velocemente di quelle di difesa; Giulia Pastorella, Cybersecurity and Data Policy Lead ad HP, apre il suo intervento sostenendo che "nell'ambito della cyber security la questione chiave non è 'se' si sarà attaccati, ma 'quando'"; secondo Marianna Vintiadis di Kroll, la cyber security non è solo un fatto di informatica, ma anche di cultura – sia da parte dei vertici delle aziende che dei loro clienti. Tutti richiami forti e autorevoli, questi, non solo a una lettura attenta dei paper che seguono, ma anche alla necessità di ulteriori occasioni di discussione in futuro.

Reati informatici e protezione dell'azienda

Nel mondo dell'azienda c'è molto da fare e lo sappiamo, ce lo dicono i dati che leggiamo ogni giorno. Abbiamo letto e continuiamo a leggere di attacchi e addirittura di epidemie di attacchi. Vediamo grandi aziende sotto tiro oltre ai privati. Ovunque vi sia tecnologia c'è il tema della cybersecurity. L'Internet of Things porta con sé, con gli oggetti intelligenti connessi tra di loro, una grande utilità ma va usato bene.
Ognuno di noi deve essere consapevole di quanto la rete sia pericolosa, dei rischi connessi e di come affrontarli. Infatti, nella maggior parte dei casi, l'attacco informatico ha successo per la debolezza del fattore umano. I danni conseguenti possono essere ingenti.
Sul tema della cybersecurity si è comunque sviluppata molto in taluni ambienti aziendali, soprattutto multinazionali, la consapevolezza sul problema e, nelle organizzazioni più virtuose, sono in atto da tempo azioni importanti per contrastare il fenomeno. Azioni a volte di natura tecnologica, a volte mirate ad incidere sui comportamenti delle persone. Si stima una significativa riduzione del rischio connesso agli attacchi informatici quando si fornisce adeguato training alle persone su temi ricorrenti quali ad esempio il phishing, il trasferimento soldi e gli aggiornamenti software.
Per quanto riguarda la normativa in vigore, esiste certamente un importante corpo normativo volto a combattere la cyber-criminalità e a costruire un sistema di diritto penale dell'informatica al passo con i tempi. È uno sforzo continuo (e a livello UE continua ad essere una priorità) che, ovviamente, non è immune da alcuni profili critici.
Va comunque menzionato in questo contesto il GDPR perché con questo regolamento europeo la privacy è trattata anche e soprattutto come messa in sicurezza dei dati. Il tutto rafforzato dalla norma che impone di notificare il data breach. Il GDPR è importante perché aumenta la sensibilità sul tema. Le aziende sono state chiamate a migliorare la sicurezza.
Se poi vediamo le altre fonti internazionali, si tratta di fare riferimento, in particolare, alle iniziative a livello di Nazioni Unite, di Unione Europea, Consiglio d'Europa, Stati e Stati Membri. La Convenzione Cybercrime del Consiglio d'Europa è un punto di riferimento internazionale nella lotta al cybercrime.
In questa situazione credo rimanga un nodo importante la cooperazione, in larga misura esistente ed efficace, tra autorità competenti degli Stati Membri e le agenzie e organismi dell'Unione Europea e non. Inoltre, le differenze ancora esistenti nel diritto degli Stati Membri possono ostacolare la lotta contro pericolose forme di criminalità e suggeriscono ulteriori azioni tempestive per il riavvicinamento delle legislazioni.
Dato il carattere cross-border del cybercrime, infatti, la collaborazione internazionale – nonostante le grosse difficoltà di identificare gli autori degli attacchi - e l'armonizzazione delle legislazioni è il terreno dove la partita si svolge.

Simone Fraschini
Of Counsel, Studio Crippa Pistochini

Il ruolo dei Cda nella cyber sicurezza delle aziende

Gli attacchi informatici sono all'ordine del giorno e comportano quasi sempre importanti danni economici e reputazionali per le aziende che li subiscono.
Il tema della cyber security è quindi fondamentale, così come lo è comprendere quali sono gli strumenti a disposizione delle imprese per prevenire e gestire gli attacchi informatici, oltre che avere chiaro prima che questo accada cosa si debba fare quando l'attacco è avvenuto.
La maggior parte delle imprese che incontriamo come Kroll pensa che il tema della cyber security sia di competenza esclusivamente del reparto IT. Relegano dunque il problema al dipartimento tecnico, pensando che per risolverlo sia sufficiente installare uno o più software, spesso costosi. In realtà il problema è di altra natura e riguarda prima di tutto un ambito sul quale il software può fare molto poco: il comportamento umano.
Un esempio banale è quello della password. Nonostante tutti ormai siamo consapevoli delle regole base alle quali dovremmo attenerci per usare questo strumento, continuiamo a usarne di troppo semplici, oppure a custodirle, in maniera poco sicura, come su un post-it attaccato allo schermo del computer, senza modificarle mai.
È importante tenere presente che il 75% degli attacchi informatici che vanno a buon fine godono della collaborazione colposa o dolosa di un insider.
È dunque necessaria con urgenza una formazione interna nelle aziende, che renda consapevole il personale dei comportamenti a rischio e li prevenga. In Italia, invece, tipicamente, questa consapevolezza arriva solo dopo il primo attacco. E' molto difficile trovare aziende che si sono formate e che hanno messo in atto delle difese preventive.
D'altra parte un approccio di questo tipo presuppone una decisione del vertice aziendale che ha valutato il grado di rischio dell'azienda e ha stabilito come intende affrontarlo e quali misure mettere in campo.
I Cda delle aziende italiane, però, raramente includono figure con competenze tecniche in grado di valutare questi fattori e di porre la giusta attenzione alla cyber security.
Oggi, però, tutto questo è indispensabile anche in settori in cui la tecnologia o i dati non rappresentano il core business. Gli attacchi informatici, infatti, non riguardano più solo il furto di dati o elaborate manomissioni, ma anche aspetti più semplici della nostra vita quotidiana in cui la tecnologia è entrata ed entrerà sempre con maggiore forza con l'"Internet of Things": un frigorifero intelligente il cui chip viene hackerato e che non conserva adeguatamente il cibo rappresenta un problema reputazionale per l'azienda produttrice che arriva in modo diretto e potente al suo cliente, causandogli un danno e un fastidio del quale difficilmente si dimenticherà.
In questa fase di sviluppo dell'Internet of Things, troppo spesso le imprese sottovalutano che l'introduzione di sistemi informativi nei propri prodotti proietta l'impresa stessa in un mondo cyber di cui non è esperta e del quale non sempre è in grado di valutare le implicazioni complessive e il potenziale di rischio.

Marianna Vintiadis
Head of Southern Europe, Kroll

La nuova geopolitica della cybersecurity

Nell'ambito della cyber security la questione chiave non è "se" si sara' attaccati, ma "quando". Il mondo cyber è uno scenario di tensioni sempre più forti tra coloro che vogliono utilizzare la ricchezza immateriale del digitale per crescere – siano essi governi, aziende o istituti di ricerca – e coloro che attraverso mezzi illeciti vogliono approfittare delle debolezze del Sistema. HP, che produce dispositivi su cui sempre più si producono e consumano i dati che sono alla base di questa ricchezza, è altamente consapevole dei rischi legati alla nuova economia immateriale. Il nostro approccio a riguardo è a 360 gradi, sia internamente nei processi aziendali sia per quanto riguarda i nostri prodotti e la sicurezza dei dati dei nostri clienti.

Internamente HP segue procedimenti molto rigorosi per la sicurezza della propria supply chain e per la segnalazione di eventuali vulnerabilità informatiche per reagire tempestivamente. I prodotti HP sul mercato – PC, stampanti 2D e 3D – hanno elevati standard di sicurezza, leader nelle loro categorie. I Laboratori di Ricerca & Sviluppo HP collaborano con enti governativi, standards bodies e associazioni di settore per garantire la priorità dei temi di cyber security nell'industria informatica internazionale, per esempio attraverso la fondazione del Trusted Computing Group.

Inoltre, nel contesto geopolitico attuale, si rivela anche importante l'analisi del ruolo sempre più rilevante della cyber security nella definizione di strategie di sicurezza nazionali. Da una parte la protezione della sovranità digitale nazionale sta diventando pratica comune per gli attori statali, che si rendono conto della criticità di mantenere i dati dei propri cittadini e delle proprie aziende al sicuro.

Dall'altra parte, dietro alla tema della protezione cibernetica spesso si nascondono barriere non tariffarie Dall'altra parte, dietro alla tema della protezione cibernetica spesso si nascondono barriere non tariffarie di tipo protezionista che prendono forme di standard e leggi di cyber security.

Per queste ragioni il cyber crime in tutte le sue sfaccettature deve essere considerato come un tema centrale sia per le aziende che per i governi. Per HP la risposta a questa minaccia deve essere una cyber security intesa come cyber-"resilienza", ovvero la capacità dei sempre più numerosi dispositivi connessi non solo di incorporare robuste funzionalità di protezione, ma anche di identificare gli attacchi avvenuti ed eseguire attività di correzione automatica in seguito alle violazioni.di tipo protezionista che prendono forme di standard e leggi di cyber security.

Per queste ragioni il cyber crime in tutte le sue sfaccettature deve essere considerato come un tema centrale sia per le aziende che per i governi. Per HP la risposta a questa minaccia deve essere una cyber security intesa come cyber-"resilienza", ovvero la capacità dei sempre più numerosi dispositivi connessi non solo di incorporare robuste funzionalità di protezione, ma anche di identificare gli attacchi avvenuti ed eseguire attività di correzione automatica in seguito alle violazioni.

Giulia Pastorella

Cybersecurity and Data Policy Lead, HP

Government Relations – Global Strategy Program

Cyber crime: il ruolo dell'avvocato penalista

Oggigiorno le realtà aziendali costituiscono un terreno assai fertile per la perpetrazione di numerose fattispecie di reato che attengono ai c.d. Cyber Crimes.
Con riguardo a possibili fattispecie di reato che possono offendere l'impresa, potremmo immaginarci un macro-insieme "bene aziendale" e annoverare una serie di sottoinsiemi costituenti diverse tipologie di reato che sono state individuate dal legislatore per "proteggere" differenti aspetti della realtà aziendale. Troviamo, così, categorie di reato che sono volte a reprimere condotte che violano la riservatezza informatica della società, reati che tutelano l'integrità dei dati, dei programmi e dei sistemi informatici, reati contro l'onorabilità dell'impresa e reati contro la fede pubblica.
In tema di Cyber Crimes, due sono le situazioni che possono coinvolgere una azienda nelle quali può entrare in gioco l'avvocato penalista: la prima si verifica allorchè l'azienda sia vittima di un reato informatico da parte di un hacker; la seconda, invece, interviene nel momento in cui si ha contezza della possibilità che un proprio dipendente abbia commesso un reato informatico.
Tra le diverse attività che possono essere svolte in questa fase a tutela dell'azienda, rientrano le indagini difensive e le investigazioni interne (cd. internal investigations), che si compiono attraverso il coinvolgimento di una serie di soggetti diversi: dalla azienda ai consulenti informatici, dai legali interni agli avvocati esterni, sino alla polizia giudiziaria e alla Procura nel momento in cui viene instaurato il procedimento penale.
Con riguardo alle indagini difensive "ordinarie", numerose e ampie sono le facoltà che il nostro ordinamento riconosce al difensore incaricato: dagli accessi ai luoghi e alla documentazione, alla nomina di consulenti tecnici, sino al compimento di accertamenti tecnici non ripetibili.
In un'ottica esclusivamente "precauzionale", invece, assumono peculiare rilevanza le cosiddette indagini difensive "preventive", in quanto, consentendo una rapida attivazione nella ricerca della prova a fronte della conoscenza di essere stati vittima di un reato informatico, impediscono la possibile perdita di elementi che il difensore potrebbe trovarsi nella necessità di reperire in seguito al formale avvio di un procedimento penale.
Da qui l'importanza della nomina di un legale che possa essere in grado sin da subito di svolgere attività investigativa preventiva eventualmente con l'ausilio di un consulente tecnico che, agendo nel rispetto delle best practices dell'attività di computer forensics, garantisca la corretta cristallizzazione ed analisi delle fonti di prova.

Alessandro Pistochini

Founder, Studio Legale Crippa Pistochini

L’attività di indagine a seguito di un cyber attacco

L’attività di indagine a seguito di un cyber attacco è un processo complesso che richiede fin da subito una capacità di intervento immediata ed il coinvolgimento di personale altamente specializzato; a riguardo, è importante sottolineare che il team investigativo non è composto solamente da persone con conoscenze informatiche, ma è un mix di competenza anche forensic e di business intelligence.
Infatti, nel caso di un’azienda che ha subito un attacco, il Consiglio di Amministrazione chiede di ricostruire l’accaduto con l’obiettivo di: (i) definire la sequenza degli eventi, (ii) accertare la causa della compromissione, (iii) identificare i soggetti coinvolti (siano essi interni ed esterni all’azienda), (v) accertare i ruoli e le responsabilità; (v) escludere la possibilità che l’attacco sia stato posto in essere con il contributo di personale della società; (vi) verificare l’esistenza di un data-breach che debba essere segnalato alle autorità competenti.
L’attività investigativa è sicuramente agevolata se la società che ha subito l’attacco ha un piano di azione e di crisi in situazioni di attacco informatico.
Il processo investigativo viene adattato sulla base della tipologia di attacco, della dimensione aziendale, della territorialità oppure extraterritorialità dell’evento, delle persone e caratteristiche delle società coinvolte.
Prendendo a puro titolo di esempio un attacco phishing che ha l’obiettivo di ottenere, rubandole, le credenziali di accesso al sistema informatico/account di posta elettronica di un terzo soggetto, l’attività investigativa che viene posta in essere prevede quantomeno i seguenti processi:
l’identificazione degli accessi effettuati da chi ha perpetrato l’attacco e della causa principale della compromissione del sistema; per esempio, nella fattispecie del “phishing attack” si fa riferimento alla mail inviata alla vittima e di come quest’ultima abbia fornito le password di accesso;
la ricostruzione delle attività condotte da chi ha effettuato l’attacco all'interno del sistema informatico della società. Riprendendo il nostro esempio, vengono ricostruite e tracciate tutte le mail lette, create, inviate, ricevute, archiviate da chi ha posto in essere l’attacco, nonché vengono identificati tutti i documenti cipiati, aperti e letti; la ricerca di ulteriori compromissioni all’interno del sistema;
un attività di intervista al personale della società che risulta coinvolto nell’ambito dell’attacco tra cui: (i) la vittima della compromissione; (ii) altro personale (a titolo di esempio, nel caso di trasferimento di denaro, oppure di creazione di anagrafiche fornitori, viene intervistato il personale dello staff ha posto in essere specifiche attività operative che possono avere agevolato l’attacco) e (iii) personale della divisione Information Technology e Security. Le interviste hanno l’obiettivo di comprendere e ricostruire fattualmente le dinamiche dell’attacco. In tale contesto, è importante la collaborazione con la struttura di internal audit che conosce le procedure aziendali e può supportare il team investigativo nell’individuare possibili violazioni;
la raccolta di informazioni su eventuali controparti terze coinvolte che il più delle volte risiedono in paesi esteri;
al termine dell’investigazione viene quindi predisposto un rapporto che riepiloga le risultanze delle attività svolte.

Cristian Battistello

Associate Managing Director, Kroll

Riassunto dell'intervento del dott. Ciro Santoriello

Il dott. **Ciro Santoriello** (Sostituto Procuratore presso il Tribunale di Torino) è intervenuto nella prima sessione del convegno illustrando la relazione tra la normativa in tema di responsabilità da reato degli enti ex D. Lgs. 231/2001 e i reati informatici soffermandosi, in particolare, sulle ragioni che dovrebbero sollecitare l'impresa a conformare il suo sistema informatico ai dettami rispondenti alla disciplina di cui al citato decreto legislativo.

Il dott. Santoriello ha evidenziato come il rispetto della normativa di cui al D. Lgs. 231/2001, ben lungi dal dover essere considerato un mero adempimento ad un comando normativo, risponda ad evidenti interessi aziendali quali, su tutti, quelli dell'ottimizzazione dei sistemi di controllo interni e del perfezionamento delle procedure interne.

Proprio con riferimento all'importanza del rispetto delle procedure interne in tema di cyber crime e cyber security, il Pubblico Ministero si è soffermato sull'importanza di una loro corretta perimetrazione da parte delle aziende, il più possibile calata nella realtà aziendale di cui si discute: se, da un lato, una procedura troppo stringente rischia di non essere eseguita correttamente dai propri dipendenti, dall'altro, una procedura che non sia sufficientemente precisa rischia di non essere percepita come efficace e, quindi, di essere "bypassata" in alcune sue fasi.

Il dott. Santoriello ha accennato, infine, all'importanza della formazione in tema di responsabilità da reato degli enti ex D. Lgs. 231/2001 soffermandosi, in particolare, sulla necessità che sia affidata a professionisti esperti in tema di cyber security.

Ciro Santoriello

Sostituto Procuratore presso il Tribunale di Torino

Riassunto dell'intervento del dott. Eugenio Fusco

Il dott. **Eugenio Fusco** (Procuratore Aggiunto presso il Tribunale di Milano, ove ricopre il ruolo di coordinatore del Dipartimento "Frodi, tutela dei consumatori e reati informatici") è intervenuto nella seconda sessione del convegno – dedicata alla gestione degli attacchi informatici – soffermandosi sul tema relativo alle indagini da parte della Procura e della polizia giudiziaria.

Il dott. Fusco ha evidenziato, anzitutto, come l'evoluzione tecnologica abbia stravolto (e stia stravolgendo) il mondo del diritto penale, consentendo una realizzazione in forma più agevolata rispetto a prima – e spesso con conseguenze ben più gravi – pressoché di qualunque reato previsto dal nostro ordinamento (dal cd. "phishing" alle frodi informatiche, dalle sostituzioni di persona al recentissimo delitto di "revenge porn").

Per cercare di contrastare questo fenomeno ormai sempre più dilagante (e foriero di rilevanti danni economici per le aziende), in molte procure sono stati creati appositi dipartimenti dedicati al contrasto ai crimini informatici e, a livello europeo, si stanno intensificando gli accordi tra le autorità giudiziarie dei diversi paesi per consentire uno scambio di informazioni più rapido, senza la necessità di dover ricorrere a rogatorie. Uno dei problemi che rendendo più difficile l'accertamento di questi reati, infatti, è dato dal fatto che la condotta passa spesso (se non sempre) attraverso diversi paesi e, conseguentemente, diverse giurisdizioni, spesso per niente collaborative.

Altro aspetto che complica lo svolgimento delle indagini è dato dalla difficoltà di "seguire le tracce" lasciate dai criminali informatici, motivo per cui il Pubblico Ministero ha evidenziato l'importanza di una denuncia in tempi rapidi da parte dell'azienda ogni qualvolta vi sia evidenza di aver subito un attacco informatico: solo così – ha affermato il dott. Fusco – si può consentire alla autorità giudiziaria di intervenire e raccogliere elementi utili alle indagini.

Eugenio Fusco

Procuratore Aggiunto presso il Tribunale di Milano

Riassunto dell'intervento del dott. Franco Ghiringhelli

Il Dr Ghiringhelli ha innanzitutto descritto quelli che, sulla base della propria esperienza, possono essere considerati i migliori strumenti a presidio della cyber security di un grande gruppo che opera a livello internazionale. Un approccio integrato tra sistema di governance, inclusivo del Codice Etico e del Modello 231, sistema procedurale e sistemi informativi, l'implementazione di un piano di crisis management ed il costante monitoraggio delle possibili minacce digitali sono le misure necessarie e imprescindibili per arginare questa minaccia, che sta evolvendo verso forme sempre più variabili e sofisticate.

In aggiunta, a necessario completamento di tali presidi, occorre riconoscere, per poterlo adeguatamente gestire e contenere, il fattore di rischio più grande, ovvero quello umano. La maggior parte degli attacchi a cui stiamo assistendo fanno leva infatti sull'ingegneria sociale sfruttando - con meccanismi sempre più imprevedibili e variabili - la vulnerabilità psicologica e comportamentale delle vittime, nei confronti delle quali i controlli ed il sopraccitato sistema integrato non sono sufficienti. E' quindi estremamente importante implementare attività di formazione e sensibilizzazione continue per accrescere la consapevolezza del rischio al quale non solo i dipendenti, ma anche i collaboratori ed i partner/fornitori, che sono parte integrante dei processi aziendali, sono esposti.

Franco Ghiringhelli

Human Resources, Organization and ICT Senior Vice President del Gruppo Maire Tecnimont

Conclusione

I professionisti che si sono alternati nelle due sessioni del convegno hanno messo in luce – ciascuno nel proprio ambito di competenza – ciò che può essere fatto concretamente dalle aziende per prevenire e gestire gli attacchi informatici.
Se è vero che più del 50% delle aziende italiane hanno subito attacchi informatici e che sono stati stimati in 5.200 miliardi di dollari i costi che gli attacchi informatici potrebbero provocare alle aziende nei prossimi cinque anni (tant'è che, come si è soliti affermare in questo campo, la domanda non è «se si subirà un attacco informatico», ma semmai «quando lo si subirà»), ogni azienda deve necessariamente fare i conti con questo problema e munirsi delle necessarie contromisure.
Queste passano attraverso una corretta formazione interna e in una rigida standardizzazione delle procedure e dei controlli interni, anche attraverso la creazione e il potenziamento di appositi dipartimenti interni all'azienda dedicati alla sicurezza informatica (per quanto riguarda la fase di prevenzione degli attacchi informatici) e nella predisposizione di una procedura di gestione delle emergenze da attivare non appena si prenda contezza di aver subito un attacco informatico (per quanto riguarda la fase di gestione deli attacchi informatici).
Tanto nella prima quanto nella seconda fase, è assolutamente fondamentale l'apporto dei consulenti esterni – società di consulenza ed investigazione, studi legali e consulenti informatici – che possano fornire alle aziende il necessario supporto per gestire la situazione eventualmente rapportandosi con l'autorità giudiziaria.

Contatti

Per approfondimenti:

Studio Legale Crippa Pistochini

Website: www.crippapistochini.it
Tel.: +39 02 5412 3627
E-mail: studio@crippapistochini.it

Kroll

Website: www.kroll.com
Tel.: +39 02 8699 8088
E-mail: info.milan@kroll.com