Alert
Corporate - Review

Cybersecurity in tempi di pandemia

GLI EFFETTI DEL COVID-19 SULLA SICUREZZA INFORMATICA DELLE IMPRESE

L'attacco alla Campari

Mentre scriviamo la Campari sta fronteggiando gli effetti di un *cyber attack* iniziato l'1 novembre u.s. Prima di Campari, analoga sciagura – perché si tratta di una vera sciagura – ha colpito ENEL, Luxottica, Geox, Carraro (soltanto per citare le più recenti).
La tecnica è ormai nota: attraverso un *malware* l'*hacker* cripta i dati del *target* e, dopo averli copiati, li trasferisce su un proprio *server* (cd. esfiltrazione). Chi è sotto attacco perde l'accesso ai dati criptati: e quindi, sotto minaccia di una loro diffusione, gli viene chiesto il pagamento di un riscatto. Secondo un recente studio più di un terzo delle imprese attaccate ha ceduto all'estorsione: ma di queste quasi una su cinque non è comunque rientrata in possesso dei dati (Fonte: O. Elimelech).
Tornando al caso della Campari, da notizie di stampa questa di seguito è la comunicazione degli hacker rivolta alla società:

> *"We have BREACHED your security perimeter and get access to every server of company's Network in different countries across all your international office. So, we have DOWNLOADED more than 2TB total volume of your PRIVATE SENSITIVE Data, including:*
> - *Accounting files, Banking Statements, Government letters, Licensing certificates*
> - *Confidential and/or Proprietary Business information, Celebrity Agreements, Clients and Employees Personal information (including Social Security Numbers, Addresses, Phone numbers and etc.)*
> - *Corporate Agreements and Contracts with distributors, importers, retailers, Non-Disclosure Agreements*
> - *Also, we have your Private Corporate Correspondence, Emails and Workbooks, Marketing presentations, Audit reports and a lot of other Sensitive Information"*

Segue la richiesta di un riscatto per un ammontare pari a circa 15 milioni di dollari.

La società, dopo aver informato le competenti autorità per la protezione dei dati, la Polizia Postale italiana e l'FBI, ha attivato tutte le misure opportune al fine di riprendere il normale corso delle attività. Tuttavia queste hanno richiesto più tempo di quanto non preventivato: tant'è che il 9 novembre u.s. la società ha comunicato al mercato che alcuni sistemi rimangono ancora "*temporaneamente e deliberatamente sospesi*

od operanti con funzionalità ridotte in più siti" ed ha quindi preannunciato effetti (negativi), per quanto temporanei, sulle performance finanziarie del Gruppo dovuti, appunto, al protrarsi della crisi.

Il COVID-19 e la cybersecurity

È opinione diffusa che l'insorgere della pandemia abbia di fatto facilitato il diffondersi di pratiche di hackeraggio: ed invero gli attacchi informatici effettuati nel primo semestre del 2020 sono aumentati – rispetto allo stesso periodo dell'anno precedente – del 390%.

Se il collegamento – tra COVID-19 e *cyber attack* – può apparire più evidente nel caso in cui il target dell'attività criminosa sia una struttura sanitaria in prima linea nella battaglia contro il virus (qual è il caso, per l'Italia, dell'attacco ai danni dell'Ospedale Spallanzani nel marzo 2020) o in presenza di attacchi *phishing* aventi ad oggetto l'emergenza sanitaria (si calcola che solo nei primi due mesi di pandemia sono state almeno 230.000 le campagne di *malspam* lanciate da attori malevoli e legate al coronavirus: il 6% di queste ha riguardato l'Italia. Fonte: Leonardo), purtuttavia interrelazioni meno evidenti, ma più significative possono essere trovate anche altrove: e più specificamente nella corsa alla digitalizzazione stimolata dalla pandemia, nel diffuso ricorso allo *smart working* come misura di contenimento dei contagi sul posto di lavoro e nell'evoluzione in modalità telematica delle pratiche di socializzazione. Ebbene, gran parte delle imprese (e degli utenti) non erano attrezzati per una simile, repentina, evoluzione (del resto è stato osservato che è come se avessimo fatto un salto di 15 anni in un mese): il che ha generato inevitabilmente un *vulnus* nei sistemi di sicurezza (informatica), ampliando la 'superficie d'attacco'.

Non a caso è stato di recente previsto che, nel caso di uso da parte dei lavoratori di dispositivi elettronici privati, le pubbliche amministrazioni "*adottano ogni misura atta a garantire la sicurezza e la protezione delle informazioni e dei dati, tenendo conto delle migliori pratiche e degli standard nazionali, europei e internazionali per la protezione delle proprie reti, nonché a condizione che sia data al lavoratore adeguata informazione sull'uso sicuro dei dispositivi*": e, al fine di agevolare la diffusione del lavoro agile quale modalità di esecuzione del rapporto di lavoro subordinato, "*acquistano beni e progettano e sviluppano i sistemi informativi e i servizi informatici con modalità idonee a consentire ai lavoratori di accedere da remoto ad applicativi, dati e informazioni necessari allo svolgimento della prestazione lavorativa, …, assicurando un adeguato livello di sicurezza informatica, in linea con le migliori pratiche e gli standard nazionali ed internazionali per la protezione delle proprie reti, nonché a condizione che sia data al lavoratore adeguata informazione sull'uso sicuro degli strumenti impiegati, con particolare riguardo a quelli erogati tramite fornitori di servizi in cloud*" (art. 31 DL 16 luglio 2020, n. 76, convertito in L. 11 settembre 2020, n. 120).

Alert
Corporate - Review

Gli effetti di un *cyber attack*, obblighi di diligenza e possibili rimedi.

In base ad un'indagine condotta su più di 500 violazioni occorse nel 2019, le aziende impiegano mediamente 207 giorni per identificare e 73 giorni per contenere una violazione; e, in Italia, il costo medio di una violazione è pari a 3,19 milioni (Fonte: IBM).
Gli effetti di un *cyber attack* possono essere rilevanti e – in alcuni casi – letali. Senza voler considerare il prezzo del riscatto, la società viene di fatto messa nella condizione di non operare, seppure temporaneamente, con impatti – a seconda dei dati presi in 'ostaggio' – sul ciclo produttivo, sulla finanza, sui segreti industriali, sui dati sensibili, sui rapporti con clienti e fornitori, etc. Ci sono poi aspetti reputazionali – permeabilità del sistema di sicurezza – così come possibili ripercussioni sul titolo (in caso di società quotate).

A fronte di tali rischi gli obblighi di diligenza degli amministratori si amplificano. In alcuni, casi, infatti, potrebbe non bastare il mero ricorso ad *anti-spam*, *firewall* e sistemi di *back-up*: e occorrerà, comunque, accrescere la consapevolezza nei lavoratori circa le problematiche connesse alla sicurezza, investendo nella formazione (visto che nella maggior parte dei casi i rischi sono connessi al comportamento umano) e, quando le dimensioni lo consentano, creando una funzione interna specificamente dedicata.
Per contrastare – almeno in parte – gli effetti economici di eventuali hackeraggi, le società possono far ricorso alla copertura assicurativa. Nel 2018 soltanto poco meno di un quinto delle imprese italiano aveva sottoscritto polizze completamente dedicate al *cyber risk*: tuttavia, considerato l'incremento di attacchi cibernetici in atto, il dato è destinato inevitabilmente a crescere.

Sul versante della contrattualistica commerciale, specie in ambiti in cui vi sia tra le parti un significativo travaso di proprietà industriale e *know-how*, l'esistenza di adeguati sistemi di *cybersecurity* – e di una copertura assicurativa apposita - costituirà un pre-requisito a contrarre e sarà oggetto di specifica disciplina (chi mai condividerà informazioni riservate senza la garanzia che il proprio interlocutore sia effettivamente in grado di proteggerle adeguatamente anche da violazioni conseguenti ad attacchi cibernetici?).

Conclusioni

Il COVID-19 ha avuto l'effetto collaterale di accelerare il processo di digitalizzazione delle imprese, rendendo al contempo evidente il livello di impreparazione e conseguente vulnerabilità del sistema: la ricca casistica di attacchi cibernetici di questi ultimi tempi - di cui si è detto – mostra che è tempo che maturi nella classe imprenditoriale una consapevolezza diffusa delle problematiche connesse alla *cybersecurity*. Del resto questa pandemia ci insegna che nessuno è invulnerabile: e che sbaglia chi pensa che il problema riguardi soltanto gli altri.

Alert
Corporate - Review

D'altra parte, se è vero che non sempre le grandi imprese – nonostante i loro sofisticati apparati - riescono ad uscire del tutto indenni da tentativi di hackeraggio, è a maggior ragione vero che imprese più piccole - che dispongono nella maggior parte dei casi di soluzioni di sicurezza di base - incontrerebbero maggiori difficoltà a respingere un eventuale attacco ai loro danni, con conseguenze anche letali per la loro attività (ma con ripercussioni lungo tutta la filiera, fino alle grandi imprese stesse, vista la stretta interrelazione tra queste ed il mondo delle PMI).

C'è evidentemente un problema di costi. Secondo uno studio della Banca d'Italia le imprese italiane nel 2018 hanno destinato alla *cybersecurity* in media meno di 4.500 euro: cifra ritenuta insufficiente, ma che riflette bene la ridotta percezione del rischio. Le imprese dovranno giocoforza mutare approccio, investire di più nella sicurezza informatica (nonostante la congiuntura attuale porti nella direzione opposta), se del caso facendo rete fra loro per contenere l'incidenza dei costi.

Per altro verso, anche lo Stato deve fare la sua parte: il sistema Italia non può permettersi il lusso di lasciare per strada le PMI. Occorre quindi agevolare gli investimenti in *cybersecurity*, rendendoli meno onerosi grazie ad esempio ad appositi sgravi fiscali. Sul punto pare ci sia convergenza: tanto che il Governo ha preannunciato per il 2021 un incremento esponenziale delle percentuali di credito di imposta sugli investimenti fatti, tra l'altro, in *cyber* sicurezza (nell'ambito del Piano Industria 4.0 plus).

Infine, è necessario incentivare una diffusa *awareness* al riguardo. Le società sotto attacco hanno spesso qualche remora a rendere nota la situazione di crisi, temendone i riflessi negativi in termini reputazionali. Nulla di più sbagliato: i criminali contano appunto sull'omertà e sul senso di colpa che – in questa come in altre fattispecie criminose - si annida inconsapevolmente nella mente della vittima. Occorre al contrario un'aperta condivisione, perché il nemico è comune e soltanto maturando questa consapevolezza si potranno mettere a fattor comune informazioni ed esperienze con l'obbiettivo di spuntare le armi ai *cyber*-criminali.

25.11.2020

Gianmatteo Nunziante, Partner
E: g.nunziante@nmlex.it
T.: +39 06 695181

Per chiarimenti o informazioni potete contattare l'autore oppure il Vostro Professionista di riferimento all'interno dello Studio