UNIVERSITA' DEGLI STUDI DI ROMA TOR VERGATA

***European Digital Law of the Person, of the Contract and of the Technological Marketplace* - EUDILA**
Cattedra Jean Monnet del Progetto ERASMUS +

La Cybersecurity a livello europeo: il legame tra sicurezza informatica e protezione dei dati personali

Elisa Di Girolamo
0352153

Anno accademico 2023/2024

Sommario

Introduzione

Con uno sviluppo tecnologico sempre in maggiore crescita, la società moderna progredisce e si sviluppa interagendo con il mondo dell'*Internet*. Si parla ad oggi di *Cyberspazio*, come lo spazio virtuale nel quale utenti (e programmi) connessi fra loro attraverso una rete telematica (per es. Internet) possono muoversi e interagire per gli scopi più diversi [1].

L'incontro tra tecnologia e diritto rappresenta uno dei punti focali della società moderna. Le leggi e le legislazioni si sono adattate alle nuove tecnologie già in passato. Il diritto applicato alla sicurezza informatica, tuttavia, rappresenta un campo relativamente nuovo ed è in costante evoluzione perché dipende direttamente dalla trasformazione tecnologica, la quale però procede ad una velocità esponenziale, per cui riuscire ad essere sempre aggiornati non è affatto semplice. Dato che lo spazio virtuale rappresenta una vasta area in cui ogni giorno si stabiliscono attraverso le frontiere geografiche miliardi di interconnessioni e si scambia conoscenza a livello globale, ridisegnando il mondo ad una velocità senza precedenti, possiamo affermare che la sicurezza informatica dà vita a numerose sfide legali. In particolare, la principale sfida è legata al fatto che il diritto internazionale per un ambito come il cyberspazio, notoriamente senza confini, dovrebbe regolare aspetti come giurisdizione, arbitrato, strumenti legali e giurisprudenza sulla criminalità, regole di intervento, attribuzione, punizione ecc. per tutti gli stati contemporaneamente.

Poiché questo spazio diventa sempre più ampio (basti pensare che ognuno di noi lascia ogni giorno una quantità di dati pari a 200MB - footprint digitale - durante la navigazione su Internet) ed è condiviso tra miliardi di persone, con il passare degli anni si è ritenuto opportuno andare a regolamentare anche questo mondo, per potervi far valere diritti e doveri della società civile, norme di rispetto dell'individuo, di libertà, eguaglianza, essendo ormai una vera e propria estensione della realtà. Per come abbiamo infatti descritto il rapporto tra la società moderna e questo spazio interconnesso senza confini, possibili compromissioni di reti o attacchi hacker diventano non solo maggiormente probabili, ma la ricaduta che avrebbero sulla società e i suoi individui sarebbe decisamente rilevante. Infatti, tali attacchi possono originarsi da qualsiasi punto della catena di rete globale e molto spesso i primi colpiti sono i più fragili, coloro che meno sanno gestirsi all'interno di questo mondo digitale (vedremo in seguito i fenomeni di *phishing*, *smishing* e *vishing*), per questo diventa importante la formazione in questo ambito. Questo può dare origini a furti, truffe, inganni, a volte così gravi da compromettere le vite di chi viene preso di mira. Ovviamente non vengono colpiti solo i singoli soggetti della società, il crimine informatico attacca anche aziende, che rischiano la sottrazione del proprio patrimonio tecnologico e la privacy dei propri clienti (successivamente

studieremo un caso reale di attacco *ransomware*), nonché intere società, mettendone a rischio la sicurezza.

La cybersecurity nel contesto del diritto europeo si riferisce all'insieme di pratiche, misure tecniche, normative e organizzative volte a proteggere i sistemi informatici, le reti, i dati, le informazioni elettroniche e le comunicazioni digitali da minacce, attacchi, accessi non autorizzati, danni o distruzioni e può includere qualsiasi cosa: dai dati personali ai segreti commerciali fino alle informazioni sulla sicurezza nazionale. In ambito europeo, il diritto relativo alla cybersecurity ha l'obiettivo di garantire un livello elevato di sicurezza informatica all'interno dell'Unione Europea, tutelando sia i cittadini che le infrastrutture critiche [2] [3].

In questa tesina vedremo dapprima un quadro generale sull'evoluzione delle direttive europee a livello di cybersicurezza, a partire dalle prime, che affiorarono negli anni 2000, fino ai provvedimenti a noi contemporanei. Successivamente vedremo nello specifico come il GDPR ha contribuito a rafforzare il concetto di cybersecurity, scandagliando nel dettaglio gli articoli di nostro interesse. Introdurremo poi brevemente i concetti di Malware e Ransomware, i quali ci saranno utili per studiare i fenomeni di phishing, smishing e vishing, che mettono a repentaglio la sicurezza informatica, capendo anche come ci si può difendere da tali attacchi. Infine, vedremo degli esempi di compromissione della cybersicurezza e a quali conseguenze hanno portato, per comprendere a fondo quanto sia effettivamente rilevante nella società odierna, mantenere elevato il livello di cybersecurity.

1. Cronistoria delle normative sulla cybersecurity

Vediamo quali normative chiave per la regolamentazione della cybersecurity si sono sviluppate a livello europeo nel corso degli anni, per meglio comprendere anche quanto rapidamente il mondo digitale si sviluppi e, allo stesso tempo, quanto sia cresciuto il rischio di minacce informatiche, ma anche l'importanza delle tecnologie digitali in vari settori.

Inizi degli anni 2000:

- *Direttiva 95/46/CE*, adottata il 24 ottobre 1995, con lo specifico scopo di armonizzare le norme in materia di protezione dei dati personali per garantirne un "flusso libero" (free flow of data) e promuovere un elevato livello di tutela dei diritti fondamentali dei cittadini. Fu un primo approccio alla regolamentazione dei dati a livello europeo, pur non parlando ancora di cybersecurity (il termine specifico "cybersecurity" non compare all'interno di questi primi documenti e non comparirà fino all'elaborazione della relazione del 2008 sull'implementazione della strategia europea in materia di sicurezza del 2003) [4].
- *Regolamento (CE) 460/2004* del Parlamento europeo e del Consiglio del 10 marzo 2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA). Tale Agenzia aveva l'obiettivo di accrescere la capacità degli Stati Membri di prevenire e affrontare i problemi di sicurezza delle reti e dell'informazione e di reagirvi, di fornire assistenza e consulenza alla Commissione e agli Stati membri su questioni connesse con la sicurezza delle reti e dell'informazione e di assistere la Commissione, su richiesta, nei lavori tecnici preparatori intesi ad aggiornare e sviluppare la normativa comunitaria nel settore della sicurezza delle reti e dell'informazione [5]. Infine, l'Agenzia contribuisce a promuovere e diffondere una nuova cultura della sicurezza, affinché la questione della cybersecurity venga adeguatamente affrontata a livello europeo e soprattutto nazionale, tramite la predisposizione degli strumenti legali opportuni.

Anni tra il 2008 e 2013:

- *Direttiva 2008/114/CE* del Consiglio dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee (ECI) e alla valutazione della necessità di migliorarne la protezione.
- Nel 2009 la Commissione europea ha presentato la comunicazione relativa alla protezione delle infrastrutture critiche informatizzate [6] [7].

- *Regolamento (UE) n. 526/2013* del Parlamento europeo e del Consiglio, del 21 maggio 2013, relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460. Con questo viene istituita l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) incaricata di svolgere i compiti che le sono affidati al fine di contribuire a ottenere un elevato livello di sicurezza delle reti e dell'informazione nell'ambito dell'Unione, di sensibilizzare il pubblico riguardo alla sicurezza delle reti e dell'informazione e di sviluppare e promuovere una cultura in materia di sicurezza delle reti e dell'informazione nella società (ossia «la capacità di una rete o di un sistema d'informazione di resistere, a un determinato livello di riservatezza, a eventi accidentali o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei relativi servizi forniti o accessibili tramite tale rete o sistema») a vantaggio dei cittadini, dei consumatori, delle imprese e delle organizzazioni del settore pubblico nell'Unione, contribuendo in tal modo alla creazione e al corretto funzionamento del mercato interno [5].
- *Strategia dell'UE per la cibersicurezza: un ciberspazio aperto e sicuro* nel 2013, fu il primo passo significativo verso una politica europea sulla cybersecurity. Questo, nella sua introduzione, parla del ciberspazio e di come ritenga necessario che nell'ambiente online si applichino le stesse norme, gli stessi principi e gli stessi valori che l'Unione europea difende offline. Ribadisce l'importanza del corretto funzionamento dei sistemi informativi, essendo la tecnologia dell'informazione e delle comunicazioni la spina dorsale della crescita economica nonché una risorsa critica da cui dipendono tutti i settori dell'economia. Inoltre, evidenzia come il mondo digitale, oltre a presentare numerosi vantaggi sia contemporaneamente molto vulnerabile, sottolineando l'aumento sempre maggiore di incidenti a carico della cibersicurezza, dove i cibercriminali si avvalgono di metodi sempre più sofisticati per infiltrarsi nei sistemi informativi, rubare dati critici o ricattare imprese. Questo documento strategico segnava la volontà dell'UE di chiarire i ruoli e le responsabilità e definire gli interventi necessari per una protezione effettiva e forte e per la promozione dei diritti dei cittadini, nell'intento di fare dell'ambiente online dell'Unione l'ambiente in linea più sicuro al mondo. I principi della strategia ai quali dovrebbe essere ispirata la politica in materia di cibersicurezza a livello unionale e internazionale sono i seguenti: validità dei valori costitutivi dell'UE sia nel mondo del digitale che nel mondo fisico; protezione dei diritti fondamentali, della libertà di espressione, dei dati personali e della vita privata; accesso per tutti; governance partecipativa, democratica ed efficiente; responsabilità condivisa per garantire la sicurezza. Inoltre, delinea cinque priorità strategiche per affrontare le sfide sopra descritte: raggiungere

la ciberresilienza; ridurre drasticamente il cibercrimine; sviluppare una politica e capacità di ciberdifesa connesse alla Politica di sicurezza e di difesa comune (PSDC); sviluppare le risorse industriali e tecnologiche per la cibersicurezza; creare una politica internazionale coerente dell'Unione europea sul ciberspazio e promuovere i valori costitutivi dell'UE [8].

Anni 2016-2019

- *Direttiva (UE) 2016/1148* del Parlamento europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, ovvero la direttiva NIS (Network and Information Security). Anche questa riconosce la centralità nella società delle reti e dei sistemi e servizi informativi, e come sia essenziale che questi risultino affidabili e sicuri per le attività economiche e sociali, oltre ad evidenziare l'aumento costante della frequenza e portata degli incidenti sulla sicurezza informatica. La direttiva vuole quindi stabilire misure volte a conseguire un livello comune elevato di sicurezza della rete e dei sistemi informativi nell'Unione così da migliorare il funzionamento del mercato interno. Questa quindi impone agli Stati Membri dell'Unione europea l'adozione di una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi; istituisce un gruppo di cooperazione al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra Stati membri e di sviluppare la fiducia tra di essi; crea una rete di gruppi di intervento per la sicurezza informatica in caso di incidente («rete CSIRT - Computer Security Incident Response Team -») per contribuire allo sviluppo della fiducia tra Stati membri e promuovere una cooperazione operativa rapida ed efficace; stabilisce obblighi di sicurezza e di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali; fa obbligo agli Stati membri di designare autorità nazionali competenti, punti di contatto unici e CSIRT con compiti connessi alla sicurezza della rete e dei sistemi informativi [9].
- *Regolamento (UE) 2016/679* del Parlamento europeo e del Consiglio del 27 aprile 2016, ovvero il GDPR (Regolamento Generale sulla Protezione dei Dati). Questo ha rafforzato significativamente la protezione dei dati personali nell'UE, con importanti implicazioni per la cybersecurity. Infatti, pure essendo focalizzato principalmente sulla protezione dei dati personali, include diverse disposizioni legate alla sicurezza dei dati, il più rilevante fra tutti è probabilmente l'Articolo 32, collocato nella sezione dedicata alla sicurezza dei dati personali e che tratta in particolare, della sicurezza del trattamento dei dati [10]**.** Approfondiremo accuratamente nel capitolo successivo.

- *Regolamento (UE) 2019/881* del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»). Questo costituisce una parte fondamentale della strategia dell'UE per la sicurezza cibernetica, che mira a rafforzare la resilienza dell'Unione agli attacchi informatici, a creare un mercato unico della sicurezza cibernetica in termini di prodotti, servizi e processi e ad accrescere la fiducia dei consumatori nelle tecnologie digitali. Il Cybersecurity Act vuole garantire il buon funzionamento del mercato interno perseguendo nel contempo un elevato livello di cibersicurezza, ciberresilienza e fiducia all'interno dell'Unione, e per questo stabilisce: gli obiettivi, i compiti e gli aspetti organizzativi relativi all'ENISA e un quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza, al fine di garantire un livello adeguato di cibersicurezza dei prodotti TIC, servizi TIC e processi TIC nell'Unione, oltre che evitare la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione della cibersicurezza nell'Unione. Tra i vantaggi conseguiti si hanno: un rinforzo del ruolo dell'ENISA, garantendole un mandato permanente e consentendole di svolgere non solo compiti di consulenza tecnica, come è stato fino a prima, ma operare anche come centro di competenze nel campo della cibersicurezza, contribuire a rafforzare le capacità di cibersicurezza a livello di Unione, assistere le istituzioni, gli organi e gli organismi dell'Unione, nonché gli Stati membri e i portatori di interessi del settore pubblico e privato nel miglioramento della protezione delle loro reti e dei loro sistemi informativi, nello sviluppo e nel miglioramento delle capacità di ciberresilienza e di risposta, nonché nello sviluppo di abilità e competenze nel campo della cibersicurezza [11] [12].

Dal 2020 a oggi:

- *Direttiva UE 2022/2555* del Parlamento europeo e del Consiglio del 14 dicembre 2022 sulla sicurezza delle reti e delle informazioni, pubblicata nella Gazzetta Ufficiale dell'Unione Europea il 27 dicembre 2022 ed entrata in vigore il 16 gennaio 2023. Nata dalla revisione della precedente Direttiva NIS (UE 2016/1148), attuata in Italia con D.lgs. n. 65 del 18 maggio 2018, la NIS2 segna un altro importante passo verso la definizione della strategia per la Cybersicurezza dell'Unione Europea, con l'obiettivo di colmare alcune carenze e coordinare le risposte degli Stati membri in caso di incidenti di sicurezza, garantendo la continuità dei servizi essenziali e importanti. Le norme dell'UE in materia di cibersicurezza introdotte nel 2016 infatti, iniziavano ad apparire inadeguate, per la grande crescita del mercato digitale, per l'evoluzione delle minacce e degli attacchi cyber, sempre più specifici e sofisticati, e per la

trasformazione digitale, per questo, sono state aggiornate dalla direttiva NIS2. Questa direttiva estende l'ambito di applicazione delle norme in materia di cibersicurezza a nuovi settori e entità, in particolare si applica a tutte quelle organizzazioni che forniscono servizi identificati come essenziali o importanti per l'economia e la società europea (es.: sanità, retailer, fornitori e provider di servizi di terze parti); inoltre migliora ulteriormente la resilienza e le capacità di risposta agli incidenti degli enti pubblici e privati, delle autorità competenti e dell'UE nel suo complesso. La Direttiva NIS2 rafforza i requisiti di sicurezza, razionalizza gli obblighi di reportistica e segnalazione, e introduce misure di supervisione e requisiti di applicazione più rigorosi. Ai sensi dell'articolo 21 della NIS2, le aziende essenziali e importanti devono, tramite un approccio multirischio, implementare una serie di misure di sicurezza tecniche e organizzative, proporzionate, per contrastare le minacce informatiche, tra cui: politiche di analisi dei rischi e di sicurezza dei sistemi informatici; gestione degli incidenti; sicurezza dei dati mediante crittografia e cifratura; strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di Cybersicurezza; pratiche di igiene informatica e formazione in materia di Cybersicurezza (Cybersecurity Awareness); uso dell'autenticazione multifattore; formazione periodica su tematiche di cybersicurezza e offrire una formazione analoga ai loro dipendenti; notificare ai rispettivi CSIRT o all'autorità nazionale competente qualunque incidente che abbia impatto significativo sulla fornitura dei loro servizi; ecc. Dal punto di vista delle sanzioni in caso di inadempienza, le entità essenziali sono soggette a controlli e multe più severe di quelle importanti.

Gli obblighi diverranno a tutti gli effetti applicabili dal giorno successivo alla data stabilita per il recepimento della Direttiva da parte degli Stati Membri, fissata per il 17 ottobre 2024. [13]

- Negli ultimi anni, l'UE ha continuato a lavorare su nuove misure legislative e iniziative per migliorare ulteriormente la cybersecurity. Per citare un esempio recente, lo scorso 13 dicembre 2023 è stato emanato il *Regolamento (UE, Euratom) 2023/2841* del Parlamento europeo e del Consiglio, che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione, entrato pienamente in vigore a partire dal 7 gennaio 2024. Il Regolamento pone particolare attenzione alla sicurezza dei sistemi informativi e di rete che gestiscono informazioni classificate dell'Unione Europea (ICUE): i soggetti dell'Unione che trattano ICUE dovranno infatti aderire a quadri normativi completi per la protezione di tali dati, incorporando meccanismi di governance specifici, nonché politiche e procedure di gestione dei rischi. L'obiettivo è garantire che i sistemi che trattano ICUE siano soggetti a standard di sicurezza più stringenti rispetto ai sistemi non

classificati, rendendoli più resilienti a minacce e incidenti informatici. Il Regolamento tratta inoltre del CERT-UE (Computer Emergency Response Team dell'UE), originariamente istituito come task force della Commissione con un mandato interistituzionale, successivamente confermato come entità permanente per migliorare la sicurezza informatica delle istituzioni, organi e agenzie dell'Unione. Infine, viene istituito anche l'Interinstitutional Cybersecurity Board, composto da rappresentanti di varie istituzioni dell'Unione Europea allo scopo di promuovere un elevato livello di cyber sicurezza tra i soggetti dell'Unione, offrendo direzione strategica e supervisionando l'attuazione del regolamento.

L'UE continua a evolvere il suo quadro normativo per affrontare le nuove sfide legate alla cybersecurity, cercando sempre di stare al passo dell'evoluzione del mondo digitale, il quale continua a crescere ogni giorno molto rapidamente, aprendo il campo a migliaia di scenari diversi che il diritto si trova a dover regolare.

2. Cybersecurity nel GDPR

Vogliamo studiare ora più approfonditamente la relazione esistente tra la materia di Cybersecurity e il Regolamento (UE) 2016/679, per l'appunto noto come GDPR, dedicato alla protezione dei dati personali, il quale però include anche disposizioni importanti per la cybersicurezza. Parliamo in particolare della problematica della Privacy e l'importanza della protezione dei dati personali all'interno di qualsiasi organizzazione e indipendentemente dal ruolo ricoperto, dei rischi connessi con il trattamento dei dati e di conseguenza, della necessità di maturare attitudini e adottare comportamenti che siano in linea con le esigenze di cybersecurity dell'intera organizzazione.

La Privacy va intesa come il diritto fondamentale ad avere una propria sfera di riservatezza che non può essere violata da terzi. L'affermazione dei processi di digitalizzazione e l'esplosione dei social hanno reso centrale il diritto dell'individuo al controllo e alla tutela dei propri dati personali, dove per *dato personale* si intende "qualsiasi informazione riguardante una persona fisica identificata o identificabile («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" (GDPR, Articolo 4, paragrafo 1).

Il GDPR (*General Data Protection Regulation*) è il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016. Tale regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati nell'Unione [14]. Ogni volta che si esegue un'operazione su un dato personale, e quindi tale dato viene trattato, si entra, cioè, nel campo di applicazione del GDPR. I suddetti dati, per la loro natura, potrebbero essere usati in modo illegittimo, creando grave danno sia alla singola persona che all'organizzazione, ed è qui che entra in gioco il legame con la cibersicurezza.

Il GDPR è emerso come una pietra miliare della protezione dei dati, dando una nuova forma al panorama globale di privacy dei dati e cybersecurity. Rinforzato nel 2018, il GDPR ha avuto un forte impatto su tutte le organizzazioni a livello globale, promuovendo una rivalutazione e un rinforzo delle pratiche di cybersecurity in modo da garantire conformità e adesione agli stringenti standard in materia di protezione dati [15].

Sono diversi gli articoli del Regolamento a cui possiamo fare riferimento quando parliamo di sicurezza informatica, a dimostrazione del fatto che non si può parlare di cybersecurity senza implicare alcuni dettami del GDPR. Infatti, il Regolamento impone agli enti e alle aziende che trattano

dati personali di adottare misure di sicurezza adeguate a proteggere tali dati da accessi non autorizzati, perdite, alterazioni e altri rischi. In particolare, tra i vari articoli evidenziamo:

Articolo 5 - Principi applicabili al trattamento dei dati personali

L'articolo 5 stabilisce i principi fondamentali per il trattamento dei dati personali, il quale deve essere lecito, corretto e trasparente nei confronti dell'interessato (articolo 5, paragrafo 1, lettera a). Alle organizzazioni è richiesto di comunicare chiaramente con gli individui titolari dei dati riguardo gli scopi del trattamento, assicurandosi che questi abbiamo compreso a pieno quale uso se ne farà. Possono inoltre raccogliere tali dati solo per finalità determinate, esplicite e legittime. Qualsiasi altro trattamento successivo deve necessariamente essere compatibile con lo scopo originario, scoraggiando l'uso indiscriminato dei dati raccolti (articolo 5, paragrafo 1, lett. b). Il GDPR incoraggia inoltre la minimizzazione del trattamento dei dati personali (articolo 5, paragrafo 1, lett. c), per cui le organizzazioni dovrebbero collezionare e trattare solamente i dati strettamente necessari per gli scopi previsti, riducendo il rischio di accessi non autorizzati e di *data breaches* (viene definita data breach 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. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali [16]). Rimanendo in tema di data breach, uno dei principi rilevanti in ambito cybersecurity è quello della "integrità e riservatezza" (art. 5, paragrafo 1, lett. f), secondo cui i dati devono essere trattati in modo da garantirne una protezione adeguata, compresa la prevenzione di accessi non autorizzati o illeciti. A chiudere il quadro dell'articolo 5, vi è il paragrafo 2 che esprime il principio di responsabilizzazione del titolare del trattamento dei dati, il quale si impegna a rispettare quanto sopra detto.

Articolo 25 - Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita

L'articolo 25 introduce i concetti di *privacy by design e privacy by default*. Secondo questo articolo, i titolari del trattamento devono implementare misure di protezione dei dati sin dalla fase di progettazione dei sistemi e dei processi e devono garantire che per impostazione predefinita siano trattati solo i dati necessari per ciascuna specifica finalità. La *privacy by design*, si fonda sui principi di prevenzione, sicurezza, visibilità e trasparenza, obbligando il titolare del trattamento ad una tutela effettiva da un punto sostanziale, non solo formale, cioè non è sufficiente che la progettazione del sistema sia conforme alla norma se poi l'utente non è tutelato. Quando facciamo riferimento alla *privacy by default* invece, ci riferiamo a come il titolare dei dati debba trattare solo i dati personali

nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. Nel paragrafo 1 possiamo leggere: "sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati", e ancora al paragrafo 2 si legge: "il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica". Viene quindi introdotto questo approccio concettuale innovativo che impone alle aziende l'obbligo di avviare un progetto prevedendo, fin da subito, gli strumenti e le corrette impostazioni a tutela dei dati personali.

Articolo 28 - Responsabili del trattamento

Nel momento in cui il Titolare del trattamento debba nominare un Responsabile del trattamento, ovviamente dovrà farlo in maniera accurata e scegliendo qualcuno che sia competente, che garantisca di rispettare tutto ciò che viene riportato nel Regolamento in merito al suo ruolo. Al paragrafo 1 si legge come, i responsabili del trattamento debbano necessariamente presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato. Inoltre, il titolare non ricorre ad altro responsabile senza autorizzazione e il trattamento da parte del responsabile è disciplinato da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri. Il GDPR impone che il titolare del trattamento scelga quindi responsabili del trattamento che possano garantire la conformità al regolamento. Questo include anche la capacità di attuare misure tecniche e organizzative appropriate per proteggere i dati personali, in linea con quanto previsto dall'articolo 32.

Articolo 32 - Sicurezza del trattamento

Questo articolo, collocato nella Sezione 2 "Sicurezza dei dati personali", può essere considerato come il fulcro del GDPR per quanto riguarda la cybersecurity. Questo, al paragrafo1, afferma che il titolare del trattamento e il responsabile del trattamento devono mettere in atto misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, come ad esempio:

- pseudonimizzazione e cifratura dei dati personali;

- capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Da tenere in considerazione anche il paragrafo 2 nel quale si parla di come sia importante considerare i rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati, quindi il rischio di data breach. Nell'ultimo paragrafo, infine, si riporta il concetto della responsabilità del titolare e responsabile del trattamento a far sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento. Il Garante può prescrivere misure correttive (art. 58, paragrafo 2, del Regolamento UE 2016/679) nel caso sia rilevata una violazione delle disposizioni del Regolamento stesso, anche per quanto riguarda l'adeguatezza delle misure di sicurezza tecniche e organizzative applicate ai dati oggetto di violazione. Sono previste sanzioni pecuniarie che possono arrivare fino a 10 milioni di euro o, nel caso di imprese, fino al 2% del fatturato totale annuo mondiale [16].

Articolo 33 - Notifica di una violazione dei dati personali all'autorità di controllo

Il GDPR impone un obbligo di notifica in caso di una violazione dei dati personali (data breach). Il titolare del trattamento deve notificare la violazione all'autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza. La notifica deve includere:

- una descrizione della natura della violazione dei dati personali (es. numero approssimativo di interessati);
- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- una descrizione delle probabili conseguenze della violazione;
- una descrizione delle misure adottate o da adottare per rimediare alla violazione e attenuarne gli effetti negativi;

L'importanza di questo articolo in materia di cybersicurezza è altrettanto rilevante, in quanto quando parliamo di sicurezza informatica, non facciamo riferimento solamente alle misure preventive, ma anche alla capacità di gestire situazioni di violazione dei sistemi e di saper reagire per cercare di

contenere i danni e minimizzarli il più possibile. Sono stati diversi i casi di attacchi informatici (ransomware), anche in Italia, dove la mancata reazione tempestiva da parte dei responsabili, ha provocato danni irreparabili, come vedremo nel caso reale di attacco ransomware alla regione Lazio.

Nominiamo infine anche i seguenti due articoli, i quali sono coerenti con gli argomenti trattati finora, sia per quanto riguarda interventi preventivi, sia il concetto di responsabilità del titolare del trattamento:

Articolo 34 - Comunicazione di una violazione dei dati personali all'interessato

In linea con l'articolo precedente, un occhio di riguardo va anche all'articolo 34, paragrafo 1 e 2, i quali affermano 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 comunica la violazione all'interessato senza ingiustificato ritardo" e come tale comunicazione all'interessato debba descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali.

Articolo 35 - Valutazione d'impatto sulla protezione dei dati

Sempre sulla misura della prevenzione, il GDPR ha introdotto la novità della DPIA (*Data Protection Impact Assesment*), ossia una valutazione dell'impatto sulla protezione dei dati. L'articolo 35 prevede che, quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, tale valutazione. Una DPIA consente quindi al Titolare di analizzare sistematicamente e approfonditamente come un nuovo trattamento, una nuova tecnologia, o un nuovo progetto impatteranno sui diritti e le libertà degli interessati e individuare, con un approccio *privacy by design & by default*, quali misure implementare per la tutela di quest'ultimi [17].

In sintesi, il GDPR impone un approccio proattivo alla **cybersecurity**, richiedendo alle aziende e agli enti di adottare misure preventive e protettive, oltre a fornire risposte tempestive in caso di violazioni. Questo rende la sicurezza informatica un elemento centrale della conformità al regolamento, con lo scopo di proteggere non solo i dati, ma anche i diritti e le libertà fondamentali delle persone.

3.Malware e Ransomware

Non si può parlare di cybersecurity senza prima andare quantomeno ad introdurre e descrivere brevemente due concetti chiave del mondo degli attacchi informatici: malware e ransomware.

3.1 Malware

Il Malware è un programma informatico che ha un intento malevolo. Si tratta spesso di un elemento tecnologico estremamente avanzato, la cui pericolosità è costituita dalla sua stessa natura. È, infatti, un software in grado di effettuare operazioni molto sofisticate, che possono provocare danni anche importanti. il termine "malware" nasce dalla combinazione dei termini "malicious" e "software", e quindi sta proprio ad indicare un programma software con intenti malevoli. Nella accezione più classica e popolare è ancora vivo il termine "virus", che richiama il concetto di infezione e quindi di diffusione incontrollata. Infatti, un programma di questo tipo non si limita a infettare il dispositivo che lo ha scaricato, ma tende poi a replicarsi all'interno delle reti di computer. Proprio come avviene per un virus reale. Si tratta quindi di un programma che può scatenare una vera e propria pandemia digitale.

All'interno della categoria dei malware si trovano tante tipologie di programmi malevoli, con comportamenti diversificati. I nomi con cui sono stati classificati sono spesso fantasiosi e richiamano proprio le funzioni principali di questi software. I principali sono:

- Worm, che richiamano la capacità dei vermi di autoreplicarsi
- Trojan, veri e propri "cavalli di troia", in grado di presentarsi come programmi utili e innocui e di camuffare la loro natura malevola

3.2 Ransomware

Nel 2013, venne diffuso quello che forse può essere definito il più pericoloso dei malware, ossia il famigerato Ransomware. Tecnicamente si tratta di un *criptolocker*, un programma che cripta tutti i dati del dispositivo infettato. Una volta che i dati vengono criptati, le organizzazioni criminali chiedono all'utente di pagare un riscatto (in inglese "ransom") in cambio della "chiave" necessaria a decriptare i file, liberandoli da questa forma di sequestro. Attualmente il ransomware è il malware più diffuso, e negli ultimi anni ha colpito milioni di organizzazioni in tutto il mondo. Oggi i ransomware sono ancora più sofisticati, perché sottopongono la vittima ad un doppio ricatto. I dati, prima di essere criptati, vengono copiati nei server dell'attaccante, e, qualora la vittima decidesse di non pagare il riscatto, magari perché pensa di poterli recuperare, allora interviene la seconda minaccia: quella di rendere pubblici i dati riservati.

4. Phishing, Smishing e Vishing

Phishing, Smishing (o phishing tramite SMS) e Vishing (o phishing tramite vocale), sono tre forme di criminalità informatica, che sfruttano principalmente l'elemento umano, che è forse l'anello più debole di tutta la catena di elementi coinvolti nello spazio cibernetico. Esaminiamo queste tre forme di violazione della cybersicurezza più nel dettaglio.

4.1 Social Engineering

Il Social Engineering è una tecnica di attacco cyber che fa leva sulla psicologia e che mira a manipolare le persone, sfruttandone la fiducia, la mancanza di conoscenza e la vulnerabilità, per indurle ad eseguire azioni che vanno a vantaggio della criminalità cyber, cercando di ottenere dati confidenziali, estorcere denaro o persino rubarne l'identità. Prima di realizzare questi tipi di attacchi basati sul Social Engineering, il criminale studia accuratamente la personalità e le relazioni della vittima. Quando il target è un'azienda, si compie un'accurata raccolta di informazioni non solo su di essa, ma anche sui dipendenti che lavorano al suo interno; dopo aver raccolto abbastanza informazioni, il criminale passa all'attacco. Tra i canali che il social engineer utilizza ritroviamo strumenti utilizzati ormai quotidianamente: e-mail, telefoni, app di messaggistica istantanea, siti web, social media [18].

È stato brevemente introdotto il social engineering perché, tra tutti i metodi che esistono per attuare questo tipo di truffa, phishing, smishing e vishing sono i più comuni.

4.2 Phishing

La e-mail è a tutti gli effetti il più importante strumento di comunicazione sia per le organizzazioni sia per i singoli individui. Passiamo la maggior parte del nostro tempo connessi a sistemi di posta elettronica e questo è il motivo per cui la mail è diventata in questi anni il mezzo più usato da criminali e truffatori per mettere in atto le loro azioni fraudolente.

Il *Phishing* è la più comune tecnica illecita utilizzata dai criminali Cyber per appropriarsi di informazioni riservate relative a una persona o a un'azienda - username e password, codici di accesso (come il PIN del cellulare), numeri di conto corrente, dati del bancomat e della carta di credito – con l'intento di compiere operazioni fraudolente (acquisizione fraudolenta di informazioni riservate, controllo e compromissione di un dispositivo -vedi Malware e Ransomware-, attraverso l'uso di programmi malevoli, progettati allo scopo; truffa con sottrazione di denaro). Il "ladro d'identità" si presenta, di solito, come un soggetto autorevole (banca, gestore di carte di credito, ente pubblico,

ecc.) che invita il destinatario a compiere un'azione, generando in esso la prospettiva di ottenere un vantaggio o semplicemente di evitare una situazione spiacevole. Questa "azione" si traduce nel fornire dati personali per risolvere determinati problemi tecnici con il conto bancario o carta di credito, per accettare cambiamenti contrattuali o offerte promozionali, per gestire la pratica per un rimborso fiscale o una cartella esattoriale, ecc... In genere i messaggi di phishing invitano a fornire direttamente i propri dati personali, oppure a cliccare su un link che rimanda ad una pagina web dove è presente un form da compilare. I dati così carpiti possono essere utilizzati per fare acquisti a spese della vittima, prelevare denaro dal suo conto o addirittura per compiere attività illecite utilizzando il suo nome o le sue credenziali.

La tecnica più comune di attacco è il Phishing Massivo (Spray Phishing), nella quale vengono inviate numerose e-mail a molti soggetti, così che il contenuto della e-mail diventi attivo nei confronti di qualcuno. Si parla invece di Phishing Diretto (Spear Phishing) quando l'attacco è sferrato nei confronti di un singolo individuo o di un gruppo ristretto di individui; questa è una tecnica più sofisticata che richiede una buona conoscenza delle potenziali vittime e quindi un'attività di acquisizione dell'informazione prima dell'attacco.

Dalla descrizione fatta, è chiaro quindi come la probabilità di successo del criminale Cyber, dipenda molto dal livello di consapevolezza che la potenziale vittima ha del rischio di subire un attacco di questo tipo e dalla sua capacità di riconoscerlo e prevenirlo.

Tra le principali accortezze da prendere in questi casi, prima fra tutte è sicuramente quella di non comunicare propri dati personali tramite e-mail, dato che banche, aziende, enti pubblici, ecc. non richiedono mai informazioni personali e sensibili via mail. Dato che i criminali Cyber fanno normalmente leva su un criterio di pressione e urgenza, insito nel contenuto della mail, per tentare di provocare azioni istintive, bisogna sempre mantenere un atteggiamento razionale e consapevole. Inoltre, è fondamentale non cliccare sui link allegati a tali e-mail, poiché potrebbero contenere virus o programmi trojan horse capaci di prendere il controllo di pc e smartphone; bisogna quindi provare sempre a decifrare il tipo di link allegato e cercare eventuali incongruenze rispetto al presupposto mittente. È necessario essere in grado di comprendere se il messaggio riporti richieste insolite (ad esempio: "sono stato aggredito e derubato" oppure " ho bisogno del tuo aiuto") e prestare attenzione ai loghi riportati nelle e-mail, i quali sono imitazioni di quelli ufficiali, che quindi possono trarci in inganno, ma che spesso contengono anche testi incoerenti ed errori grossolani, sia grammaticali che di formattazione che di traduzione da altre lingue. Si deve poi prestare attenzione al mittente (ad esempio, se l'indirizzo della mia banca è www.miabanca.com, è sicuramente anomalo ricevere una mail da un indirizzo come: @50percentosconto.com, ma anche da un @miabanca-supporto.com o da @supporto-miabanca.com. Diverso è invece ad esempio: @servizioclienti.miabanca.com) e in

generale diffidare da messaggi con tono intimidatorio, parte di una subdola strategia. Infine, è consigliabile intervenire preventivamente, dato che questi fenomeni sono sempre meno rari, installando ad esempio dei programmi antivirus oppure verificando che i sistemi di protezione che indirizzano queste e-mail direttamente nello spam siano attive, o ancora, non memorizzando password e dati personali nei browser per navigare online e impostando password alfanumeriche complesse e difficili da decifrare (molti telefoni e computer hanno già in sé la funzione di generazione di una password sicura). Per gli acquisti online invece è consigliato usare carte di credito prepagate o altri sistemi di pagamento che permettono di evitare la condivisione dei dati del conto bancario o della carta di credito, che possono inoltre essere protetti controllando spesso le movimentazioni e attivando sistemi di alert automatico che avvisano l'utente di ogni operazione effettuata [10].

4.3 Smishing

Lo *Smishing* è una forma di truffa che utilizza messaggi di testo e sistemi di messaggistica (compresi quelli delle piattaforme social media) per appropriarsi di dati personali a fini illeciti (ad esempio, per poi sottrarre denaro da conti e carte di credito, esattamente come nel phishing). I messaggi di smishing invitano i destinatari a compiere azioni (cliccare link, ecc.) o fornire informazioni con urgenza, per non rischiare danni (es: blocco di utenze, blocco della carta di credito o del conto) o sanzioni. I truffatori ("smisher") inviano messaggi per chiedere ad esempio alle vittime di:

- cliccare un link che conduce ad un form online in cui inserire dati personali, dati bancari o della carta di credito, ecc… Il link da cliccare può anche essere utilizzato per installare sullo smartphone della vittima programmi malevoli capaci di carpire dati personali conservati sul dispositivo o addirittura in grado di accedere alle app e ai programmi con cui si gestiscono Internet banking, carte di credito, ecc.;
- scaricare un allegato che può contenere programmi malevoli capaci di prendere il controllo dello smartphone o accedere ai dati in esso contenuti;
- rispondere ai messaggi ricevuti inviando dati personali (il codice fiscale, il PIN del Bancomat o quello utilizzato per l'Internet banking, il numero della carta, il codice di sicurezza della carta, i dati dell'OTP, cioè della password temporanea per eseguire operazioni sul conto bancario e sulla carta di credito, ecc.);
- chiamare un numero di telefono, dove poi un finto operatore o un sistema automatizzato chiedono di fornire informazioni di vario tipo, compresi dati bancari e/o della carta di credito.

Tra vari possibili messaggi da valutare con cautela abbiamo ad esempio: offerte di sconti straordinari su beni e servizi, anche proposte di ricariche telefoniche da effettuare subito a costi incredibilmente vantaggiosi, amministrazioni pubbliche che segnalano la necessità di fornire dati,

sanzioni da pagare (multe, cartelle esattoriali), anomalie da verificare, piattaforme che offrono servizi di social media o di messagistica che segnalano una violazione dell'account personale e chiedono di fornire dati e/o compiere determinate azioni (cliccare link, compilare form, chiamare numeri o inviare messaggi, ecc.).

Anche gli smisher, come i phisher, fanno leva sul timore legato ad un rischio incombente per convincere le vittime ad abbassare il livello di prudenza e a reagire d'impulso, si tratta di tecniche di attacco su base psicologica, nelle quali il criminale cerca di ingannare le sue vittime, avvantaggiandosi di informazioni che ha precedentemente acquisito su di loro.

Per difendersi da questo fenomeno si possono prendere anche qui delle misure preventive: non comunicare mai dati e informazioni personali o dati come codici di accesso, PIN, password, dati bancari e della carta di credito a sconosciuti; non conservare le credenziali (password, PIN, codici) di dati bancari o della carta di credito sullo smartphone; controllare spesso le movimentazioni ed eventualmente attivare sistemi di alert automatico che avvisano l'utente di ogni operazione effettuata; non cliccare sui link e non aprire eventuali allegati; prestare attenzione a quei messaggi che provengono da numerazioni anomale o particolari (es.: numeri con poche cifre). Può anche capitare che il truffatore abbia preso il controllo del dispositivo e/o numero di un nostro conoscente o di un soggetto con cui abbiamo rapporti o pratiche in corso ("*spoofing*"). In questo caso è buona pratica verificare se il testo presenta anomalie, errori linguistici, grammaticali, lessicali e fare attenzione che il tipo di richiesta sia coerente con il soggetto con cui stiamo chattando [10].

4.4 Vishing

Infine, il *Vishing* è una forma di truffa, sempre più diffusa, che utilizza il telefono come strumento per appropriarsi di dati personali - specie di natura bancaria o legati alle carte di credito - e sottrarre poi somme di denaro più o meno ingenti.

In particolare, di solito le vittime vengono contattate telefonicamente da finti operatori (di banche o di società che gestiscono bancomat o carte di credito) i quali, con la scusa di presunte "anomalie", chiedono alle persone, nel loro stesso interesse, di collaborare a mettere in atto necessarie (e false) "procedure di sicurezza". Nel caso più frequente, i truffatori ("visher") chiedono direttamente di fornire i riferimenti del conto corrente o della carta di credito (come il PIN del bancomat o quello utilizzato per l'Internet banking, il numero della carta, il codice di sicurezza sul retro della carta, i dati dell'OTP, cioè della password temporanea per eseguire operazioni sul conto bancario e sulla carta di credito, ecc.). In altri casi - durante o dopo la finta telefonata di allarme - viene inviato sul cellulare un messaggio con un codice di conferma e viene chiesto alla vittima di leggerlo ad alta voce

all’operatore. Tale codice serve in realtà ad autorizzare trasferimenti di denaro a vantaggio dei truffatori, entrati precedentemente in possesso dei dati bancari o della carta di credito (ad esempio, attraverso altre azioni di phishing o tramite altri cybercriminali). Può anche essere chiesto di scaricare e installare app e programmi, che ufficialmente dovrebbero servire per proteggere conti e carte di credito, ma che in realtà possono operare come trojan.

Per difendersi, anche in questo caso ci sono diverse accortezze da mettere in atto. Istituzioni e aziende chiamano di solito da numeri fissi e comunque con prefissi nazionali, chiamate provenienti, ad esempio, da numeri anonimi, da numeri di cellulare o da prefissi stranieri possono essere considerate anomale e dovrebbero renderci prudenti. Meglio diffidare delle chiamate con toni ultimativi o intimidatori, che ad esempio minacciano la chiusura del conto bancario, il blocco della carta di credito o eventuali sanzioni se non si compie subito una certa azione, possono essere subdole strategie per spingere il destinatario a fornire informazioni e dati personali senza rifletterci troppo; infatti, gli operatori telefonici hanno normalmente un atteggiamento cortese nei confronti dei clienti. Ovviamente è bene non comunicare mai i propri dati personali senza prima aver controllato che il numero che sta chiamando corrisponda a quello ufficiale. Inoltre, è meglio non provare mai a richiamare numeri sconosciuti, soprattutto nel caso di telefonate mute e con immediata caduta della linea. Infine, se si ha il dubbio di essere stati vittime di un attacco alla propria cybersicurezza, è consigliabile contattare immediatamente le autorità competenti.

5.Due casi di compromissione della cybersecurity

Dopo aver ampiamente discusso della cybersicurezza e delle normative a livello europeo che si occupano di questo argomento, vediamo due casi reali di compromissione della cybersecurity, per comprendere anche a quali gravi e soprattutto reali conseguenze possono portare fenomeni di questo tipo.

5.1 Primo caso: attacco ransomware alla regione Lazio

La notte tra il 31 luglio e il 1° agosto 2021, un attacco informatico da manuale scuoteva le fondamenta del sistema sanitario regionale del Lazio, causando un grave data breach che ha compromesso la sicurezza dei dati personali di milioni di assistiti. L'attacco ha avuto origine dall'introduzione di un ransomware tramite un portatile di un dipendente in smart-working, bloccando l'accesso a molti servizi sanitari per un tempo che è andato da alcune ore ad alcuni mesi, impedendo pagamenti, la gestione delle prenotazioni, il ritiro dei referti e la gestione e registrazione delle vaccinazioni contro il Covid-19. Asl, aziende ospedaliere, case di cura non hanno potuto utilizzare alcuni sistemi informativi regionali, attraverso i quali sono trattati i dati sulla salute di milioni di assistiti. L'attacco alla Regione Lazio ha suscitato un grande clamore mediatico, conquistandosi le prime pagine di molti giornali e venendo etichettato come "attacco senza precedenti"; tuttavia, lungi dall'essere stato un attacco nuovo. Si è trattato di un ransomware già noto nell'ambito della cybersecurity, entrato nel sistema attraverso una campagna di phishing ben riuscita e a causa delle scarse protezioni del sistema. I ransomware, come quello utilizzato nell'attacco, sono notoriamente insidiosi. Sono programmi dannosi che, una volta entrati nel sistema, cifrano i dati, rendendoli inutilizzabili. Gli hacker dietro tali attacchi poi richiedono tipicamente un pagamento, solitamente in criptovalute, per la chiave di decrittazione. La pericolosità del ransomware risiede nella sua capacità di colpire rapidamente e inaspettatamente, sfruttando spesso punti deboli come errori umani o lacune nella sicurezza del software.

Per quanto riguarda le sanzioni imposte dal Garante, queste sono state calcolate in base alla natura, alla gravità delle violazioni e al grado di responsabilità. LAZIOcrea, la società responsabile dei sistemi informativi regionali della Regione Lazio stessa, è stata gravata dalla sanzione maggiore per non aver adeguatamente aggiornato i propri sistemi, i quali risultavano obsoleti, e per la mancata implementazione di misure di sicurezza adeguate a prevenire tempestivamente le violazioni dei dati personali. In particolare, LAZIOcrea è stata accusata di non aver agito prontamente per gestire l'attacco informatico e le sue conseguenze, decidendo di spegnere tutti i sistemi senza essere in grado di determinare quelli effettivamente compromessi o di prevenire ulteriori propagazioni del malware.

Questa mancanza di azione ha aggravato notevolmente l'impatto dell'attacco, causando disagi significativi per le strutture sanitarie regionali e i loro assistiti. Non vi è stata una corretta predisposizione delle azioni necessarie per una gestione corretta del data breach e delle sue conseguenze, in particolare nei confronti dei soggetti per i quali svolge compiti da responsabile del trattamento, rappresentando una grave violazione delle disposizioni del GDPR. La Regione Lazio, essendo il titolare del trattamento dei dati, è stata ritenuta responsabile per non aver esercitato un'adeguata vigilanza sul proprio responsabile del trattamento, trascurando di garantire un livello di sicurezza adeguato ai rischi e di proteggere i dati fin dalla progettazione, come richiesto dalla normativa sulla privacy. La sanzione minore alla Asl Roma 3, invece, è stata attribuita per la mancata notifica tempestiva del data breach. Per tutti questi motivi, la sanzione inflitta dal Garante Privacy è stata di €271.000 per LAZIOcrea, 120.000€ per la Regione Lazio e €10.000 per l'Asl Roma 3.

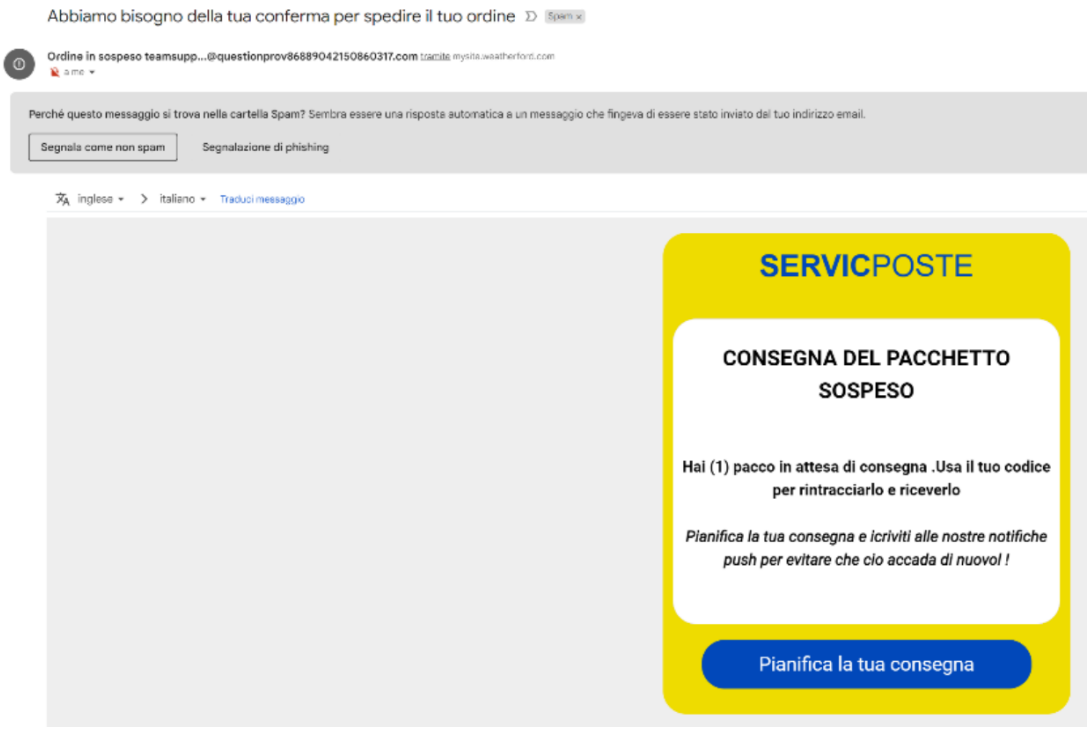
Questo attacco ha messo a nudo la vulnerabilità di enti che gestiscono dati di particolare sensibilità e rilevanza. La decisione di spegnere circa 180 server per prevenire ulteriori danni ha interrotto servizi essenziali, sottolineando l'importanza di avere piani di risposta agli incidenti e sistemi di rilevamento e mitigazione degli attacchi. L'incidente rivela che la gestione delle crisi informatiche deve essere agile, proattiva e supportata da protocolli solidi che non compromettano la continuità operativa delle strutture critiche. È imperativo che le istituzioni sanitarie rivedano i loro approcci alla sicurezza dei dati, integrando la cybersecurity come parte integrante del loro funzionamento quotidiano. La formazione del personale, gli aggiornamenti regolari dei sistemi e l'adozione di strumenti di sicurezza avanzati dovrebbero diventare prassi comune, non eccezioni. Il Garante, con queste sanzioni, non solo punisce, ma lancia un chiaro messaggio al settore: la sicurezza informatica dei dati personali e la salute dei cittadini sono indissolubilmente collegate. Le istituzioni devono elevare il proprio livello di preparazione, trasformando la sicurezza dei dati in un imperativo strategico non più rimandabile. [19] [16] [2]

5.2 Secondo caso: phishing "Poste Italiane"

Tra le migliaia di casistiche di fenomeni di phishing, riportiamo uno, a cui ho personalmente assistito. Si tratta di una e-mail, apparentemente inviata da Poste Italiane, che comunica la sospensione della consegna di un certo pacco e richiede di "pianificare" la propria consegna. Ci sono numerosi elementi che segnalano la vera natura di questa e-mail e con un po' di formazione, tutti noi possiamo essere in grado di riconoscerli. Innanzi tutto, l'indirizzo del mittente è particolarmente lungo e dovrebbe farci insospettire, dato che contiene una serie di caratteri casuali e non appare come una mail "ufficiale",

solitamente più breve, di chiara lettura e non confusionaria come invece in questo caso: *teamsupportXXXX4839363721847985589826519645025842538239144589942363351312635312001@questionprov86889042150860317.com*, inoltre contiene il nome del destinatario (*XXXX*). Altro aspetto rilevante è il titolo del messaggio: "Abbiamo bisogno della tua conferma per spedire il tuo ordine", decisamente vago e mancante di quel minimo grado di ufficialità che ci si aspetta da una e-mail spedita da una società come quella di Poste Italiane. Terzo aspetto rilevante è che il messaggio è stato inviato tramite un sito (*mysite.weatherford.com*) mentre l'e-mail sembra provenire da Poste Italiane. Quarto campanello d'allarme, il pulsante che siamo invitati a cliccare, è collegato ad un link sospetto:
https://storage.googleapis.com/i8x7a6l1z8v0m7z0/l2f9p1o5h1a9m9x7.html#h0oh0o.aspx?d4HY4gcctWZLcyhTCcdcYWcJcGdL3fczFcbbb4W, anche questo appare come confusionario e non sembra corrispondere al sito originario di Poste Italiane. Inoltre, il link per annullare l'iscrizione alle notifiche è lo stesso del pulsante e degli altri link contenuti nel messaggio, chiaro segno di come il criminale cyber vuole indurci a tutti i costi a cliccare su tale link, sperando in un nostro momento di distrazione. Infine, il segnale più evidente è quello relativo all'aspetto grafico; i colori e il font ricordano quelli del sito di Poste Italiane, tuttavia appare la scritta "SERVICPOSTE", e all'interno del riquadro il messaggio contiene degli errori grammaticali come ad esempio "icriviti", anziché "iscriviti", spazi prima dei segni di punteggiatura, punti e maiuscole mancanti, "cio" invece di "ciò", "nuovol !" anziché "nuovo!". [20]

Di seguito uno screen della e-mail:



Bibliografia

[1] E. Treccani. [Online].

[2] «Cybersecurity360,» [Online].

[3] «Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico,» 2013.

[4] B. Saetta, «Protezione dati personali,» 22 luglio 2018. [Online]. Available: https://protezionedatipersonali.it/direttive-europee.

[5] «EUR-Lex, access to European Union law,» [Online]. Available: https://eur-lex.europa.eu/.

[6] C. europea, Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica, 2001.

[7] R. A. J. e. C. Team, «LA CYBERSECURITY IN EUROPA. FONTI, LEGISLAZIONE E VISIONE».

[8] «Comunicazione congiunta al Parlamento Europeo, al Consiglio, al Comitato Economio e Sociale Europeo e al Comitato delle Regioni: Strategia dell'Unione europea per la cibersicurezza, un ciberspazio aperto e sicuro,» 7 febbraio 2013. [Online].

[9] «Gazzetta ufficiale dell'Unione Europea,» 19 luglio 2016. [Online].

[10] «Garante per la protezione dei dati personali,» [Online]. Available: https://www.garanteprivacy.it.

[11] «Network Digital 360,» [Online]. Available: https://www.agendadigitale.eu/sicurezza/cybersecurity-act-ecco-cosa-ci-aspetta-dopo-la-direttiva-nis/.

[12] «REGOLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 17 aprile 2019».

[13] «Agenda Digitale,» [Online]. Available: https://www.agendadigitale.eu/sicurezza/obblighi-di-cyber-sicurezza-come-adeguarsi-alla-direttiva-nis2/.

[14] «Regolamento generale sulla protezione dei dati; Regolamento (UE) 2016/679 del Parlamento europeo,» 27 Aprile 2016. [Online].

[15] A. Olukunle Oladipupo, A. Akoh, O. Femi, A. Temitayo Oluwaseun, S. A. Benjamin e F. Oluwatoyin Ajoke, «GDPR's impact on cybersecurity: A review focusing on USA and European practices,» *International Journal of Science and Research Archive,* 2024.

[16] «Garante per la Protezione dei Dati Personali,» [Online]. Available: https://www.garanteprivacy.it/data-breach.

[17] «ICT Security Magazine,» [Online]. Available: https://www.ictsecuritymagazine.com/articoli/quando-procedere-ad-una-dpia-ex-art-35-gdpr-la-prevalutazione-dimpatto/.

[18] «Osservatori.net,» 3 giugno 2024. [Online]. Available: https://blog.osservatori.net/.

[19] «Diritto.it,» [Online]. Available: https://www.diritto.it/garante-privacy-sanzioni-lazio-attacco-ransomware/.

[20] «pandasecurity,» [Online]. Available: https://www.pandasecurity.com/it/mediacenter/phishing-vediamo-caso-reale/.