Attacchi informatici all'azienda, responsabilità ex D.Lgs. 231/2001 e ruolo dell'organismo di vigilanza

Author : Lorenzo Nicolò Meazza

Date : 6 Novembre 2019

In un sistema basato sostanzialmente sui **rischi** e sulla loro **prevenzione**, come quello della responsabilità da reato degli enti (prevista dal D.Lgs. 231/2001), oggi il settore informatico è sicuramente uno degli ambiti che destano maggiore attenzione nelle società.

Già nel 2014, solo per fornire alcuni **esempi** della sempre crescente sensibilità sul tema, l'United Nations Interregional Crime and Justice Research Institute (UNICRI) ha pubblicato le "Linee guida per la sicurezza informatica per le PMI", mentre di recente l'"ECB Banking Supervision: Risk Assessment for 2019", un documento ufficiale della Banca Centrale Europea, ha individuato proprio l'informatica come uno dei settori con i più alti fattori di rischio per probabilità e impatto nelle grandi organizzazioni.

A chiudere il cerchio abbiamo un'**aggressione dello Stato**, nei confronti dei nostri sistemi telematici, via via più stringente. Da un lato, si registra l'ormai sdoganato utilizzo come mezzi di captazione dei Trojan Horse; tali strumenti, nati per combattere la criminalità organizzata e il terrorismo, oggi, con l'emanazione della Legge n.3/2019, la c.d. "Spazzacorrotti", sono adoperati anche per un numero di reati sempre più nutrito, compresi i delitti contro la Pubblica Amministrazione.
D'altro canto, sono sempre più estesi dalla giurisprudenza potere e perimetro del sequestro di tutti quei dispositivi (pc, tablet, pen drive...) che, in fase di indagine, si ritiene possano essere stati utilizzati per commettere dei crimini o che comunque possano fornire la prova della commissione degli stessi (Cass. pen. sez. V, 17 settembre 2019 n. 38456).

La tecnologia, sostanzialmente, ha travolto non solo il Codice Penale (che reca la data del 19 ottobre 1930), ma anche il più recente Codice di Procedura Penale (22 settembre 1988). Con riferimento agli aspetti procedurali, soprattutto sotto il profilo di accertamento dei fatti, molteplici sono le risposte che il processo penale deve ancora dare rispetto all'evoluzione informatica. Analogamente, bisogna considerare che tutti i reati (o quasi) con le nuove tecnologie possono essere commessi molto più facilmente. Tanto che è stata coniata appositamente l'espressione di ***"computer facilitated crimes"*** per indicare quei delitti comuni dopati dall'informatica (si

pensi al riciclaggio di denaro e alle sue molteplici sfaccettature che può assumere con il reimpiego di somme derivante da un illecito in criptovalute).

I beni aziendali che possono essere aggrediti dagli attacchi informatici, inoltre, sono davvero molteplici: riservatezza informatica, integrità dei dati, patrimonio e onorabilità della stessa società e dei suoi membri.

Più nel dettaglio, dal punto di vista dell'azienda, destano preoccupazione **due diverse e opposte condotte**. Innanzitutto devono essere segnalati gli attacchi informatici commessi da terzi nei confronti della società. Si pensi all'ipotesi delle *"Fake CEO Mail"*, ossia delle comunicazioni di posta elettronica inviate da un soggetto che si finge l'amministratore e ordina pagamenti ai propri sottoposti da una casella mail che magari si differenzia di un solo carattere da quella ufficiale.

Vi sono, d'altro lato, reati commessi da un soggetto intraneo all'ente e che possono, seppur "di rimbalzo" (o *"par ricochet"*, secondo il sistema di imputazione delle persone giuridiche in Francia), portare a un danno per l'azienda. Si pensi al caso di una fattispecie illecita portatrice di un interesse (quindi di un'utilità valutata *ex ante*) o di un vantaggio (utilità magari anche non effettivamente voluta, ma comunque maturata *ex post*) per l'impresa, come stabilito dall'art. 5 del D.Lgs. 231/2001, il testo normativo disciplinante la responsabilità da reato degli enti, che così dispone: "1. L'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio(…). 2. L'ente non risponde se le persone indicate nel comma 1 hanno agito nell'interesse esclusivo proprio o di terzi". Nel caso in cui, ad esempio, un dipendente di una società ponesse in essere un **accesso abusivo a un sistema informatico** (art. 615 ter c.p.) utilizzando un computer aziendale finalizzato a carpire segreti industriali di una concorrente, anche l'impresa sarebbe suscettibile di sanzioni, perché beneficerebbe di un interesse o un vantaggio. Qualora lo stesso dipendente commettesse invece una frode informatica (art. 640 ter c.p.) volta a farsi accreditare sul proprio conto una somma di danaro, sarebbe più evidente la sussistenza di un interesse esclusivo dell'autore del reato, tale da escludere il coinvolgimento dell'ente.

Bisogna a questo punto soffermarsi sul **ruolo dell'Organismo di Vigilanza** in materia.
L'art. 6 del D.Lgs. 231/2001, difatti, tra gli elementi necessari affinché un ente possa non rispondere di un reato commesso da un soggetto in posizione apicale, annovera il seguente requisito: "il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo". Il compito proattivo del c.d. OdV consiste, quindi, nell'effettuare una sorta di *stress test* di procedure e protocolli interni (che assieme costituiscono il Modello di organizzazione, gestione e controllo), volti a prevenire la commissione di reati all'interno dell'azienda.

In relazione a degli attacchi informatici, pertanto, l'organismo sarà tenuto a vigilare che il sistema di *compliance* interno sia adeguato a una prevenzione più ampia possibile (il rischio zero, purtroppo, non esiste), in modo da evitare *in primis* il verificarsi delle stesse condotte illecite o, quantomeno, escludere un coinvolgimento di responsabilità da parte dell'azienda stessa.

Utile, da questo punto di vista, il ricorso a *internal investigations* o specifici ***audit*** tesi a verificare l'effettiva vulnerabilità della rete e - allo stesso tempo - l'affidabilità del personale dell'ente. Non di rado vengono effettuati da parte dei responsabili Information e Technology, in accordo con amministratori o dirigenti, invii di false mail di *phishing*, tese a verificare se e chi nell'azienda potrebbe essere più esposto a un attacco.

Importante è, in ogni caso, che l'azione dispiegata dall'Organismo di Vigilanza nella lotta al *cybercrime* sia frutto di risoluzioni assolutamente **coscienti e consapevoli**. A titolo esemplificativo, un'investigazione interna, non disposta con le forme previste dal codice di procedura penale, potrebbe condurre a risultati paradossali. Gli esiti delle indagini societarie, finalizzate a fornire elementi a favore, potrebbero al contrario costituire una prova a carico dell'ente, già predisposta dallo stesso e impacchettata per la Procura.

Articolo a cura di **Lorenzo Nicolò Meazza**