FORNARI E ASSOCIATI
STUDIO LEGALE

FOCUS

Ransomware: prevenzione e reazione

fornarieassociati.com

Milano • Roma • Bari

Agosto 2023

PREMESSA.

Varcata la soglia di una azienda o di un ente pubblico per dare inizio alla giornata lavorativa, ci si rende conto che i *personal computers* non sono funzionanti: sono bloccati in una schermata su cui compare unicamente l'avviso di essere vittima di un attacco hacker, l'eventuale nome in gergo degli autori dell'attacco e, componente essenziale, la richiesta di inoltrare una determinata quantità di *bitcoin* (o altra valuta virtuale) ad un preciso *wallet* in *blockchain*.

Si è vittima di un *ransomware attack*. Una risorsa vitale per la produttività aziendale – i dati informatici – sono stati, nel migliore dei casi, criptati, e, nel peggiore dei casi, criptati ed esfiltrati: sono dunque per certo inaccessibili e, potenzialmente, nella disponibilità di terzi.

Da questo momento, il *management* ha poche ore per compiere importanti decisioni strategiche, che possono significativamente condizionare gli esiti dell'attacco informatico e i danni subiti dalla persona giuridica amministrata:

- è possibile recuperare i dati aziendali da un precedente backup locale e recente, o questi sono da considerarsi irrimediabilmente inaccessibili?

- è necessario denunciare il fatto alle Autorità? Come gestire le notificazioni dovute al Garante Privacy ai sensi della normativa GDPR?

- è necessario pagare il riscatto in favore dei criminali per rientrare in possesso dei dati? Quali le conseguenze giuridiche ed economiche dell'eventuale pagamento?

- quali professionisti possono essere di aiuto nella calibrazione della miglior strategia difensiva?

- in che modo è possibile prevenire un *ransomware attack*?

Con ogni evidenza, il *ransomware attack* è un evento dal grande impatto economico ed emotivo, il quale richiede oculate valutazioni da compiersi in un contesto convulso e condizionato dall'urgenza.

A seguire, dei brevi appunti per una strategia di prevenzione e reazione.

1. COS'È UN RANSOMWARE?

Il ransomware è un tipo di *malware* (*malicious software*) che, introdotto in dispositivi informatici, può rubare informazioni, aprire le porte a controlli remoti o, attraverso tecniche di cifratura dei file, rendere inutilizzabili documenti, archivi, immagini e qualunque altro *file* memorizzato sul disco fisso.

Un attacco ransomware, oltre a compromettere singoli dispositivi informatici, può mirare alla compromissione di una intera rete informatica (*e.g.* la rete informatica aziendale), espandendosi al server centrale e ai sistemi collegati.

Il virus, dopo aver criptato i file informatici, trasmette sulla schermata della vittima una richiesta di riscatto – che nella maggior parte dei casi dovrà essere corrisposta in bitcoin o in altra valuta virtuale – finalizzata al recupero dei dati e, spesso, anche a garanzia della riservatezza dei file esfiltrati. In assenza del pagamento del riscatto, i dati aziendali potrebbero risultare definitivamente inaccessibili ed essere divulgati a terzi.

Breve: i ransomware sono dei *trojan horse* crittografici finalizzati all'estorsione di somme di denaro.

2. QUANTO È DIFFUSO IL FENOMENO?

In tempi recenti, la frequenza e la portata degli attacchi ransomware hanno registrato un significativo incremento.

Già nel 2016, la US Federal Trade Commission (FTC) definiva il ransomware come "*una delle minacce online più gravi per le persone e le aziende*", nonché "*la forma più redditizia di malware utilizzata dai criminali*".

Più recentemente, un report pubblicato dall'Agenzia dell'Unione europea per la cybersicurezza (ENISA) ha rivelato come, nel periodo maggio 2021-giugno 2022, circa 10 terabyte di dati sono stati esfiltrati ogni mese da hacker specializzati in attacchi ransomware. Significativamente, il report individua, tra i Paesi più colpiti dai cybercriminali, gli Stati Uniti, seguiti da Germania, Francia e Italia.

Alla recente accelerazione del fenomeno ha senz'altro contribuito la diffusione di soluzioni *RaaS* (*Ransomware as a Service*), le quali, reperibili nel dark-web, permettono lo sviluppo di attacchi ransomware anche da parte di soggetti privi delle necessarie competenze informatiche: in questo caso, invero, l'attacco viene portato a termine da soggetti qualificati per conto dei mandanti; il tutto a fronte del pagamento di una *flat-fee* o di una percentuale del riscatto ricavato dall'illecito.

Emerge la tendenza dei cybercriminali a bersagliare soggetti ai quali è possibile estorcere somme di denaro consistenti: *in primis*, aziende e enti pubblici. Ciò con evidenti danni al tessuto produttivo del Paese coinvolto e pregiudizi all'esercizio delle funzioni necessarie a garantire il *welfare* nazionale.

A titolo di esempio – stando a una ricerca della società multinazionale Trend Micro (svolta nei mesi di maggio e giugno 2022 e che ha coinvolto 2.958 IT Decision Makers in 26 Paesi)

– delle organizzazioni colpite da un attacco *ransomware*, il 25% ha affermato di aver dovuto interrompere completamente le operazioni a causa dell'attacco informatico, mentre il 60% ha rivelato che alcuni processi aziendali hanno dovuto subire modifiche in seguito all'attacco. La maggior parte delle organizzazioni ha impiegato giorni (56%) o settimane (24%) per ripristinare le operazioni. Inoltre, il 60% del campione ha ammesso di aver subito il furto di dati sensibili, aumentando così i rischi legati alla *compliance*, i danni reputazionali e i costi di indagine, riparazione e pulizia.

3. LA SITUAZIONE ITALIANA?

L'Agenzia per la Cybersicurezza Nazionale (ACN) ha osservato 130 attacchi ransomware in danno di Pubbliche Amministrazioni e operatori privati nel corso del 2022.

È tuttavia verosimile ritenere che tale dato rappresenti soltanto una parte del numero complessivo degli attacchi ransomware effettivamente avvenuti in Italia: in alcuni casi le vittime – in particolar modo se appartenenti al tessuto produttivo delle Piccole Medie Imprese, spesso sprovviste di *know-how* e strutture interne dedicate – sono (imprudentemente) inclini a non segnalare gli attacchi subiti.

I settori più colpiti nel nostro Paese sono quello manifatturiero, seguito dal tecnologico, dal *retail* e dal settore sanitario. Inoltre, anche in Italia - in linea con quanto avviene nel resto del mondo - gli attacchi ransomware alle Pubbliche Amministrazioni sono in continuo aumento.

Da un punto di vista geografico, le zone maggiormente interessate dal fenomeno corrispondono alle grandi aree metropolitane di Roma, Milano, Torino e ai distretti manifatturieri del Nord Ovest e Nord Est.

4. QUALI FATTISPECIE DI REATO INTEGRA L'ATTACCO RANSOMWARE?

Non vi è dubbio che un attacco ransomware integri il delitto di *estorsione* previsto e punito dall'art. 629 c.p.

Si ravvisano poi ulteriori fattispecie delittuose che, a seconda dei casi, potrebbero essere oggetto di possibile contestazione nei confronti dell'autore di un attacco ransomware, tra cui: *i*) Accesso abusivo ad un sistema informatico o telematico *ex* art. 615 *ter* c.p.; *ii*) Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici *ex* art. 615 *quater* c.p. *iii*) Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico *ex* art 615 *quinquies* c.p.; *iv*) Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche *ex* art. 617 *quater* c.p.; *v*) Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità *ex* art. 635 *ter* c.p.

5. COSA PREVEDE IL GDPR IN CASO DI *DATA BREACH*?

Può essere definito quale *data breach* un evento – quale il *ransomware attack* – in grado di compromettere la riservatezza, l'integrità o la disponibilità dei dati personali.

L'art. 33 del GDPR prevede l'obbligo per il titolare del trattamento (*data controller*) di notificare il *data breach* – senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza – al Garante per la protezione dei dati personali.

La notifica della violazione deve: *i*) descrivere la natura del *data breach* (numero e categorie di soggetti e dati coinvolti); *ii*) descrivere le probabili conseguenze derivanti dalla violazione dei dati; *iii*) descrivere le misure adottate o che il titolare del trattamento adotterà per porre rimedio alla violazione dei dati personali e attenuarne gli effetti negativi. Ove la suddetta comunicazione fosse tardiva, il titolare del trattamento deve fornire una motivazione adeguata, pena l'irrogazione di una sanzione. Naturalmente, sanzioni sono altresì previste in caso di omessa notifica.

La segnalazione al Garante non è necessaria qualora il titolare del trattamento ritenga che il *data breach* occorso non comporti rischi per i diritti e le libertà delle persone fisiche. In questa ultima ipotesi, il titolare si potrà limitare a tenere nota dell'avvenuta violazione, così da consentire all'Autorità di effettuare eventuali verifiche circa il rispetto della normativa.

È bene rilevare che - complice la stretta tempistica imposta dalla normativa - il titolare del trattamento non deve attendere un esame forense dettagliato e/o le prime misure di mitigazione per valutare se la violazione dei dati debba essere notificata o meno: la valutazione dovrà essere effettuata nel momento in cui si ha contezza della violazione.

Ai sensi dell'art. 34 GDPR, nel caso in cui la violazione comporti un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve notificare il *data breach* senza ingiustificato ritardo anche agli interessati (*i.e.* i *data subjects*: soggetti a cui si riferiscono i dati personali coinvolti nel *breach*). Al tempo stesso, la medesima disposizione normativa contempla tre distinte deroghe all'obbligo di notifica del *data breach* ai soggetti interessati:

I. il titolare del trattamento ha messo in atto adeguate misure tecnico/organizzative di protezione, e tali misure erano state applicate ai dati personali oggetto di violazione in un momento antecedente al *data breach* (in particolare quelle misure, quali la cifratura, destinate a rendere i dati personali inaccessibili a soggetti non autorizzati);

II. il titolare del trattamento ha adottato, successivamente al *data breach*, misure atte a scongiurare il materializzarsi di un rischio elevato per i diritti e le libertà degli interessati;

III. la comunicazione ai singoli interessati richiederebbe uno sforzo sproporzionato. In tal

caso, tuttavia, è necessario procedere a una comunicazione pubblica o ad altra comunicazione idonea ad informare i *data subjects* con analoga efficacia.

Di seguito si riportano, in sintesi, alcuni esempi di *data breach* con associati i relativi obblighi di notifica, così per come ricostruiti dal Comitato europeo per la protezione dei dati (*European Data Protection Board*: "EDPB") tramite le linee guida n. 01/2021:

I. attacco ransomware che colpisce dati criptati senza coinvolgere dati sensibili. Inoltre, il backup è adeguato e i dati non sono stati esfiltrati.

   In una siffatta ipotesi non è necessaria la notifica al Garante né tantomeno alcuna comunicazione agli interessati: è improbabile che la violazione comporti un rischio per le libertà e i diritti dei *data subjects* poiché i dati (inaccessibili ai criminali, poiché adeguatamente criptati) possono essere ripristinati rapidamente grazie al backup;

II. attacco ransomware senza esfiltrazione di dati. Non vi è un adeguato backup e neppure una criptazione dei dati.

   In questa circostanza, è necessaria la notifica al Garante; tuttavia, non è necessario comunicare il *breach* agli interessati: sussiste il rischio per i diritti e le libertà delle persone fisiche (*non-availability* dei dati), ma senza raggiungere un livello di rischio elevato (*confidentiality* dei dati non compromessa);

III. attacco ransomware senza esfiltrazione dati ai danni di una struttura ospedaliera.

   In questo caso la violazione deve essere notificata sia al Garante sia ai soggetti interessati: sussiste un grave rischio per i diritti e le libertà dei *data subjects* a causa della natura sensibile dei dati sottratti.

6. PAGARE IL RISCATTO INTEGRA UNA CONDOTTA ILLECITA?

Il pagamento del riscatto in favore dei cybercriminali non costituisce, di per sé, una condotta illecita penalmente rilevante.

Tuttavia, è bene porre attenzione tanto alle modalità di contabilizzazione del pagamento, quanto al soggetto che viene foraggiato.

L'omesso o fittizio inserimento in bilancio del costo sostenuto per il pagamento del riscatto potrebbe configurare l'ipotesi delittuosa di "False comunicazioni sociali" (o di "False comunicazioni sociali delle società quotate") di cui agli artt. 2621 e 2622 c.c.

Inoltre, le condotte finalizzate ad occultare l'avvenuto pagamento del riscatto, ostacolando così l'attività di controllo dei soci e degli altri organi sociali, potrebbero integrare il reato previsto dall'art. 2625 c.c. di "Impedito controllo".

Parimenti, nel rapporto con le Autorità Amministrative Indipendenti, potrebbe venire in rilievo la fattispecie incriminatrice di "Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza" *ex* art. 2638 c.c.

Ove, invece, il pagamento del riscatto dovesse essere effettuato utilizzando una provvista proveniente dalla commissione di un illecito, potrebbe configurarsi il reato di riciclaggio di cui all'art. 648 *bis* c.p.

Sul versante tributario, l'Agenzia delle Entrate ha avuto modo di ribadire l'orientamento già consolidato in giurisprudenza per cui sono deducibili esclusivamente i costi inerenti all'esercizio dell'attività d'impresa, ossia i costi all'impresa imprescindibilmente e indissolubilmente correlati. Sul punto, l'Agenzia ha puntualizzato che l'onere della prova circa la stretta correlazione del pagamento con l'attività imprenditoriale gravi sul contribuente.

A tal proposito, va chiarito che la condotta della vittima dell'attacco ransomware che, al fine di detrarre fiscalmente i costi sostenuti per il riscatto, indichi in dichiarazione elementi passivi fittizi avvalendosi di fatture o di altri documenti per operazioni inesistenti – e.g. una falsa consulenza - integra la fattispecie delittuosa di cui all'art. 2 del D. Lgs n. 74/2000 "Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti".

Con riferimento ai reati appena passati in rassegna deve essere fatto un richiamo al D. Lgs. 231 del 2001. Infatti, qualora il pagamento del riscatto venisse sostenuto utilizzando risorse aziendali e nell'interesse o a vantaggio dell'ente, le fattispecie incriminatrici summenzionate potrebbero essere contestate anche alla persona giuridica.

Quanto agli enti pubblici, laddove il funzionario dovesse pagare il riscatto utilizzando risorse finanziarie della Pubblica Amministrazione, egli potrebbe incorrere in responsabilità personale per danno all'erario, salvo la prova che la condotta abbia evitato all'Amministrazione danni maggiori.

Da tenere in considerazione sono poi i rischi connessi all'identità dei soggetti sovvenzionati tramite il pagamento del riscatto.

Negli USA, i pagamenti di riscatti in favore di organizzazioni terroristiche straniere (*Foreign Terrorist Organizations: "FTOs"*) o terroristi internazionali (*Specially Designated Global Terrorists: "SDGTs"*) identificati dall'"OFAC" sono vietati per legge. Nello specifico: *(i)* i contributi finanziari alle FTOs sono preclusi ai sensi dell'art. 18 U.S.C. 2339B, poiché considerati un sostegno materiale ai gruppi terroristici; *(ii)* i trasferimenti in favore degli SDGTs costituiscono una violazione delle sanzioni economiche imposte dalla legge federale statunitense "International Emergency Economic Powers Act" (IEEPA).

Venendo allo scenario europeo, preme invece approfondire il pagamento di riscatti ransomware a gruppi di cybercriminali legati alla Russia.

Gli attacchi ransomware in Occidente sono aumentati in modo esponenziale dall'inizio della guerra in Ucraina: il fenomeno può

essere interpretato, non solo come un atto ritorsivo dello Stato russo contro le sanzioni economiche adottate, ma altresì come una precisa strategia di aggiramento di tali misure.

Per quanto di nostro interesse, il pagamento del riscatto in favore di hacker legati alla Russia potrebbe integrare un'ipotesi di aggiramento delle sanzioni previste dai Regolamenti UE nn. 269 - 883 del 2014 s.m.i., e attivare dunque le relative responsabilità penali in capo alla vittima pagante.

7. PAGARE IL RISCATTO È LA SCELTA GIUSTA?

L'attacco ransomware è un fenomeno improvviso, dal notevole impatto economico ed emotivo. Non è insolito, dunque, che le vittime del ransomware decidano di pagare il riscatto, ritenendo ciò il modo più efficace e veloce per risolvere la vicenda.

Tuttavia, sebbene il pagamento del riscatto non è una condotta di per sé illecita, tale decisione potrebbe rivelarsi inefficiente sotto il profilo economico.

È di certo probabile che i cybercriminali, una volta ottenuto il pagamento, forniscano le chiavi per decrittare e recuperare i file; tuttavia, è altrettanto probabile che questi chiedano in seguito un nuovo pagamento per non divulgare le informazioni esfiltrate al pubblico (c.d. doppia estorsione).

Un'altra argomentazione che dovrebbe dissuadere dal pagamento del riscatto è quella per cui, laddove la vittima dovesse procedere con il pagamento, essa verrebbe in seguito riconosciuta dai cybercriminali come "buona pagatrice", accrescendo così il rischio di subire attacchi futuri.

In ultimo luogo, cedere al pagamento del riscatto, ove la notizia si diffondesse tra il pubblico, avrebbe conseguenze anche sul piano reputazionale, disvelando la presunta vulnerabilità dei sistemi informatici interni all'azienda e la sopravvenuta necessità di finanziare organizzazioni criminali per il recupero dei dati.

8. COME REAGIRE AD UN ATTACCO RANSOMWARE?

Anzitutto, è fondamentale creare un gruppo di lavoro (*Incident Response Team*: "IRT") che sia capace di rispondere all'incidente informatico in modo tempestivo ed efficace.

È di basilare importanza che l'IRT sia composto da soggetti dotati di diverse e specifiche competenze, tra cui:

I. esperti di sicurezza informatica, i quali provvedano in modo tempestivo ad *i*) isolare i sistemi o i dispositivi infetti al fine di evitare un'ulteriore propagazione del ransomware; *ii*) analizzare i dati colpiti per determinare la portata dell'incidente; *iii*) disattivare gli account o chiudere le porte di rete e, infine, *iv*) ove possibile, ripristinare i dati;

II. esperti nell'ambito OSINT e *Forensic Analysis*, i quali dovranno ottenere più informazioni possibili sugli autori del ransomware e sulle modalità dell'attacco (utili non solo all'autorità giudiziaria, ma anche alla compagnia

assicurativa ove sia stata stipulata una polizza);

III. *Data Protection Consultant/Specialist*, figura basilare per agire in modo conforme alle disposizioni previste dal GDPR;

IV. *Data Protection Officer*, il quale deve essere tempestivamente coinvolto in tutti i casi di *data breach*. Il DPO svolgerà le proprie attività a stretto contatto, sia con gli eventuali altri *Data Protection Officer*, sia con l'Autorità Garante, sia con i soggetti interessati;

V. esperto di comunicazione in stato di crisi, figura utile a gestire l'incidente nel modo più oculato per la reputazione della vittima;

VI. esperto di negoziazione in ambito ransomware, figura incaricata di acquisire e gestire i rapporti con i cybercriminali;

VII. esperto di diritto penale, di *cybercrime* e di normativa AML (antiriciclaggio), professionalità imprescindibili per adottare tutti gli accorgimenti necessari sia sul versante della *compliance* sia sul fronte giudiziario. Inoltre, ove si volesse procedere con il pagamento del riscatto, gli esperti in materia penale dovranno valutare attentamente gli eventuali rischi penali correlati al pagamento;

VIII. esperto in criptovalute, il quale, ove si optasse per il pagamento, può mettere a disposizione le proprie competenze al fine di acquistare in modo lecito e sicuro le criptovalute e procedere in sicurezza con il trasferimento del denaro.

9. COME SI PREVIENE UN ATTACCO RANSOMWARE?

Com'è facilmente intuibile, la forte diffusione degli attacchi informatici è dovuta soprattutto ad una scarsa cultura della sicurezza informatica, nonché ad un livello medio/basso di alfabetizzazione digitale.

In primo luogo, è da tenere presente che l'infiltrazione del *malware* è spesso facilitata da una o più interazioni inconsapevoli di un agente interno al bersaglio. Pertanto, al fine di garantire un'efficace attività di prevenzione, è imprescindibile assicurare un'adeguata e costante formazione degli operatori che hanno accesso ai sistemi informatici. Quest'ultimi, infatti, devono conoscere la politica di sicurezza e la politica di protezione della privacy aziendale, così da possedere quel bagaglio di conoscenze utile a riconoscere una possibile minaccia, isolarla tempestivamente ed evitare che si diffonda ulteriormente.

Sotto il profilo tecnico, si raccomanda di:

I. mantenere un backup aggiornato dei file e dei dati personali, isolato dalla rete. Inoltre, applicare la regola 3-2-1 del backup: 3 copie, 2 diversi supporti di memorizzazione e 1 copia fuori sede;

II. mantenere i dati personali crittografati secondo le disposizioni del GDPR e con controlli adeguati basati sul rischio;

III. controllare gli accessi, limitare i privilegi amministrativi e utilizzare sempre il principio del privilegio minimo quando si concede qualsiasi tipo di accesso;

IV. condurre una valutazione regolare del rischio e prendere in considerazione la possibilità di stipulare un'assicurazione ransomware sulla base di siffatta valutazione;

V. in seguito ad un attacco ransomware, agire in ottica *lesson learned*: identificare le falle del proprio sistema IT che hanno reso possibile l'attacco e porvi rimedio.

Contatti

Giuseppe Fornari
Founding Partner

g.fornari@fornarieassociati.com

Nicolò Biligotti
Senior Associate

n.biligotti@fornarieassociati.com

Filippo Cacciola
Trainee Lawyer

f.cacciola@fornarieassociati.com

Milano
Via Chiossetto 18
T: +39 0254122206
E: milano@fornarieassociati.com

Roma
Piazza Adriana 5
T: +39 0622201000
E: roma@fornarieassociati.com

Bari
Via Principe Amedeo 25
T: +39 080 918 4280
E: bari@fornarieassociati.com

Fornari e Associati
www.fornarieassociati.com