Digital Crimes e Modello 231: gestione dei rischi (Information Security Policy), presìdi di controllo e formazione interna

Premessa

L’avvento della digitalizzazione ha modificato profondamente il mondo aziendale. L’inarrestabile diffusione di internet e delle nuove tecnologie ha imposto alle aziende un grado sempre più elevato di informatizzazione aziendale. Questo processo, volto a, condizionare l’intera dimensione dell’impresa all’utilizzo di strumenti e sistemi informatici, è ormai divenuto condizione imprescindibile per ottimizzare l’organizzazione di diversi processi interni.

Il ricorso all’informatica ed al mondo virtuale rappresenta però un’“arma a doppio taglio” in quanto ha comportato non solo diversi effetti positivi, legati all’innegabile miglioramento del funzionamento di diverse aree di attività, ma anche un significativo innalzamento del rischio di commissione di comportamenti illeciti all’interno del contesto aziendale, dovuto al fatto che il sistema di protezione cyber non è sempre implementato alla stessa velocità, frequenza e grado rispetto all’informatizzazione dei processi produttivi.

Sebbene in maniera meno sistematica di quanto avrebbe meritato la materia, il legislatore ha previsto un compendio di norme volte a tutelare penalmente le condotte fraudolente nel settore informatico, con l’introduzione dei c.d. *digital crimes* (L. n. 48/2008).

A questa responsabilità – tipicamente personale – è stata opportunamente aggiunta quella amministrativa derivante da reato con l'inserimento dei delitti informatici nel novero dei reati-presupposto previsti ex D.Lgs. 231/2001 (art. 24 bis).

I reati informatici inseriti nel Decreto dalla novella normativa si possono distinguere in tre gruppi:

1. il primo gruppo comprende i reati che puniscono il danneggiamento di *hardware*, di *software* e di dati (artt. 615 ter, 617 quater, 617 quinquies, 635 bis, 635 ter, 635 quater e 635 quinquies c.p.): viene punito l'accesso abusivo ad un sistema e l'intercettazione o l'interruzione di dati compiuti attraverso l'installazione di appositi *software* o *hardware* e viene punita come aggravante la commissione degli stessi reati in sistemi informatici di pubblica utilità;
2. il secondo gruppo di reati è costituito dai reati che puniscono la detenzione e la diffusione di *software* e/o di attrezzature informatiche atte a consentire la commissione dei reati di cui alla precedente lett. a) (artt. 615 quater e 615 quinquies c.p.);
3. il terzo gruppo di reati comprende i reati con cui viene punita la violazione dell'integrità dei documenti informatici e della loro gestione attraverso la falsificazione di firma digitale (artt. 491 bis e 640 quinquies c.p.).

Tali reati sono spesso interconnessi tra loro e la prevenzione degli stessi è particolarmente difficile e complessa, soprattutto perché non necessitano di elaborati processi di gestione/organizzazione aziendale, né del coinvolgimento di un elevato numero di soggetti, atteso che, solitamente, l'attività fraudolenta è perpetrata da un singolo soggetto che sfrutta le proprie conoscenze informatiche e la larghezza delle maglie della rete di protezione cibernetica aziendale.

Il massiccio trasferimento della criminalità *on-line* ha fatto

sì che ormai i *digital crimes* non costituiscano più solamente una minaccia interna al perimetro aziendale, ma colpiscano anche – anzi soprattutto – dall'esterno le società, attraverso attacchi *cyber* e *data breach*. Con il proliferare di episodi di violazione dei sistemi informativi aziendali perpetrati da parte di *hacker* anonimi sempre più esperti, i vertici aziendali hanno dovuto prendere coscienza della necessità di provvedere non solo alla difesa della rete aziendale interna, ma anche ad un'azione di tutela rivolta verso l'esterno.

L'occasione privilegiata per attuare questa protezione a doppio raggio d'azione dell'azienda si è rivelata proprio la redazione o l'implementazione del Modello adottato ai sensi del D.Lgs. 231/01.

Cybersecurity e gestione dei rischi di commissione di reati informatici

Nell'ambito dell'attività di predisposizione del Modello 231, la gestione dei rischi legati al mondo dell'informatica si fonda principalmente su tre pilastri:

1. Prevenzione
2. Controlli
3. Formazione

Il primo pilastro viene normalmente attuato attraverso la previsione di specifiche misure di sicurezza volte a ridurre la possibilità che vengano commessi reati all'interno della rete aziendale; il secondo attraverso l'introduzione di presìdi di controllo *ad hoc*, finalizzati a supervisionare la gestione ed il funzionamento dei diversi ambiti aziendali condizionati dall'uso di *internet* e di *device* tecnologici e l'ultimo consiste nella diffusione di una cultura aziendale in materia informatica attraverso la formazione del personale e la responsabilizzazione di alcune figure.

A livello di **prevenzione**, è importante che ogni azienda si

doti di apposite regole comportamentali e di sicurezza per gli utenti sia interni che esterni.

Quanto agli utenti interni risulta fondamentale innanzitutto definire i livelli di accesso in base alla confidenzialità delle informazioni ed alla responsabilità di ogni soggetto. Si tratta, in particolare, di adottare una *policy* di sicurezza del sistema informatico (*ICS policy*), che regolamenti in maniera strutturata l'accesso ai documenti ed alle informazioni aziendali ed il loro utilizzo. Al fine di garantire la correttezza e la sicurezza dell'operatività dei sistemi informativi interni, ogni azienda dovrebbe provvedere all'adozione di un'*ICS policy* inserendovi quanto meno le seguenti previsioni:

- la protezione da *software* pericoloso ricorrendo all'uso di antivirus ed al loro monitoraggio/aggiornamento costante;
- i *back-up* periodici delle informazioni in possesso all'azienda e dei *software* dalla stessa utilizzati;
- la protezione dello scambio di informazioni attraverso l'uso di tutti i tipi di strumenti per la comunicazione anche con terzi (ad esempio regolamentando l'uso di dispositivi removibili quali USB);
- la tracciatura delle attività eseguite sulle applicazioni, sui sistemi e sulle reti e la protezione di tali informazioni contro accessi non autorizzati;
- la verifica periodica dei *log* che registrano le attività degli utilizzatori, le eccezioni e gli eventi concernenti la sicurezza;
- l'accesso ai servizi di rete esclusivamente da parte degli utenti che sono stati specificatamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete;
- la rivisitazione dei diritti di accesso agli utenti ad intervalli di tempo predefiniti ed in caso di cambiamento del rapporto che attribuiva loro il diritto

di accesso;
- il rinnovo periodico delle credenziali degli utenti;
- la segmentazione della rete affinché sia possibile assicurare che le connessioni e i flussi di informazioni non violino le norme di controllo degli accessi delle applicazioni aziendali;
- la chiusura di sessioni inattive dopo un predefinito periodo di tempo;
- la custodia dei dispostivi di memorizzazione (quali, ad esempio, chiavi USB, CD, hard disk esterni, ecc.) e l'adozione di regole di *clear screen* per gli elaboratori utilizzati;
- l'implementazione e lo sviluppo sull'uso dei controlli crittografici per la protezione delle informazioni e sui meccanismi di gestione delle chiavi crittografiche;
- l'esecuzione periodica di *test* di sicurezza informatica come presidio contro le minacce *cyber*.

Con riferimento ai casi di accesso da parte di utenti esterni, per tutelare la realtà aziendale risulta utile prevedere ad esempio la richiesta di abilitazione preventiva da parte del responsabile della funzione aziendale competente con la quale la terza parte dovrà interagire, la costruzione di una rete per soggetti terzi diversa da quella accessibile al personale aziendale, oltre che applicare – come detto – le procedure di sicurezza adottate con riferimento allo scambio di informazioni tramite strumenti di comunicazione quali USB o CD-ROM.

Per quanto riguarda i **controlli**, l'impresa deve provvedere a nominare un amministratore di sistema (c.d. S.I.A.), un esperto di IT che si occupi del monitoraggio dei sistemi informativi aziendali e che risponda a tutte le segnalazioni provenienti dalle varie funzioni. Inoltre, risultano fondamentali la programmazione di *audit* interni da eseguire periodicamente (anche mediante attività di penetrazione ed ingegneria sociale) ed il controllo costante sui cambiamenti

apportati agli elaboratori e ai sistemi.

Tutti gli strumenti e le misure sopra indicate sono estremamente utili anche nella tutela dagli attacchi esterni.

L'implementazione del Modello 231 ad oggi può infatti rivelarsi uno strumento prezioso ed efficace anche per tutelare l'azienda da eventuali minacce *cyber* provenienti dall'esterno. Negli ultimi anni ormai sono diventati sempre più frequenti i reati (anche non ricompresi nell'elencazione di cui all'art. 24 bis) commessi nel *cyberspace*, i quali provocano gravissime conseguenze alle aziende sia a livello economico che a livello strutturale e di *web reputation*.

Basti pensare ai frequentissimi casi di *phishing* o di *cyber-laundering* oppure ancora di diffamazione *on-line*. Si tratta di reati (come detto, anche non rientranti nell'elenco ex D.Lgs. 231/01) perpetrati da autori che il più delle volte restano anonimi e sono collocati in Paesi esteri difficilmente rintracciabili. Tali soggetti conoscono perfettamente i punti deboli a livello tecnico-informatico delle loro principali vittime perciò li sfruttano per agire illecitamente causando considerevoli danni reputazionali ed economici.

L'incremento delle misure di prevenzione e controllo contenute nel Modello anche con strumenti di contrasto a tali fenomeni provenienti dall'esterno, si rivela sempre più vantaggioso per le aziende che vogliono una tutela a 360 gradi e, quindi, una continuità della loro attività. È importante, dunque, che le aziende non solo prevengano, ma anche costituiscano un sistema di *disaster recovery* per il trattamento degli incidenti e delle anomalie di qualsiasi tipo relativi alla sicurezza informatica. A questo proposito risulta estremamente utile l'introduzione di meccanismi di comunicazione immediata tramite *alert* automatici che segnalino eventuali episodi di *hackeraggio* e di appropriati canali gestionali per la comunicazione immediata degli incidenti e dei problemi oltre che l'analisi periodica di tutti gli incidenti singoli e

ricorrenti e l'individuazione della rispettiva *rootcause* in modo da poter creare una rete di prevenzione-protezione sempre più ampia e sofisticata.

Un ulteriore strumento di tutela a livello informatico per il mondo aziendale è poi la certificazione ISO/IEC 27001:2017. Dal momento che l'informazione è un bene che aggiunge valore all'impresa, e che ormai la maggior parte delle informazioni aziendali sono archiviate su supporti informatici, ogni organizzazione deve essere in grado di garantire la sicurezza dei propri dati, in un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono continuamente in crescita. L'obiettivo del nuovo standard ISO 27001:2017 è proprio la protezione dei dati e delle informazioni aziendali da minacce di qualsiasi tipo, allo scopo di assicurarne l'integrità, la riservatezza e la disponibilità e fornire alle società i requisiti per adottare un adeguato sistema di gestione della sicurezza delle informazioni (SGSI) finalizzato ad una gestione efficace e corretta dei dati sensibili dell'azienda.

Da ultimo, occorre sottolineare come per una tutela efficace delle aziende in tema *digita/cyber crime* oltre ad un'azione specifica sul piano tecnico-procedurale nell'ambito della sicurezza informatica, è indispensabile diffondere una cultura aziendale in tal senso. Sia l'attuazione effettiva del Modello 231 sia il contrasto agli attacchi *hacker* possono essere infatti più agevolmente realizzati se affiancati da un'intensa attività di **formazione** del personale aziendale.

Avere dipendenti e figure professionali specifiche che sappiano gestire eventuali segnalazioni di anomalie interne nonché riconoscere ed evitare le minacce informatiche della rete è fondamentale per proteggere l'impresa. La sensibilizzazione di tutto il personale e la responsabilizzazione di specifiche figure – referenti per la sicurezza informatica – favoriscono da un lato una migliore collaborazione nella gestione di dati ed informazioni interni

all’azienda e dall’altro una maggiore tempestività d’intervento in caso di evento sinistro, sia esso accidentale o fraudolento.

Articolo a cura di **Avv. Chiara Langé** e **Avv. Francesco Rubino**

L’articolo Digital Crimes e Modello 231: gestione dei rischi (Information Security Policy), presìdi di controllo e formazione interna proviene da ICT Security Magazine.

https://www.ictsecuritymagazine.com/articoli/digital-crimes-e-modello-231-gestione-dei-rischi-information-security-policy-presidi-di-controllo-e-formazione-interna/