La gestione dei ransomware, un approccio multidisciplinare

Fabrizio Di Geronimo
Manager dell'operating unit New Law di PwC TLS Avvocati e Commercialisti

Caterina Maggia
Associate dell'operating unit New Law di PwC TLS Avvocati e Commercialisti

PwC Incident Response & Threat Intelligence Competence Center

1. Introduzione: un approccio multidisciplinare per la gestione del ransomware

Negli ultimi decenni l'evoluzione tecnologica e il contestuale emergere dello spazio cibernetico[1] quale dominio di fondamentale rilevanza per gli operatori economici ha indubbiamente consentito rilevanti sviluppi ed efficientamenti economici per enti pubblici e privati di ogni dimensione, esponendo tuttavia, al tempo stesso, tali soggetti a nuove minacce. La crescente interconnessione tra i sistemi ha infatti comportato un contestuale aumento del rischio di potenziali vulnerabilità degli stessi e dei loro contenuti.

La minaccia *cyber*, intesa quale "*insieme delle condotte controindicate che possono essere realizzate nel e tramite lo spazio cibernetico ovvero in danno di quest'ultimo e dei suoi elementi costitutivi*"[2], nel corso del 2021 ha provocato

[1] "Spazio cibernetico quale insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti, nonché delle relazioni logiche stabilite tra di essi. Esso dunque comprende internet, le reti di comunicazione, i sistemi su cui poggiano i processi informatici di elaborazione dati e le apparecchiature mobili dotate di connessione di rete", Presidenza del Consiglio dei Ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico,* dicembre 2013, bit.ly/3LzVuE3, p. 10.

[2] *Ivi*, p. 11.

impatti economici stimati in 6 trilioni di dollari[3]. Secondo il Rapporto Clusit 2022, nel 2021 si è registrata un'ulteriore crescita di attacchi *cyber* che sono aumentati del 10% rispetto all'anno precedente[4]. Dei 42 milioni di attacchi registrati nel 2021 dal *Security Operations Center* (SOC) di Fastweb – il 16% in più rispetto all'anno precedente – il maggior numero di segnalazioni ha riportato impatti di grande severità nelle aree *Finance/Insurance*, della Pubblica Amministrazione e dell'Industria[5]. In quest'ultimo ambito è stata registrata una crescita importante di attacchi: dal 7% di casi di *cybercrime* registrati nel 2020, si è passati al 18% nel 2021. Con specifico riferimento ai *ransomware*, tali attacchi sono passati dal rappresentare il 23% di tutti i *malware* nell'anno 2018 fino ad arrivare al 67% nel 2020[6].

In un siffatto contesto la tecnica di attacco che ha conosciuto la crescita maggiore risulta essere proprio il *ransomware*[7], ovvero un *malicious software* capace, nella definizione offerta dal National Institute of Standards and Technology ("**NIST**"), di perpetrare un "*tipo di attacco malevolo nel quale l'attaccante cifra i dati di un'organizzazione e chiede il pagamento di un riscatto per ripristinarne l'accesso*". Il termine *ransomware* deriva infatti dal termine inglese *ransom* (*i.e.*, riscatto): nel momento in cui attacca un dispositivo e viene attivato, tale *software* malevolo procede alla cifratura dei file presenti sul *device* insieme a "*tutti i file di tutti i computer collegati nella stessa rete del personal computer infetto, compresi i dischi NAS di backup e reti remote collegate in VPN*"[8]. L'accesso al sistema informatico viene bloccato e i file presenti al suo interno vengono resi inutilizzabili da colui che ha messo in atto l'attacco. Inoltre, gli attacchi ransomware sono sempre più spesso accompagnati da una componente di esfiltrazione delle informazioni, idonea a compromettere quindi non solo l'accessibilità del dato ma anche la sua confidenzialità.

[3] S. Morgan, *Cybercrime to Cost the World $10.5 Trillion Annually by 2025* in *Cybersecurity Ventures*, 13 novembre 2020, bit.ly/3vACMXt.

[4] CLUSIT, *Rapporto Clusit 2022 sulla sicurezza ICT in Italia*, marzo 2022, https://clusit.it/rapporto-clusit.

[5] Fastweb, *Cyber Security, Fastweb fotografa le principali evoluzioni nel panorama della sicurezza italiana per il Rapporto Clusit 2022*, in *Fastweb.it*, 7 marzo 2022.

[6] *Id*.

[7] Il primo caso di *ransomware* risale al 1989. Il biologo americano Joseph Popp utilizzò il trojan AIDS - noto anche come Aids Info Disk o PC Cyborg Trojan – e lo diffuse attraverso migliaia di floppy disk consegnati ai partecipanti ad un congresso sull'Aids (da qui il nome del *ransomware*). Per sbloccare i file criptati, gli utenti dovettero pagare un riscatto di 189 dollari da inviare ad un ufficio postale di Panama (G. Sbaraglia, *Guida al ransomware: cos'è, come si prende e come rimuoverlo* in Cybersecurity360, 20 aprile 2021, bit.ly/3s7BHnP).

[8] A. Sagliocca, *Le minacce più comuni: difendersi da malware e da altri attacchi*, p. 72, Giuffrè Editore, 2017.

Peraltro, oltre al rischio di totale illeggibilità dei dati attaccati, il mancato pagamento del riscatto può anche comportare la diffusione pubblica sul *dark web* di dati aziendali o di segreti industriali dell'entità colpita: in tal caso si parla di "*double extortion attack*"[9]. Tale fenomeno, che fu rilevato per la prima volta nel novembre 2019 ai danni dell'americana Allied Universal[10], secondo alcuni esperti del settore è stata la risposta dei *criminal hacker* alla presa di posizione di tantissime società che si rifiutavano di pagare il riscatto per ottenere la chiave di decifratura.

Nel corso del 2020, il *ransomware* ha subito un'ulteriore evoluzione (c.d. "*triple extortion*"): la richiesta di riscatto non è più destinata esclusivamente all'azienda vittima di attacco ma coinvolge anche i clienti della società, i quali si trovano ad essere obbligati a pagare il riscatto per evitare che i loro dati vengano resi noti e pubblicati[11], o per evitare, nei casi più comuni, degli attacchi di tipo DoS (*Denial of Service*) o DDoS (*Distributed Denial of Service*). Gli effetti potenzialmente disastrosi di una simile tipologia di attacco sono evidenti: si apre, infatti, la possibilità che i dati esfiltrati vengano rivenduti a terzi nel mondo del *cyber crime* per attuare ulteriori campagne di ricatto *ad personam*, aumentando ancora di più gli incentivi a portare avanti attacchi contro le organizzazioni in possesso di dati particolarmente "sensibili" per i soggetti coinvolti.

Non è un caso che, nonostante, diversamente dal passato, ogni *industry* risulti essere *target* di attacchi ransomware, tali attacchi colpiscano oggi più che in passato settori particolarmente *data-sensitive*, come quello sanitario, o enti che erogano servizi essenziali per la collettività (si pensi alle organizzazioni governative, o al settore bancario e assicurativo, alle società di trasporto o a quelle operanti nel settore energetico). La necessità degli enti operanti in tali settori di poter accedere alle proprie informazioni comporta una maggiore propensione al pagamento del riscatto, per evitare le conseguenze economiche e sociali devastanti che deriverebbero dalla perdita dei dati o anche solo dalla temporanea impossibilità di accedervi.

Un altro fenomeno che ha sicuramente concorso alla proliferazione e

[9] Redazione ANSA, *Attacchi ransomware, cresce tecnica della 'double extortion'* in *ANSA*, 6 agosto 2022, bit.ly/3OUPA2y.

[10] P. Iezzi, *L'evoluzione del ransomware, la doppia estorsione: ecco di cosa si tratta* in *Cybersecurity360*, 8 settembre 2021, bit.ly/3ksGwns.

[11] Il primo caso di "*triple extortion*" risulta essere avvenuto in Finlandia ai danni della società Vastaamo, specializzata in supporto psicoterapeutico. Numerosi pazienti dell'azienda hanno infatti riferito di aver ricevuto e-mail con la richiesta di un riscatto da pagare in bitcoin al fine di evitare che le proprie cartelle mediche venissero divulgate sul web (vd. J. Masucci, *Le sedute con lo psicologo fatte online sono il nuovo obiettivo degli hacker* in *Espresso*, 29 luglio 2021, bit.ly/3s0YL7F).

al successo di questo tipo di attacchi è il c.d. *Ransomware as a Service* ("**RaaS**"), un modello di business che consente a diversi soggetti – tra cui anche coloro che non sono dotati di particolari abilità tecniche e che non sarebbero in grado di creare un ransomware autonomamente – di lanciare un attacco con successo.

Il modello RaaS prevede che almeno due soggetti prendano parte all'accordo, lo sviluppatore, in grado di scrivere e creare il programma malevolo capace di cifrare e potenzialmente rubare i dati della vittima, e l'affiliato, il quale, una volta ottenuta la licenza di utilizzo del *ransomware* da parte dello sviluppatore, esegue l'attacco e riscuote il riscatto. Tale sistema consente dunque anche a una persona scevra di competenze tecniche di acquistare il "servizio" e perpetrare un attacco *cyber* con successo.

Un ulteriore fattore che ha determinato la recente diffusione dei *ransomware*[12] è stata la progressiva diffusione delle criptovalute, sempre più sfruttate dai cyber criminali per via della loro tendenziale pseudonimia, e in taluni casi anonimità: durante gli attacchi *cyber*, i pagamenti del riscatto vengono infatti spesso richiesti in Bitcoin o in Monero, monete virtuali che possono essere tracciate con più difficoltà e che quindi incrementano la possibilità, per gli autori degli attacchi, di restare anonimi[13].

Alla luce delle suddette considerazioni è evidente come quella del *ransomware* si posizioni tra le minacce più pericolose, sia per società ed enti, sia per le singole persone coinvolte. Le organizzazioni vittime di attacco potrebbero infatti considerare di pagare i riscatti multimilionari al fine di proteggere il proprio business così come i dati dei propri clienti senza però avere cer-

[12] In tal senso, si evidenzia anche come, un ulteriore elemento che ha contribuito alla diffusione degli attacchi ransomware è consistito con la diffusione dello *smart working* a causa della pandemia da Covid-19. Ciò è spesso avvenuto perché i dipendenti che si sono trovati a doversi collegare da remoto ai sistemi aziendali, spesso non godevano degli stessi strumenti di sicurezza di rete presenti all'interno delle aziende o comunque non erano dotati di competenze sufficienti a permettergli di essere consapevoli degli attacchi che stavano subendo. Per questo motivo molte aziende hanno dovuto fare i conti con il fenomeno della sicurezza informatica implementando sistemi di *cyber security* in grado di tutelare i dati dei propri clienti e dipendenti, nonché i segreti industriali quali colonne portanti del loro *business*. È quindi ormai diffusa la consapevolezza che, per difendersi da tali attacchi, sia necessario dotarsi di sistemi di *governance* adeguati e in grado di prevenire i sempre più complessi *ransomware attacks*. (vd F. Chiesa, *Cyber attacchi ai pc di casa raddoppiati: le responsabilità del lavoratore in smart working* in *Corriere*, 28 aprile 2021, bit.ly/3s50t84).

[13] D'altro canto, è stato fatto notare come, "*a fare da contraltare all'anonimità c'è il carattere pubblico della blockchain che registra e rende pubblicamente disponibili tutte le transazioni effettuate, fornendo agli investigatori tracce preziose da cui poter risalire ai soggetti coinvolti*" (vd. L. Damiano, M. Giulioli, *Ransomware e criptovalute, coppia di fatto del malaffare: le azioni di contrasto* in *Agendadigitale*, 29 giugno 2021, bit.ly/3w0lIsz).

tezze sull'"onestà" dei *cyber* criminali, i quali, nonostante il pagamento del riscatto, potrebbero negare la consegna della chiave di decifratura dei file attaccati e pubblicare comunque i dati aziendali sul *web* o distruggerli[14].
A ciò si aggiunge anche il dubbio relativo all'uso che i criminali medesimi possono fare del denaro ricevuto in seguito al riscatto, il cui pagamento pone inevitabilmente un dilemma di ordine non solo etico e morale, ma anche legale e reputazionale. Il denaro ottenuto dai *cyber criminal*, autori dell'attacco, potrebbe infatti essere utilizzato per l'acquisto di *server* o domini o ancora per finanziare associazioni terroristiche, stati dittatoriali, traffico di esseri umani così come l'acquisto di armi di distruzione di massa. Peraltro, è utile sottolineare come molti gruppi di *criminal hacker* siano *state-sponsored*, ovvero finanziati e supportati da Stati per cui agiscono e che ne assicurano l'impunità (si pensi al gruppo russo Cozy Bear o al nord coreano Lazarus Group)[15].
Considerati i potenziali impatti di natura non solo *cyber* e legale ma anche economica e reputazionale che la minaccia *ransomware* comporta per le società, la sua corretta gestione richiede un approccio multidisciplinare che spazia dalla creazione di una *governance structure* in grado di scongiurare la perdita di informazioni o il blocco di sistemi interni fino ad arrivare all'adozione di strategie *post-incident* essenziali per garantire il contenimento

[14] A differenza dei comuni *malware*, il *ransomware* non è programmato per rimanere nascosto. Al contrario, dopo l'infezione, viene immediatamente trasmessa una nota nel sistema della vittima, la quale viene informata del fatto che il suo sistema è stato infettato. Talvolta, nella stessa nota sono visibili un *timer*, un indirizzo sul quale effettuare il pagamento del riscatto, che sempre più spesso sfrutta l'anonimità tipica di molte criptovalute, nonché le istruzioni per poter acquistare la criptovaluta scelta.
Una volta pagato il riscatto, la vittima dovrebbe ricevere la chiave di decifratura in grado di garantire di nuovo l'accesso ai propri *file*. Tale esito, tuttavia, è tutt'altro che scontato. Numerosi rapporti sulla sicurezza informatica evidenziano l'imprevedibilità di ogni singolo caso di attacco *ransomware*: in alcuni casi le vittime, nonostante il pagamento del riscatto nei tempi indicati, non ricevono alcuna chiave di decifratura; mentre, in altri casi, la chiave viene regolarmente fornita e i dati recuperati anche se il *ransomware* nel frattempo ha già provveduto a installare componenti e *software* malevoli sul sistema al fine di lasciare una "via libera" per futuri attacchi e richieste di denaro.
[15] Tra i casi più emblematici di *ransomware* lanciati da gruppi di hacker *state-spondored* si ricorda NotPetya (Institute for Security and Technology, *Combating Ransomware. A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force*, 2021, bit.ly/3769CGb), definito dalla Casa Bianca come "*l'attacco informatico più distruttivo della storia*". Avvenuto nel 2017, questo attacco ha colpito sistemi di trasporto, multinazionali, banche e sistemi di pagamento in Ucraina, e disattivato, per la prima volta dopo 31 anni, i sistemi di monitoraggio delle radiazioni all'interno della Centrale di Chernobyl. Nel 2018 i governi membri dell'UKUSA Community (Stati Uniti, Regno Unito, Nuova Zelanda, Australia e Canada) hanno formalmente accusato la Russia, e in particolare l'agenzia di intelligence militare (GRU), di aver creato e diffuso NotPetya.

delle perdite economiche derivanti dall'interruzione della *business continuity* dell'azienda, dai furti di proprietà intellettuale e di dati personali, nonché dalle sanzioni e dagli obblighi risarcitori.
Il presente commento si propone, suddividendo nei due successivi capitoli gli aspetti *pre* e *post incident*, di analizzare i principali adempimenti che le società, rispettivamente, in previsione di un attacco ransomware e successivamente alla scoperta dello stesso, devono rispettare al fine, da un lato, di prevenire efficacemente l'evento e, dall'altro, di gestirlo opportunamente, mitigandone gli effetti e rispettando i doveri imposti dalla normativa vigente.

2. Gli adempimenti pre-incident

La gestione di un evento ransomware richiede un approccio multidisciplinare che coinvolge numerose competenze sia in una fase preventiva all'eventuale incidente sia nella fase successiva. Per quanto concerne quei processi che devono caratterizzare la fase preparatoria all'evento di sicurezza, si può parlare di attività *"pre-incident",* intese come l'insieme di iniziative preparatorie che devono essere adottate per garantire una gestione efficace nell'evenienza che si verifichi un attacco ransomware.

2.1 La prevenzione informatica

Tra le attività *pre-incident* di natura informatica più rilevanti vi è anzitutto la Compromise Discovery, che consiste nell'identificazione delle minacce e dunque delle vulnerabilità che possono potenzialmente già insistere all'interno dell'infrastruttura IT/OT[16] (Information Technology/Operational Technology).
Dette rilevazioni possono essere effettuate sia attraverso scansioni di PC e server (*host-based scanning*) così da identificare le vulnerabilità insistenti su server, workstation e altri *host* di rete consentendo di avere una maggiore visibilità delle impostazioni di configurazione e della cronologia delle patch installate, sia attraverso la Network Traffic Inspection sull'infrastruttura di rete IT/OT che consente invece di rilevare e analizzare il traffico di rete, individuando ad esempio, la potenziale ricezione di pacchetti malevoli.
La Compromise Discovery consente, di fatto, di avere una visibilità circa il livello di sicurezza dell'infrastruttura e di valutare dunque, *ex-ante,*

[16] *Operational Technology* (OT) è il termine utilizzato per fare riferimento agli impianti industriali automatizzati, che hanno quasi sempre anche una connessione all'infrastruttura ICT, e sono quindi suscettibili ad attacchi ransomware.

l'eventuale opportunità di migliorare le misure di prevenzione e la *cyber posture* dell'organizzazione.
Di fondamentale rilevanza è poi il processo di Threat Modelling che consente di identificare, enumerare e prioritizzare le potenziali minacce che potrebbero insistere sull'organizzazione ed avere significativi impatti sull'infrastruttura tecnologica della stessa.
La preventiva identificazione e prioritizzazione delle minacce consente di pervenire non solo ad una maggiore consapevolezza dei rischi cui l'organizzazione va incontro, ma anche di individuare prontamente le più adatte ed efficaci misure di sicurezza da adottare per poter fronteggiare ogni eventuale scenario individuato.
Imprescindibile nella fase di *pre-incident* è poi la definizione di Crisis Framework o Playbook contenenti le azioni da adottare al verificarsi di un incidente. Il Crisis Framework può essere dunque utilizzato quale guida cui attingere per individuare le misure da adottare al verificarsi di un evento cyber.
Se tutte le attività fin qui descritte si presentano come fondamentali al fine di pervenire ad un'efficace gestione di un evento cyber, è anche vero che l'efficacia delle stesse può essere testata tramite apposite simulazioni.
Nel caso di specie, di essenziale rilievo è l'attività di Ransomware Attack Simulation consistente nell'esecuzione di simulazioni interattive capaci di evidenziare, non solo l'efficacia e la correttezza delle analisi ed attività *pre-incident* finora illustrate, ma anche di verificare le capacità di risposta del personale a ciò preposto e dunque di intervenire laddove le misure adottate non fossero sufficienti per l'efficace gestione della situazione emergenziale dettata dall'attacco ransomware.

2.2 Governance structure

Quale fondamentale misura di prevenzione di un *cyber incident*, le aziende non devono sottovalutare l'opportunità di dotarsi di una struttura interna finalizzata a scongiurare la perdita di informazioni o il blocco di sistemi interni derivanti da *cyber disaster*, adottando una struttura organizzativa idonea a gestire un possibile evento *ransomware*, in modo da assicurare che l'eventuale fase di *cyber incident response* sia gestita da un *team* specializzato, in grado di operare con efficienza e di gestire gli incidenti in maniera tempestiva.
L'organizzazione del sistema di sicurezza informatica dovrà ovviamente variare in base alle diverse realtà aziendali ma è comunque possibile delineare una struttura generale di divisione dei compiti e delle responsabilità in materia di *cybersecurity*.

Ruolo di preminente importanza nell'opera di individuazione e corretta gestione degli aspetti di sicurezza informatica propri di un'impresa spetta direttamente al Consiglio di Amministrazione[17], che ha il compito di stabilire gli obiettivi strategici della società e di valutarne l'assetto organizzativo e amministrativo in relazione anche ai potenziali rischi *cyber* individuati unitamente alle funzioni con competenze tecniche.

Certamente, per l'ordinaria gestione degli eventi cyber gli amministratori potranno avvalersi di un preciso sistema di deleghe, più o meno ampie. In particolare, nello stabilire la *governance* aziendale dal punto di vista della sicurezza informatica, gli amministratori possono ricorrere a modelli organizzativi di tipo centralizzato o decentralizzato a condizione che vengano garantite misure "*adeguate e proporzionate alla gestione dei rischi, alla sicurezza delle reti e dei sistemi informativi o di policy per la prevenzione e gestione degli incidenti informatici*"[18]. Se da un lato il modello centralizzato si basa sulla concentrazione delle responsabilità in ambito *cyber* in capo al Consiglio di Amministrazione, dall'altro il sistema organizzativo decentralizzato è solitamente adottato all'interno di realtà aziendali di notevoli dimensioni che spesso presentano sedi tra loro dislocate[19].

La delega di funzioni viene spesso adottata in realtà aziendali di non modeste dimensioni, all'interno delle quali è necessario segmentare i centri decisionali in capo a soggetti dotati di competenze specifiche in materia di sicurezza informatica, i quali possono essere interni o esterni all'azienda. I soggetti a cui è riconosciuta la delega si trovano così a ricoprire una posizione di responsabilità rispetto alla gestione dei rischi e delle strategie in ambito *cyber*, dovendo ad ogni modo rendere conto del proprio operato di fronte al Consiglio di Amministrazione il quale ricopre il ruolo di garante cui spetta un obbligo di vigilanza.

I vertici aziendali possono altresì provvedere alla creazione di un piano integrato di *cybersecurity* "*definendo chiaramente i ruoli e le responsabilità e la loro opportuna separazione (principio della segregazione dei compiti) che individui tre livelli di controllo: controllo di primo livello, sotto la responsabilità diretta di chi opera la funzione (produzione, IT, vendite, ecc.); controlli*

[17] È stato infatti notato come "*Una risposta organizzativa sistematica che parta da una visione d'insieme è il modus operandi più efficace e funzionale, capace di tenere conto delle diverse implicazioni che un attacco o incidente informatico possa avere sulla produttività dell'impresa*" (vd. B. Panattoni, *Compliance, Cyber security e sicurezza dei dati personali*, I Edizione, Ipsoa, gennaio 2020, p. 50).

[18] C.A.M. Corazzini, G.M. Amato, *Il modello organizzativo per la gestione dei rischi in ambito IT*, Cyberlaws, 12 ottobre 2020, bit.ly/3kwrSLP.

[19] *Id*.

di secondo livello, sotto la responsabilità di una funzione di sicurezza, esterna alle funzioni di produzione/business; controlli di terzo livello, sotto la responsabilità delle funzioni di controllo interno"[20].

Tra le principali figure professionali delegate a gestire la sicurezza informatica all'interno di una realtà aziendale è necessario richiamare il *Chief Information Security Officer* ("**CISO**"), che ricopre il ruolo fondamentale di Responsabile della sicurezza informatica all'interno dell'azienda ed è incaricato della protezione dei sistemi di *information technology* presenti. Tra le responsabilità affidate al CISO rientrano solitamente i doveri di valutazione della struttura di sicurezza informatica adottata e l'individuazione di eventuali vulnerabilità, la definizione di *policy* e *standard* necessari a garantire la tutela dei dati e delle informazioni aziendali, l'individuazione di eventuali minacce e la successiva elaborazione di piani di intervento tempestivi in caso di attacchi.

Un ulteriore aspetto meritevole di considerazione nell'ambito della prevenzione per la gestione di un'emergenza ransomware è quello legato alla *business continuity*, ovvero alla continuità operativa.

Sempre più aziende e organizzazioni, anche laddove non siano mai state vittime di un attacco ransomware, sperimentano quotidianamente l'esigenza di creare e avere al proprio interno un Business Continuity Plan (BCP) che sia in grado di ridurre le conseguenze di un incidente tanto di natura cyber quanto di natura operativa.

È bene rammentare come all'interno della norma internazionale ISO 23301:2019 finalizzata a definire "*la struttura e i requisiti per l'implementazione e il mantenimento di un sistema di gestione della continuità aziendale (BCMS)*" venga fatto un esplicito riferimento agli "scenari" da considerare per la predisposizione di un adeguato BCP e delle relative esercitazioni.

È evidente, valutato il contesto in cui ormai operano aziende e organizzazioni, come un attacco ransomware non possa più essere considerato alla stregua di uno scenario inaspettato, richiedendo al contrario un apposito piano di continuità operativa che contenga le indicazioni necessarie per evitare un'interruzione del servizio oltre i livelli stabiliti dall'organizzazione. In particolare, si richiede che all'interno del BCP siano riportati i due seguenti parametri: (i) RTO – Recovery Time Objective, ossia le tempistiche stabilite per il totale recupero dell'attività operativa di un sistema che si concretizza nello stabilire la durata massima tollerata di un downtime e

[20] Osservatorio Nazionale per la Cyber Security, Resilienza e Business Continuity delle Reti Elettriche, *Principi, Linee Guida e Good Practices per la gestione della Cyber Security, Resilienza e Business Continuity degli Operatori Elettrici*, 23 settembre 2018, p. 8.

(ii) RPO – Recovery Point Objective, che offre la misura massima tollerata di dati che il sistema può perdere[21].

2.3 I framework giuridici di riferimento: gli adempimenti privacy e il Perimetro di sicurezza nazionale cibernetica

Da un punto di vista più strettamente giuridico, i principali *framework* di riferimento da considerare per prepararsi a un possibile evento cyber sono costituiti dal Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (regolamento generale sulla protezione dei dati; "GDPR") e il più recente Perimetro di sicurezza nazionale cibernetica istituito dal decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni dalla L. 18 novembre 2019, n. 133 (il "Decreto Legge"). Tali sistemi normativi, solo parzialmente coincidenti in quanto ad ambito di applicazione, stabiliscono specifiche obbligazioni che devono essere rispettate dalle società nel caso in cui subiscano un incidente informatico e impongono, in caso di mancato rispetto delle stesse, pesanti sanzioni[22]. Inoltre, entrambe le normative, al fine di scongiurare, fin dove possibile, il rischio di un incidente informatico, richiedono l'adozione di specifiche misure di sicurezza[23].

2.3.1. Il Perimetro di sicurezza nazionale cibernetica

Sulla spinta di un sempre maggiore riconoscimento della rilevanza delle minacce derivanti dal dominio cibernetico a livello europeo, anche l'Italia ha, negli ultimi tre anni, compiuto diversi passi in avanti per garantire la sicurezza delle proprie reti. A tal fine, la svolta fondamentale è stata l'adozione del decreto legge, che istituisce il perimetro di sicurezza nazionale cibernetica[24] al "*fine di assicurare un livello elevato di sicurezza delle reti, dei*

[21] Per meglio comprendere l'importanza di un adeguato ed efficace piano di continuità operativa si pensi all'attacco ransomware che il 10 settembre 2020 colpì l'ospedale universitario di Düsseldorf portando, indirettamente, alla morte di una paziente. Sebben si parlò inizialmente di "*prima morte per ransomware*", un'analisi più approfondita ha dimostrato quanto non sia stato un problema di *security* a portare alla tragedia quanto piuttosto alla mancanza di un adeguato piano di Business Continuity (Per maggiori informazioni sull'attacco ransomware citato vd. F. Cilona, *Morte per ransomware in ospedale, è stato un problema di continuità operativa: ecco perché* in *Cybersecurity360*, 25 settembre 2020, bit.ly/3OSojNW).

[22] Il GDPR prevede, per il mancato rispetto delle norme in materia di *data breach*, sanzioni fino a 10 milioni di euro o, se superiore, fino al 2% del fatturato mondiale annuo dell'esercizio precedente, se superiore (vd. art. 83, GDPR); il Decreto Legge prevede invece, una sanzione fino a 1,5 milioni di euro in caso di mancata notifica (vd. articolo 1, comma 9, b), Decreto Legge).

[23] In particolare, si veda gli articoli 24 e 33, GDPR e l'articolo 1, comma 3, Decreto Legge, nonché il Decreto del Presidente del Consiglio dei Ministri 14 aprile 2021, n. 81.

[24] Articolo 1, Decreto Legge.

sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale"[25]. Si evincono, a ben vedere, da tale preliminare disposizione, tutti gli elementi cardine posti alla base della costituzione del perimetro di sicurezza nazionale cibernetica, costituito da quell'insieme di enti, indifferentemente pubblici e privati, da cui dipende l'esercizio di una funzione essenziale o la prestazione di un servizio essenziale e che si avvalgano di reti, sistemi informativi e servizi informatici per tali funzioni e/o servizi essenziali.

Il decreto legge attribuisce poi a quattro successivi D.P.C.M. la specificazione delle obbligazioni previste. Ad oggi, risultano già adottati e implementati i seguenti tre D.P.C.M.: (i) Decreto del Presidente del Consiglio dei Ministri 30 luglio 2020, n. 131 ("D.P.C.M. 1"); (ii) Decreto del Presidente del Consiglio dei Ministri 14 aprile 2021, n. 81 ("D.P.C.M. 2"); e (iii) Decreto del Presidente del Consiglio dei Ministri 15 giugno 2021 ("D.P.C.M. 3").

Il primo D.P.C.M. ha definito i fondamentali concetti di funzione essenziale dello Stato e di servizi essenziali per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato[26] e individuato i settori di attività – salvi futuri aggiornamenti – nei quali sono inclusi i soggetti da ricomprendere nel perimetro[27]. Il D.P.C.M. 1 individua, inoltre, le modalità e i criteri per l'individuazione dei soggetti inclusi nel perimetro da parte delle competenti amministrazioni pubbliche. Tale inclusione viene quindi comunicata agli enti e alle società rilevanti ai sensi dell'articolo 1, comma 2-bis, decreto legge entro trenta giorni dall'avvenuta iscrizione.

Una comunicazione di fondamentale importanza per le società interessate poiché comporta la necessità di rispettare i numerosi adempimenti previsti dalla normativa. Il primo di essi consiste con la predisposizione dell'elenco di beni ICT[28], inclusivo dell'indicazione delle reti, dei sistemi informativi e

[25] *Id.*

[26] Si veda l'art. 2, D.P.C.M. 1.

[27] Ai sensi dell'articolo 3, D.P.C.M., tali settori sono: interno, difesa, spazio e aerospazio, energia, telecomunicazioni, economia e finanza, trasporti, servizi digitali, tecnologie critiche ai sensi del Regolamento (UE) 2019/452 ed enti previdenziali e lavoro.

[28] L'articolo 7, D.P.C.M. 1 prevede inoltre l'aggiornamento almeno annuale di tale elenco di beni ICT.

dei servizi informatici che li compongono[29], che dovrà essere comunicato all'Agenzia per la cybersicurezza nazionale entro sei mesi dall'avvenuta iscrizione[30].

Ai sensi dell'articolo 8 del D.P.C.M. 2, inoltre, i soggetti inclusi nel perimetro devono adottare, per ciascun bene ICT, le misure di sicurezza specificamente elencate all'allegato B del D.P.C.M. 2, entro un termine rispettivamente di sei o trenta mesi, a seconda delle misure[31], dalla comunicazione dei beni ICT. Peraltro, oltre a mappare i beni ICT rilevanti, al fine di adempiere alle obbligazioni previste dalla normativa, le società dovranno dotarsi delle necessarie risorse, umane e tecniche, idonee a implementare e mantenere le misure di sicurezza indicate dal D.P.C.M. 2. A tal riguardo, a conferma dell'accentramento del controllo dell'adeguatezza delle misure, si segnala come anche le misure di sicurezza adottate dovranno essere comunicate al DIS e all'Agenzia per la cybersicurezza nazionale.

Il D.P.C.M. 2 definisce, inoltre, una tassonomia degli incidenti di sicurezza aventi un impatto sui beni ICT di pertinenza dei soggetti inclusi nel perimetro[32] differenziando conseguentemente la tempistica entro i quali i rispettivi incidenti dovranno essere comunicati. Termini comunque estremamente ristretti in considerazione dell'interesse nazionale dei beni ICT oggetto dell'incidente, pari a sei ore nel caso degli incidenti meno gravi e, addirittura, un'ora per gli incidenti considerati più gravi[33]. Sul punto, è stato peraltro fatto notare come, essendo gli incidenti identificati all'allegato A del D.P.C.M. 2 un numero chiuso, non sarebbe certa la classificazione – e il relativo termine per effettuare la notifica – per eventuali ulteriori categorie di incidenti[34]. Ciò richiederà, in fase di *pre-incident*, l'adozione di dettagliate procedure, che individuino con chiarezza ruoli e processi interni da attivare per poter rispettare le stringenti tempistiche di notifica in caso di incidente informatico.

Analogamente, le società incluse nel perimetro dovranno altresì disciplinare, definendo i relativi processi interni, l'aggiornamento periodico dei beni ICT rilevanti al fine di poter procedere periodicamente, e comunque almeno annualmente[35], all'aggiornamento della comunicazione effettuata

[29] Articolo 7, D.P.C.M. 1.
[30] Vd. Art. 1, comma 2, lett. b), Decreto Legge e Articolo 9, D.P.C.M. 1.
[31] Per una classificazione delle misure, si veda appendice n.2 dell'allegato B del D.P.C.M. 2.
[32] Si veda allegato A, D.P.C.M. 2.
[33] Articolo 3, D.P.C.M. 2.
[34] G. Muccioli, *Perimetro di sicurezza nazionale, una delicata questione legislativa*, in *Cybersecurity 360*, 31 gennaio 2022, bit.ly/3s553TC.
[35] Articolo 7, D.P.C.M. 1.

ai sensi del D.P.C.M. 1, nonché le modalità di selezione di nuovi fornitori. Ai sensi del D.P.C.M. 3, infatti, i soggetti inclusi nel perimetro devono procedere a specifiche procedure di affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sistemi informativi e per l'espletamento dei servizi informativi che impattano sui servizi e le funzioni essenziali ai sensi del decreto legge. In particolare, tale procedura di affidamento, definita più nel dettaglio in un ulteriore decreto implementativo della normativa, il Decreto del Presidente della Repubblica 5 febbraio 2021, n. 54, prevede, prima dell'avvio delle procedure di affidamento o, ove non previste, della sottoscrizione di contratti aventi ad oggetto tali forniture di beni, sistemi e servizi ICT, la comunicazione al Centro di Valutazione e Certificazione nazionale ("**CVCN**") o ai centri di valutazione del Ministero dell'interno e del Ministero della difesa (i "**CV**"), che svolgeranno le verifiche e valutazioni di rispettiva competenza su requisiti hardware e software[36]. Ad esito di tali valutazioni, il CVCN e i CV redigeranno un rapporto di valutazione che potrà, se negativo, comportare l'obbligo di abbandono del progetto di fornitura e, se positivo, imporre il rispetto di specifiche prescrizioni da includere nel bando di gara o nel contratto di fornitura ICT[37].

2.3.2 La protezione dei dati personali a confronto con gli incidenti di sicurezza

L'articolo 4, n. 12, GDPR, definisce un data breach come una "violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati". Pertanto, un data breach, o violazione di dati personali, costituisce una particolare tipologia di incidente di sicurezza, che impatta su un particolare tipo di informazioni, i dati personali[38]. E infatti, come chiarito dal Gruppo di Lavoro Articolo 29 nelle Guidelines on Personal data breach notification under Regulation 2016/679 (rispettivamente, "**WP29**" e "**Guidelines on Personal Data**

[36] Art. 4, D.P.R. 5 febbraio 2021, n. 54.
[37] Art. 8, D.P.R. 5 febbraio 2021, n. 54.
[38] Ai sensi dell'articolo 4, par. 1, num. 1), GDPR, i dati personali sono "*qualsiasi informazione riguardante una persona fisica identificata o identificabile [definita a sua volta («interessato»)]; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*".

Breach")[39], "whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches"[40]. In particolare, qualora la violazione di sicurezza riguardi altresì dati personali, e ne comprometta dunque la riservatezza, integrità e/o disponibilità, sarà necessario rispettare le obbligazioni previste dal GDPR in materia e, in particolare, valutare, alla luce della gravità dell'incidente per i diritti e le libertà degli interessati, la necessità e/o opportunità di notificare l'evento al Garante per la protezione dei dati personali e/o agli interessati[41], nonché documentare internamente l'accaduto tramite la predisposizione di un c.d. registro dei data breach.

La rilevanza di tali obbligazioni trova la conferma nelle conseguenze sanzionatorie connesse dal GDPR all'omessa notificazione di un data breach ai sensi dei parametri indicati dagli articoli 33 e 34, GDPR; in tal caso, infatti, la supervisory authority potrà esercitare i poteri correttivi a sua disposizione, nonché imporre una sanzione amministrativa pecuniaria appropriata per un valore che potrebbe ammontare fino a € 10.000.000 o fino al 2% del fatturato totale annuo globale, se superiore[42].

Rinviando le analisi di dettaglio sulle valutazioni di un eventuale data breach e delle conseguenti considerazioni in merito agli obblighi di notifica[43], in uno scenario pre-incident, i soggetti rientranti nell'ambito di applicazione del GDPR[44] dovranno adottare le necessarie azioni al fine di essere in grado, nell'ipotesi in cui si dovesse verificare una violazione di dati personali, di rispettare le obbligazioni previste dalla normativa.

Anzitutto, i titolari (e responsabili) del trattamento hanno una vera e propria obbligazione di adottare, alla luce dei rischi insiti nei trattamenti effettuati, le misure tecniche e organizzative idonee a garantire un livello

[39] Gruppo di Lavoro Articolo 29, *Guidelines on Personal data breach notification under Regulation 2016/679*, adottate il 3 ottobre 2017, Versione emendata e adottata in data 6 febbraio 2018, WP250rev.01.

[40] *Guidelines on Personal Data Breach*, p. 7.

[41] Come noto, qualora la violazione di sicurezza coinvolga dati personali, e sia pertanto qualificabile quale *data breach* ai sensi del GDPR, il titolare del trattamento è anzitutto chiamato, ai sensi dell'articolo 33, GDPR, a notificare al Garante per la protezione dei dati personali la violazione dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che il *data breach* presenti un rischio per i diritti e le libertà degli interessati.
L'articolo 34, GDPR, prevede inoltre che quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve comunicare tale violazione agli interessati senza ingiustificato ritardo.

[42] Articolo 83, par. 4, lett. a), GDPR.

[43] Si veda il successivo capitolo 3.B.2.

[44] Si considerino gli articoli 2 e 3, GDPR.

sicurezza adeguato[45]. In particolare, tali misure dovranno includere non solo quelle necessarie a mitigare i rischi e scongiurare un possibile incidente informatico ma, alla luce della nota impossibilità di evitare ogni rischio, anche gli strumenti idonei a identificare una minaccia in corso e a mitigarne le conseguenze dannose. Ad esempio, nel caso specifico degli attacchi ransomware, l'European Data Protection Board ("**EDPB**") ha specificato che l'adozione di backup separati dal sistema principale e la crittografia dei dati personali trattati risultano misure fondamentali per mitigare gli effetti di un eventuale attacco[46].

Inoltre, più in generale, i titolari del trattamento dovranno adottare idonee procedure interne che definiscano ruoli e responsabilità per essere in grado, in caso di data breach, di attivare i processi interni idonei a individuare prontamente l'evento, effettuare le necessarie valutazioni, definire le azioni da intraprendere ed essere in grado di rispettare tempistiche e modalità di notifica al Garante per la protezione dei dati personali e agli interessati.

Da ultimo, al fine di rispettare l'articolo 33, par. 5, GDPR, i titolari del trattamento dovranno dotarsi di un registro delle violazioni di dati personali nel quale documentare tutti i data breach, anche quelli che si sarà deciso di non notificare, comprese le circostanze ad essi relativi, le conseguenze e le misure adottate per porvi rimedio.

3. L'inevitabilità dell'incidente: adempimenti post-attacco

Per le realtà aziendali è fondamentale avere la consapevolezza che eventuali incidenti *cyber* possano comportare danni di diversa natura che spaziano dai danneggiamenti ai sistemi informatici, ai furti di informazioni confidenziali e coperte da diritti di proprietà intellettuale, nonché dati personali, fino ad arrivare a danni reputazionali mettendo inoltre a rischio la *business continuity* dell'azienda stessa. L'adozione di strategie *post-incident* è pertanto altrettanto essenziale per mitigare gli effetti dell'incidente informatico, contenere le perdite economiche ed evitare sanzioni e obblighi risarcitori. In particolare, qualora gli impatti provocati dal ransomware dovessero essere tali da comportare una situazione di crisi, dovrebbe essere attivato il sistema di gestione della stessa al fine di assicurare un efficace processo decisionale atto a soddisfare le aspettative formulate dai diversi *stakeholder* – interni ed esterni – all'organizzazione.

[45] Art. 32, GDPR.

[46] EDPB, *Guidelines 01/2021 on Examples regarding Personal Data Breach Notification*, 14 dicembre 2021, v. 2.0.

Sarà dunque necessario attivare immediatamente il team competente alla gestione della crisi secondo quanto definito nella strategia precedentemente adottata. A seguito di un intervento di *immediate rescue*, finalizzato ad eliminare o impedire il prodursi delle conseguenze negative legate all'evento, dovranno essere attivate, se necessario, tutte le attività di *crisis governance* per avviare ogni azione relativa alla risoluzione dell'incidente con il supporto di tutte le figure necessarie per minimizzare le conseguenze operative, legali ed economiche.

3.1 Le risposte cyber all'attacco ransomware

Da un punto di vista tecnologico, di fondamentale importanza risulta l'insieme di attività che prendono il nome di Cyber Incident Response, intese come il "set" di azioni di risposta ad un attacco ransomware che costituiscono la base delle attività di risposta. L'*incident response* prevede lo svolgimento di un'analisi tempestiva dell'evento in corso o da poco avvenuto e la definizione del perimetro compromesso e del *patient 0*[47], essenziale per adottare tutte le contromisure necessarie ad impedire o limitare gli effetti derivanti dalla compromissione e la relativa diffusione all'interno dell'intero perimetro aziendale.

Mentre le attività di *incident response* proseguono, è essenziale che gli analisti che si occupano di *threat intelligence* diano avvio alle indagini al fine di individuare i *threat actor* coinvolti nell'attacco e tutti i dati ad essi correlati, così da supportare la risposta all'attacco con informazioni riguardo le tattiche, le tecniche, e le procedure (TTP) utilizzate dai *threat actor*, i file da rimuovere per bloccare eventuali ulteriori attacchi o la persistenza nei sistemi colpiti.

Le attività svolte dal team di *threat intelligence* sono peraltro imprescindibili per comprendere lo scopo principale dei criminali, intuire le loro mosse e dunque capire cosa aspettarsi e come reagire. Per esempio, le analisi potrebbero condurre all'individuazione di una *advanced persistent threat* (APT), che ha interesse a creare persistenza nei sistemi, a esfiltrare informazioni sensibili nonché informazioni coperte da diritti di proprietà intellettuale in un lasso temporale che può durare anche più anni, o, diversamente, delle minacce di tipo ransomware, caratterizzate invece da un interesse a esfiltrare dati rapidamente e a richiedere il riscatto una volta bloccati i sistemi della vittima. Altre tipologie di minacce potrebbero essere le *insider threat*, che possono concretizzarsi sia in attacchi simili ad APT o in attacchi più evidenti, nonché l'*hacktivism* spesso in forma di *denial of service* o furto di dati.

[47] Per *patient 0* ovvero paziente 0 si intende il primo dispositivo compromesso dall'attacco.

In parallelo con le analisi di *threat intelligence* e *incident response*, i file malevoli devono essere estratti dai sistemi compromessi per permettere l'esecuzione delle attività di analisi del *malware* e di *reverse engineering*, volte a studiare il comportamento e la capacità dei *threat actor* e dei file da questi utilizzati. Solo attraverso tale attività di studio è poi possibile identificare la strategia di risposta migliore per arginare l'attacco e mitigarne gli effetti.

3.2 Gli adempimenti imposti dalla normativa: le valutazioni sul rischio per i diritti e le libertà degli interessati

Da un punto di vista giuridico, la scoperta di un incidente di sicurezza determina anzitutto la necessità di verificare le normative di settore innescate dallo stesso al fine di comprendere e prioritizzare i diversi adempimenti da rispettare.

3.2.1. Perimetro cibernetico: CSIRT italiano e tempestività della notifica

Con riferimento alla normativa in materia di perimetro di sicurezza nazionale cibernetica, i soggetti inclusi nel perimetro dovranno, *in primis*, verificare se l'attacco ha coinvolto uno dei beni ICT rilevanti ai sensi del decreto legge e, *in secundis*, riportare l'incidente subito nella corretta categoria alla luce della tassonomia indicata nell'Allegato A del DPCM 2. Se, infatti, una risposta positiva al primo quesito determinerà l'applicabilità della normativa di settore, è la seconda analisi sopra richiamata che consentirà alla vittima dell'attacco di determinare la specifica obbligazione. In particolare, il D.P.C.M. 2 prevede che gli eventi meno gravi dovranno essere notificati al CSIRT italiano, oggi istituito presso l'Agenzia per la cybersicurezza nazionale, entro 6 ore dalla scoperta, mentre gli eventi considerati più severi entro una sola ora dall'individuazione[48]. Inoltre, qualora il soggetto incluso nel perimetro venga a conoscenza di nuovi elementi significativi a seguito di ulteriori indagini circa l'evento, la notifica dovrà essere tempestivamente integrata, oltre a dover chiaramente aggiornare il CSIRT in caso di richieste di chiarimenti, entro un termine di sole sei ore da tale richiesta[49].

3.2.2 Normativa GDPR: il data breach e la valutazione del rischio per gli interessati

Più complessi gli adempimenti relativi alla normativa in materia di prote-

[48] Art. 3, D.P.C.M. 2.
[49] *Id.*

zione dei dati personali che richiedono alcune valutazioni preliminari e, in primo luogo, la necessità di comprendere se l'incidente di sicurezza sia o meno qualificabile anche come *data breach*. Come già sopra richiamato, infatti, sebbene tutti i *data breach* costituiscano incidenti di sicurezza, non è necessariamente vero il contrario[50]; pertanto, sarà opportuno verificare se l'evento abbia riguardato o meno dati personali al fine di comprendere se troverà applicazione la normativa GDPR.

Successivamente, sarà peraltro altresì necessario verificare se l'evento abbia causato o possa ragionevolmente comportare un rischio per i diritti e le libertà degli interessati, venendo meno in caso contrario gli obblighi di notifica. Pertanto, se nel caso della normativa in materia di Perimetro di sicurezza nazionale cibernetica, proprio in ragione degli interessi nazionali tutelati, poco margine è lasciato alla società vittima dell'attacco, la normativa GDPR mantiene quale principale linea guida il principio di *accountability*, rimettendo la propria applicabilità alle valutazioni, motivate, del titolare.

Come anticipato, un *personal data breach* consiste in una "*violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*"[51]. Il legislatore ha voluto così adottare una definizione di violazione di dati personali il più ampia possibile che includesse, da un lato, gli eventi dovuti a un attacco esterno che quelli dovuti a cause "interne"[52] e, dall'altro, conseguenze tanto diverse quanto la distruzione, il danneggiamento, la perdita, e l'accesso o divulgazione dei dati personali a terzi non autorizzati[53].

Da un punto di vista classificatorio, già nel 2014, il WP29 aveva chiarito come le violazioni di dati personali potessero essere suddivise in *confidentiality, integrity* o *availability breach*[54] a seconda proprio del tipo conseguenza che caratterizza l'incidente[55]. In particolare, nel caso dei *ransomware*, che costituiscono il *focus* del presente commento, si è detto che l'attacco è caratterizzato dall'utilizzo di un codice *malware* finalizzato a criptare e

[50] WP250, p. 7.

[51] Articolo 4, par. 1, num. 12, GDPR.

[52] A tal riguardo, il WP29 ha chiarito come "*a security incident is not limited to threat models where an attack is made on an organisation from an external source, but includes incidents rom internal processing that breach security principles*" – *Guidelines on Personal Data Breach*, nota 13.

[53] *Ivi*, p. 7.

[54] Vd. WP29, *Opinion 3/2014 on Personal Data Breach Notification*, 25 marzo 2014, WP213.

[55] In tal senso, si avrà una violazione della riservatezza in caso di divulgazione o accesso non autorizzati di dati personali, una violazione dell'integrità in caso di modifica non autorizzata o accidentale e, infine, una violazione della disponibilità in caso di perdita di accesso o distruzione dei dati personali (Vd. *Guidelines on Personal Data Breach*, p. 7).

rendere conseguentemente indisponibili i dati personali al titolare, dietro la promessa di decriptarli previo pagamento del riscatto. Si intuisce come tale tipologia di attacco costituisca anzitutto un *availability breach*, in quanto obiettivo primario di ogni *ransomware attack* è proprio quello di sottrarre la disponibilità dei dati al titolare. Tuttavia, come descritto nei paragrafi precedenti, in molte ipotesi, con la progressiva sofisticazione di tale categoria di *software* malevoli, l'attaccante mira sempre più spesso anche ad accedere e/o esfiltrare i dati, rientrando in tal caso l'evento, a pieno titolo, anche nella definizione di *confidentiality breach*.

3.2.3 La valutazione del rischio degli interessati

Una volta verificato che l'incidente subito si qualifichi quale violazione di dati personali, il titolare dovrà procedere con la fondamentale valutazione circa la gravità dello stesso alla luce del primario criterio del rischio per gli interessati. Come evidenziato, infatti, l'obbligo di notifica al Garante per la protezione dei dati personali e agli interessati dipenderà dalla valutazione del rischio per i diritti e le libertà degli interessati connesso al *data breach*[56], che si pone dunque come fondamentale parametro per determinare le obbligazioni in capo alla società vittima dell'attacco.

Nonostante la rilevanza della nozione di "*rischi per i diritti e le libertà delle persone fisiche*"[57], la disciplina vigente non ne fornisce una definizione, né tantomeno chiarisce cosa debba intendersi per "*rischio elevato*"[58].

A tal riguardo, i considerando del GDPR offrono una prima indicazione utile di quali rischi il titolare debba considerare, tra cui in particolare la possibilità che la violazione di dati personali possa causare danni fisici, materiali o immateriali agli interessati, comportare una limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, perdita di riservatezza dei dati personali protetti da segreto professionale o ogni altro danno economico o sociale significativo[59]. Inoltre, dalla lettura del Considerando 76, GDPR, si evince che la valutazione del rischio deve considerare tanto la probabilità quanto la gravità del rischio per i diritti e le libertà degli interessati[60], che dovranno essere determinate in

[56] A tal proposito, si ricorda come, in generale, una violazione di dati personali dovrà essere notificata al Garante salvo che sia improbabile che essa comporti un rischio per i diritti e le libertà degli interessati, mentre dovrà essere notificata direttamente a questi ultimi qualora il rischio sia elevato.

[57] Articolo 33, GDPR.

[58] Articolo 34, GDPR.

[59] Si vedano Considerando 75 e 86, GDPR.

[60] Considerando 76, GDPR. Si veda anche *Guidelines on Personal Data Breach*, p. 23.

considerazione della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e sulla base di una valutazione oggettiva[61]. Infine, il WP29, nelle Guidelines on Personal Data Breach, ha chiarito che, a seguito dell'accertamento di una violazione di dati personali, il titolare dovrà valutare la gravità del rischio per i diritti degli interessati alla luce di diversi criteri quali la tipologia di *data breach* (*i.e.*, se abbia comportato una perdita di confidenzialità, disponibilità e/o integrità dei dati personali), la natura, il carattere sensibile e il volume di dati personali coinvolti, la facilità di identificazione degli interessati, la quantità delle persone fisiche coinvolte e la loro eventuale vulnerabilità, nonché eventuali particolari caratteristiche del titolare. Il WP29 ha altresì specificato che qualora il *data breach* riguardi categorie particolari di dati personali, il rischio per i diritti e le libertà degli interessati dovrà senz'altro essere considerato probabile, ferma restando la valutazione circa la sua gravità[62].

3.2.4 Gli use case *dell'EDPB: un parametro per le valutazioni dei titolari*

Con specifico riferimento agli attacchi ransomware, alcune valutazioni sono state esemplificate dall'EDPB nelle *Guidelines 01/2021 on Examples regarding Personal Data Breach Notification*[63] ("**Guidelines 01/2021**"). Sebbene gli *use cases* indicati dall'EDPB coprano, inevitabilmente, un novero di ipotesi estremamente limitato rispetto alla vasta applicazione offerta dalla prassi, risulta comunque utile un'analisi ragionata di tali esempi al fine di comprendere le valutazioni che dovranno essere compiute da ogni titolare vittima di un attacco ransomware.

La prima ipotesi analizzata dall'EDPB[64] consiste in un *ransomware attack* compiuto a danno di dati personali comuni, protetti da criptazione di ultima generazione da parte del titolare, la cui chiave crittografica non è stata compromessa nell'attacco. Inoltre, l'attacco esemplificato dall'EDPB prevede esclusivamente la cifratura dei dati senza alcuna esfiltrazione degli stessi da parte dell'attaccante. I dati personali coinvolti sono alcune decine e, grazie a un *backup* immediatamente disponibile, è possibile ripristinare l'accesso a tutti i dati criptati in poche ore, con ciò evitando ogni paralisi delle operazioni quotidiane della società e ogni ritardo nel pagamento dei dipendenti e/o nel gestire le richieste dei clienti.

[61] Considerando 76, GDPR.
[62] Vd. *inter alia*, *Guidelines on Personal Data Breach*, p. 25
[63] EDPB, *Guidelines 01/2021 on Examples regarding Personal Data Breach Notification*, 14 dicembre 2021, v. 2.0.
[64] Vd. *Guidelines* 01/2021, CASE no. 01.

Tale ipotesi, che si pone – sia per il ridotto numero degli interessati coinvolti, sia per l'impossibilità da parte dell'attaccante di accedere ai dati personali – tra gli esempi di attacchi a bassa intensità, costituisce un mero *breach of availability*. Peraltro, rileva notare come, sebbene estremamente limitato nel tempo, l'attacco vada ugualmente qualificato come *data breach* in quanto, come chiarito dal WP29, anche una indisponibilità estremamente limitata nel tempo dei dati personali costituisce una violazione ai sensi del GDPR[65]. Ciononostante, le misure adottate precedentemente all'attacco e la capacità di reagire prontamente allo stesso onde evitare conseguenze ulteriori per gli interessati, consentono in una tale ipotesi di ritenere il rischio per gli individui limitato, in quanto esclusivamente connesso a una temporalmente limitata indisponibilità dei dati dalla quale non seguirebbero conseguenze dannose. Conseguentemente, non risulterà necessario effettuare la notifica al Garante né procedere alla comunicazione agli interessati coinvolti[66].

Il secondo esempio di *ransomware attack* ipotizzato dall'EDPB[67] si differenzia dal precedente non tanto per la gravità dell'attacco in sé quanto, piuttosto, per le conseguenze da esso derivanti a causa delle misure di sicurezza precedentemente adottate dal titolare. Nello *use case* n. 2, infatti, sebbene siano stati criptati (e non esfiltrati), al pari dell'esempio precedente, esclusivamente dati personali comuni relativi a poche decine di interessati, l'assenza di backup in formato elettronico idonei a ripristinare in tempi rapidi l'accesso dei dati coinvolti, impone un tempo di ripristino di cinque giorni; inoltre, in assenza di misure di criptazione adottate dal titolare, la possibilità di qualificare l'evento anche come un *breach of confidentiality* non potrebbe essere del tutto esclusa. Tali differenze sono, nella valutazione ipotizzata dall'EDPB, sufficienti per giustificare la necessità di notificare l'evento all'Autorità competente, sebbene non ai singoli interessati coinvolti in assenza di un rischio elevato. Come già discusso nei paragrafi precedenti, questo esempio dimostra quindi come, anche da un punto di vista esclusivamente legale della gestione degli eventi informatici, un'adeguata preparazione *pre-incident* consente di sgravare il titolare, in uno scenario *post-incident*, di numerosi adempimenti che, come noto, potrebbero altresì condurre a una sanzione amministrativa.

Le ultime due casistiche esemplificate dall'EDPB si pongono, senza lasciare peraltro particolari dubbi, nella parte finale di un ipotetico spettro di gravità

[65] *Guidelines on Personal Data Breach Notification*, p. 8

[66] Si veda anche, per una conferma, *Guidelines 01/2021*, par. 25.

[67] *Ivi,* CASE No. 02.

degli attacchi *ransomware*. Nel *CASE No. 03*[68], il titolare coinvolto è un ospedale/struttura sanitaria e la cifratura dei dati personali riguarda migliaia di interessati, tra cui numerosi pazienti le cui operazioni soffrono ritardi e cancellazioni a causa dell'indisponibilità dei dati. Nel *CASE No. 04*[69], invece, si assiste a una cifratura ed esfiltrazione di dati di contatto, documenti d'identità e informazioni relativi a carte di credito di migliaia di individui; inoltre, anche il backup dei dati risulta coinvolto nell'attacco. È evidente come, in entrambi i casi, sia per la sensibilità dei dati personali coinvolti che per le carenti misure di ripristino adottate, nella fase *pre-incident*, dal titolare, le conseguenze nei confronti degli interessati rischiano di essere estremamente elevate, pertanto giustificando non solo la notifica all'Autorità di controllo ma anche agli interessati coinvolti[70].

3.2.5 Esito delle analisi: gli adempimenti ai sensi del GDPR

Questa sintetica disamina delle casistiche *ransomware* con implicazioni *data protection* offerta dall'EDPB consente di comprendere come, a seguito della qualificazione dell'incidente quale *data breach*, il titolare debba attivare tutte le funzioni interne, con competenze sia legali che tecnologiche, al fine di comprendere, in concreto, e in una valutazione *case by case*, quali possano essere gli impatti per i diritti e le libertà degli interessati. In particolare, nell'ambito di tale valutazione, il titolare dovrà senz'altro comprendere la natura della violazione, le categorie e il numero di dati personali e interessati coinvolti, nonché le conseguenze per i diritti e le libertà di questi ultimi[71].
Ad esito di tale analisi, e sulla base dei risultati di quest'ultima, la società vittima dell'attacco dovrà, da un lato, adottare tutte le misure tecnico-procedurali necessarie per porre rimedio alla violazione ed eliminarne o attenuarne gli effetti negativi. Dall'altro lato, e dal punto di vista più prettamente legale, sarà necessario decidere circa la necessità/opportunità di notificare l'evento al Garante per la protezione dei dati personali e/o agli interessati coinvolti, e formalizzare tali valutazioni in appositi documenti di *accountability*.
A prescindere, infatti, dall'esito delle valutazioni e della gravità dell'evento, il principio di *accountability*, previsto in via generale all'articolo 5, GDPR, continua ad operare come linea guida principale per tutti i titolari del trat-

[68] *Ivi*, par. 36 ss.
[69] *Ivi*, par. 41 ss.
[70] Vd. *Ivi*, par. 39 e 46.
[71] Si noti che tali elementi costituiscono altresì informazioni necessarie da fornire al Garante per la protezione dei dati personali nel caso in cui si decida di procedere con la notifica ai sensi dell'articolo 33, GDPR.

tamento. Nello specifico caso dei *data breach* è, peraltro, lo stesso articolo 33, par. 5, GDPR che richiede l'adozione di un registro in cui documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio, a prescindere da ogni ulteriore valutazione[72]. Peraltro, tale documentazione interna consentirà anche al titolare di dimostrare, in caso di ispezione dell'Autorità di controllo, di aver posto in essere tutte le misure idonee a gestire i rischi derivanti dall'incidente.

3.3 Strategia comunicativa e danni reputazionali

Un aspetto talvolta poco considerato ma con effetti di primaria importanza nella gestione dei un attacco informatico consiste con la strategia di comunicazione adottata dalla società. Un evento informatico avverso espone infatti, indubbiamente, l'organizzazione a danni reputazionali, derivanti sia dalla percezione di inefficaci misure di sicurezza e quindi di potenziale esposizione delle informazioni affidate alla società vittima dell'attacco, sia, più in generale, a valutazioni connesse all'eventuale pagamento del riscatto, che come argomentato in precedenza potrebbe poi essere collegato al finanziamento di organizzazioni criminali o terroristiche.

Una strategia comunicativa consolidata è pertanto di fondamentale importanza per evitare o arginare ingenti danni reputazionali, soprattutto in caso di eventi particolarmente significativi, come ad esempio attacchi ransomware diffusi o Distributed Denial of Service (DDoS)[73].

Uno studio interno condotto da PwC nel corso del 2021 ha mostrato come la comunicazione, per potersi definire efficace, debba contenere almeno i

[72] Si noti peraltro che il WP29 raccomanda di dare espressa evidenza del ragionamento alla base delle decisioni prese in risposta a una determinata violazione, anche e soprattutto laddove si sia deciso di non provvedere alla relativa notificazione, fornendo specifica indicazione dei motivi per cui il titolare/responsabile non ha ritenuto la violazione potenziale causa di rischi per i diritti e le libertà degli individui (vd. *Guidelines on Personal Data Breach*, p. 27).

[73] Un esempio di strategia comunicativa efficace e degli effetti positivi nella percezione dell'evento subito è offerto dal *ransomware attack* subito da Luxottica a settembre 2020, che ha portato all'interruzione delle attività produttive. Sebbene, la chiusura degli strumenti informatici abbia consentito di respingere l'attacco e di isolare il malware prima che questo potesse compromettere l'infrastruttura o comportare la perdita di dati e informazioni riservate, le attività di *containment* ed *eradication* sono state avviate troppo tardi, consentendo al gruppo Nefilim di fare una copia dei *database* attaccati, cifrare i dati di *backup* e vandalizzarne il contenuto. Una vera e propria *debacle digitale* che, tuttavia, non è stata percepita dal pubblico proprio grazie a una strategia comunicativa efficace e tempestivamente gestita, che ha consentito di focalizzarsi sugli aspetti positivi delle misure adottate (Per maggiori informazioni sull'attacco citato vd. P. Tarsitano, *Attacco ransomware blocca Luxottica, ma la reazione è da manuale: ecco perché* in *Cybersecurity360*, 22 settembre 2020, bit.ly/3kyKM4G e A. Longo, *Attacco Luxottica: c'è stato furto di dati, la conferma* in *Cybersecurity360*, 26 ottobre 2020, bit.ly/3OQaZtz.

seguenti elementi: (i) dinamiche dell'evento mediante l'utilizzo di una chiara linea temporale; (ii) tipologia di attaccante e profilo tecnico del ransomware; (iii) modalità di gestione dell'evento; (iv) eventuale coinvolgimento delle autorità; e (v) Cyber Awareness verso gli *stakeholder*.

Naturalmente, sebbene sia raccomandabile non fornire troppi dettagli tecnici o sensibili, specie in una fase iniziale, è altrettanto importante rendere i propri clienti e il pubblico consapevoli di quanto stia avvenendo, senza negare l'evento o sminuirne l'effettiva portata. Allo stesso tempo, sarà necessario evitare il fenomeno della "caccia al colpevole", specie nel caso in cui non si abbiano informazioni sufficienti, ed evitare il rischio di diffondere ipotesi azzardate e inverosimili.

Si richiede dunque una divulgazione responsabile della notizia e dell'evento e anche, ogniqualvolta ciò sia possibile, un aggiornamento relativo alla gestione dello stesso.

In quest'ottica è importante l'identificazione – preferibilmente già in una fase di *pre-incident* – all'interno dell'azienda di un punto di contatto, o *Point of Contact* (POC)[74], a cui attribuire l'onere di comunicare con l'esterno così come la scelta dello strumento con cui comunicare (ad esempio, *social network* come LinkedIn o Twitter), o dell'interlocutore a cui affidare la narrazione dei fatti (ad esempio, riviste specifiche di settore, quotidiani, agenzie di stampa, radio)[75].

4. Conclusione

La crescita delle infrastrutture ICT e delle infrastrutture di automazione degli impianti industriali o analoghi ha fornito a enti pubblici e privati una

[74] L'individuazione di un Point of Contact responsabile della comunicazione con l'esterno viene riportata anche all'interno dello standard "NIST.SP. 800.62" così come all'interno dell'"ISF – Standard of Good Practice for Information security 2020".

[75] Peraltro, un seppur diverso tipo di comunicazione – rientrante più propriamente nell'ambito della collaborazione tra imprese –è stata presa in considerazione anche dal legislatore che, con la Direttiva (UE) 2016/1148 (c.d. Direttiva NIS) ha previsto la comunicazione di un "Extintion Level Attack" tra società operanti all'interno di uno stesso settore. Inoltre, sia con la Direttiva NIS sia, successivamente, con l'emanazione del Regolamento DORA, i legislatori hanno sottolineato l'importanza di condividere i dati inerenti gli attacchi con altre organizzazioni affini in modo da disporre di informazioni aggiuntive per gestire l'attacco, oltre che a fornire delle *lesson learned* affinchè altre organizzazioni possano rispondere prontamente ove dovessero concretizzarsi scenari analoghi o simili. Spesso gli "Extintion Level Attack" possono infatti interessare più società contemporaneamente, rendendo la collaborazione all'interno di una ampia rete di organizzazioni affini particolarmente efficace al fine di comprendere le strategie da adottare e condividere informazioni dedotte dallo studio delle TTP (tattiche, tecniche e procedure) utili per la risoluzione dell'evento.

possibilità impareggiabile di sviluppare processi più efficienti e raggiungere i propri obiettivi con maggiore rapidità e a costi più contenuti. Al tempo stesso, tuttavia, la progressiva tendenza a sfruttare Internet come strumento fondamentale per le proprie attività e, in particolare, per l'accesso, il trasferimento e la conservazione di informazioni e dati (personali e non) ha esposto società ed enti pubblici a nuove minacce, di natura cibernetica. In particolare, negli ultimi anni si è assistito a una esponenziale crescita degli attacchi ransomware, finalizzati peraltro non più esclusivamente a criptare le informazioni contenute sui server attaccati al fine di ottenere il pagamento del riscatto, ma anche a esfiltrare informazioni e sfruttarle per perpetrare la minaccia anche verso i soggetti cui tali informazioni fanno riferimento.

Come rilevato, la natura estremamente complessa di un attacco ransomware presenta rischi non solo economici e operativi ma anche legali e reputazionali. Per tale motivo è necessario che le organizzazioni esposte adottino un approccio multidisciplinare per la gestione preventiva e successiva di un evento ransomware.

In primo luogo, è opportuno effettuare una analisi di *compromise discovery* finalizzata a determinare con precisione le minacce a cui l'organizzazione risulta esposta, anche al fine di pianificare opportunamente le successive attività.

Inoltre, ogni organizzazione dovrebbe dotarsi di una *governance structure*, che preveda un tavolo operativo *ad hoc* composto da professionisti legali, di sicurezza informatica, *business continuity* ed esperti di comunicazione, al fine di poter fronteggiare in maniera efficace un potenziale attacco ransomware. Peraltro, nel prepararsi a un potenziale attacco cibernetico e nell'adottare le misure finalizzate a scongiurare tale rischio, sarà necessario tenere sempre in considerazione quale principale bussola legale i framework normativi di riferimento e, principalmente, il GDPR e, ove applicabile, la normativa in materia di perimetro di sicurezza nazionale cibernetica.

In uno scenario *post-incident*, la società vittima dell'attacco dovrà seguire le procedure adottate e, in primo luogo, attivare il tavolo operativo costituito per la gestione di eventi ransomware. A seguito di interventi di *immediate rescue*, sarà poi necessario adottare tutte le misure tecniche e legali finalizzate a gestire l'evento e mitigare il rischio per l'azienda ma anche per i diritti e le libertà di terze parti, in primo luogo eventuali interessati coinvolti.

Da un punto di vista più propriamente giuridico, risulta di fondamentale importanza avviare sin da subito una collaborazione con le Autorità di volta in volta competenti. In particolare, qualora la violazione consista altresì in un *data breach*, verificare la necessità e/o opportunità di notificare lo stesso

al Garante per la protezione dei dati personali risulterà prioritario, sia per evitare procedimenti sanzionatori, sia per avviare un approccio collaborativo con l'Autorità. Ancora più stringenti, da un punto di vista cronologico, gli adempimenti di notificazione per le società incluse nel perimetro di sicurezza nazionale cibernetica, che dovranno procedere alla notificazione al CSIRT italiano entro una o sei ore dalla scoperta dell'incidente.

È ormai noto tra gli operatori del settore che evitare un attacco informatico equivale a una *mission impossible*. Tuttavia, è certamente possibile, oltre che doveroso, adottare un adeguato sistema di prevenzione finalizzato a mitigare tale rischio e ad assumere tutte quelle misure fondamentali, qualora l'evento si dovesse realmente verificare, per gestire l'incidente con celerità ed efficacia al fine di arginarne i possibili effetti ed evitare conseguenze economiche, operative, sanzionatorie e risarcitorie.