Attacco hacker della Corea del Nord a Pfizer, l'healthcare in crisi di sicurezza?

Alcuni hacker nordcoreani hanno cercato di violare il sistema informatico del colosso farmaceutico **Pfizer** per sottrarre informazioni sul vaccino contro il coronavirus.

A riferire l'accaduto sono i media sudcoreani, citando i servizi d'Intelligence. **Ha Tae-keung**, deputato di Seul, ha detto che il Parlamento è stato informato *che "la Corea del Nord ha cercato di ottenere tecnologie comprendenti il vaccino e le cure attraverso un cyberattacco a Pfizer".*

Secondo Bloomberg non è chiaro se il sistema informatico della Pfizer sia stato violato o meno anche perché né l'azienda farmaceutica statunitense né lo stesso deputato sudcoreano hanno voluto rilasciare ulteriori dettagli al riguardo.

L'esercito di hacker di di Kim Jong Un

La Corea del Nord ha investito molto negli ultimi anni in capacità d'attacco cibernetiche, consentendo al Paese di guadagnare denaro, attaccare i nemici e perseguire le priorità del regime di **Kim Jong Un.**

Recentemente le Nazioni Unite hanno accusato gli hacker di **Pyongyang** di aver rubato 316,4 milioni di dollari tra il 2019 e il novembre 2020, denaro utilizzato per finanziare i

programmi nucleari e missilistici balistici del Paese.

Al momento, secondo fonti di intelligence, la Corea del Nord sta facendo tutto il possibile per ottenere un vaccino per l'intera nazione, anche se ciò significa ricorrere al furto. Per questo motivo il regime di Kim ha dirottato le proprie capacità cibernetiche la ricerca di un vaccino nonostante il Paese, grazie al programma di condivisione del vaccino **Covax**, riceverà quasi due milioni di dosi del vaccino **AstraZeneca-Oxford** entro la prima metà del 2021.

Healthcare: un settore in crisi di sicurezza

"Gli attacchi nel settore sanitario sono sempre più invasivi, per varie motivazioni legate al furto di know how, brevetti, cartelle cliniche per agevolare le analisi e ricerche in alcuni settori o per mero sabotaggio", spiega **Gerardo Costabile**, CEO di **DeepCyber** (Gruppo Maggioli).

"Il coronavirus ha certamente acuito, in tutti i settori, questo trend e i dati sulle casistiche, sulle cure e sui vaccini sono un target di attacco politicamente e strategicamente molto importante. Negli ultimi mesi, continua Costabile*, un attacco simile, sempre sul vaccino* ***Pfizer****, aveva colpito anche l'Agenzia* ***EMA*** *e i dati erano stati pubblicati sul darkweb. Anche se non è ufficialmente stata definita una connessione tra quell'attacco e questo odierno, vi è il ragionevole dubbio che esista un enorme interesse strategico ed economico, in questo tipo di azioni. Come avviene in altri settori, esistono vere e proprie "tariffe" per la vendita di questi dati, si parla di milioni di euro per singolo attacco da parte dei bad actor cosiddetti "state sponsored".*

Secondo il CEO di **DeepCyber** *"per settore sanitario non si intende solo la società farmaceutica, ovviamente, perché alcune informazioni sono disponibili in varie aree della*

filiera della sanità: si pensi alla catena del freddo del vaccino, oggetto di attacco qualche settimana fa. In tal caso l'informazione era disponibile in varie organizzazioni di settore. Allo stesso tempo, l'healthcare è settore che vede meno investimenti nella cyber security e questo si può verificare velocemente. Basti pensare quanti pochi manager della sicurezza esistano negli organigramma e nelle organizzazioni e la sicurezza viene trattata come una normale commodity.

"Secondo il DBIR 2020, l'healthcare ha registrato lo scorso anno quasi 800 incidenti e in oltre 500 casi con data breach (contro i 300 dello scorso anno), quasi per metà dall'esterno e metà dall'interno. Nell'88% dei casi, conclude Costabile, *gli attacchi avevano motivazioni finanziarie e nel 67% erano presente dati medici".*

https://www.key4biz.it/attacco-hacker-della-corea-del-nord-a-pfizer-lhealthcare-in-crisi-di-sicurezza/345673/

Sanità, +177% di cyber attacchi agli ospedali di tutto il mondo. L'IoT aumenta l'esposizione ai data breach

Nella seconda metà dell'anno passato si è assistito ad un aumento considerevole degli **attacchi informatici alle strutture ospedaliere e sanitarie** di tutto il mondo.

Crescono i cyber attacchi ad ospedali e strutture sanitarie

Secondo il nuovo **Report** CI Security, **la violazione/sottrazione di dati sensibili è cresciuta del +36% nel secondo semestre del 2020**.

I cyber attacchi con data breach hanno riguardato 21,3 milioni di record di dati sanitari, con un impressionante **aumento del +177%** rispetto allo stesso periodo dell'anno prima (quando la violazione riguardò 7,7 milioni di record di dati).

Un dato triplicato, frutto di una strategia criminale che ha preso di mira sistemi informatici ospedalieri, sanitari e a disposizione dei medici sul territorio, fino ai laboratori di farmaceutica e di ricerca e innovazione, o alle strutture di riabilitazione.

Probabilmente, il risultato diretto di un processo di digitalizzazione e di impiego di tecnologie avanzate di rete, che se da un lato hanno facilitato il lavoro del personale medico-sanitario nei mesi più duri della pandemia di Covid-19, dall'altro hanno esposto l'intera rete sanitaria ed ospedaliera ad attacchi informatici sempre più distruttivi e mirati.

Data breach più facili con la diffusione dell'IoT

"*Si tratta di scenari critici frutto diretto dell'integrazione dei servizi tradizionali offline con quelli che ora sono online, accessibili via internet. Oggi possiamo vedere la nostra cartella clinica da uno smartphone, perché i sistemi che prima giravano su rete locale, o Local Area Network, di fatto dei circuiti chiusi, ora sono disponibili in rete. Una situazione che aumenta notevolmente la superficie di attacco*

per i cyber criminali. Se prima potevano prendere di mira solo il web server, con i siti web, ora possono scendere più in profondità, fino ai sottosistemi che consentono di raggiungere i record di dati sanitari dei pazienti, tra cui quelli contenuti nelle cartelle cliniche", ha spiegato a Key4biz, **Antonio Mauro**, PhD Department of Engineering, University of Northwest USA.

"*Molta della strumentazione un tempo analogica, ora è digitale. È l'evoluzione dell'internet delle cose. Se un elettrocardiogramma fino a qualche anno fa si traduceva in dati cartacei, oggi è tradotto in un pacchetto di dati informatici immessi nella rete interna dell'organizzazione sanitaria, che può essere un ospedale, a sua volta però connessa a internet.*
L'Internet delle cose ha ampliato il panorama dei dispositivi elettronici che in strutture ospedaliere sono connessi a internet – ha affermato l'esperto – *aumentando notevolmente così anche l'esposizione agli attacchi informatici*".

Obiettivo dei cyber criminali sono sempre i dati sensibili

"*I dati sensibili sono l'obiettivo primario dei cyber criminali, che poi li venderanno per fare profitti. Questi dati però sono anche utili per generare documenti falsi, ma realizzati a partire da informazioni reali. Parliamo di documenti di identità e carte di credito, ma non solo, realizzati a partire dai dati rubati in rete*", ha proseguito Mauro.

"*Altri obiettivi perseguiti dai cybercriminali sono invece finalizzati al blocco delle attività critiche di una struttura sanitaria. Con l'utilizzo di malware e ransomware, si possono mandare in tilt sistemi di massima rilevanza per il funzionamento di un ospedale* – ha precisato il Professore – *compresi gli stessi strumenti utilizzati per diagnosi e*

interventi chirurgici, fino alla richiesta di un riscatto finale.
Si tratta di criticità informatiche che sono emerse non solo in ambito sanitario, ma in qualsiasi altro settore in cui sia avvenuta la convergenza di innovazione tecnologica, digitalizzazione e impiego dell'internet delle cose".

Crescono gli attacchi ransomware

Il rapporto, infatti, rileva che **la frequenza degli attacchi ransomware giornalieri è aumentata del +50%** nel terzo trimestre del 2020, rispetto alla prima metà dell'anno.

I cyber criminali hanno anche preso di mira società terze che lavorano per il settore sanitario e della salute, fornitrici di diversi servizi, principalmente di tipo amministrativo, tanto che è loro il 75% dei record di dati violati nella seconda metà del 2020.

Il 97% di tutti gli attacchi è stato finalizzato al furto dei dati.

Fondamentale, secondo i ricercatori, è sviluppare sistemi di identificazione digitale più specifici, formare il personale al tema della cybersecurity, potenziare la difesa dei sistemi di archiviazione dati, rivedere il sistema di responsabilità attinente alla sicurezza informatica di una struttura.

> *Sanità, +177% di cyber attacchi agli ospedali di tutto il mondo. L'IoT aumenta l'esposizione ai data breach*

IA e guida autonoma, l’Ue: “Troppi rischi informatici, serve più sicurezza”. Il report

I sistemi di IA dei veicoli a guida autonoma, come tutti i sistemi IT, sono vulnerabili ad attacchi informatici che possono comprometterne il funzionamento.

Lo ha dichiarato l’Agenzia dell’Unione Europea per la cybersicurezza, **Enisa**, nel rapporto sui rischi legati all’utilizzo dell’Intelligenza Artificiale nei veicoli a guida autonoma.

IA e guida autonoma: troppi rischi di sicurezza per l’Ue

Al di là dei rischi causati da malfunzionamenti, questi sistemi sono anche vulnerabili ad attacchi intenzionali con lo specifico obiettivo di sabotarne le funzioni. Stando al rapporto, inoltre, l’aggiunta di vernice sul manto stradale o l’applicazione di adesivi su di un cartello per prevenirne il riconoscimento possono spingere il sistema a classificare informazioni errate e di conseguenza indurre il veicolo a comportarsi in maniera pericolosa.

Tra le raccomandazioni formulate nel rapporto, la manutenzione regolare dei componenti con controlli ciclici di sicurezza, la ricerca continua nelle cause accidentali e volontarie dei rischi e la creazione di un set di norme apposite per la gestione di tutta filiera produttiva del settore.

Infine la richiesta al settore dell'automotive di rinforzare la preparazione nella capacità di gestione ed intervento in eventuali emergenze nel caso di violazione della cybersecurity dei loro prodotti.

"Quando un mezzo insicuro a guida autonoma attraversa i confini di uno stato membro dell'Ue – ha osservato **Juhan Lepassaar** direttore dell'Enisa – *porta con sé tutti i suoi rischi.* L*a sicurezza non dovrebbe essere un pensiero collaterale, ma dovrebbe essere il prerequisito per un utilizzo credibile ed affidabile di questi prodotti nelle strade europee".*

Per approfondire

https://www.key4biz.it/ia-e-guida-autonoma-lue-troppi-rischi-informatici-serve-piu-sicurezza-il-report/344779/

LodaRAT, il trojan bancario affina lo spying e diventa multipiattaforma

Una campagna malspam in corso distribuirebbe una variante del malware **LodaRAT** capace di infettare non solo sistemi operativi Windows ma anche dispositivi Android. Lo rendono noto i ricercatori di Cisco Talos sul loro blog.

Da quanto si apprende gli attori della minaccia, nascosti dietro LodaRAT, probabilmente afferenti (come sviluppatori e/o

operatori) al gruppo criminale Kasablanca starebbero conducendo campagne mirate ibride e multipiattaforma mettendo in repentaglio, con una nuova iterazione, la sicurezza e la privacy di target specifici in Bangladesh. Insieme ad una variante Android nella stessa campagna sarebbe stata individuata anche una versione aggiornata di LodaRAT per Windows.

La campagna in Bangladesh

LodaRAT, scoperto per la prima volta nel 2016, nasce come trojan di accesso remoto (RAT) con varie funzionalità per captare registrazioni audio/video e rubare informazioni bancarie.

Però, nella campagna in Bangladesh (iniziata a ottobre 2020 e ancora in atto), i ricercatori hanno costatato un particolare interesse degli attaccanti alla raccolta d'informazioni e ad attività di spionaggio piuttosto che all'ottenimento di un guadagno diretto finanziario, mettendo sotto tiro varie organizzazioni, comprese banche e fornitori di software VoIP carrier-grade.

Secondo gli esperti, per la distribuzione dei dropper del malware multipiattaforma sarebbe stato impiegato l'invio massivo di e-mail con collegamenti ad app o documenti/software dannosi e l'utilizzo di tecniche "typosquatting" con riferimenti a nomi di domini e di file collegati a prodotti/servizi delle stesse vittime.

In particolare per scaricare il payload LodaRAT su sistemi Windows, gli attaccanti hanno utilizzato documenti malevoli con estensione .RTF, sfruttando una vulnerabilità classificata come CVE-2017-11882 e che riguarda l'esecuzione di codice remoto per mezzo di documenti Microsoft Office.

La variante LodaRAT4Android

La versione Android del malware LodaRAT, battezzata con il nome di “Loda4Android”, presenta tutti i comandi tipici di un trojan bancario allestito ad hoc per i sistemi del robottino verde. Il malware che possiede anche un kit integrato di phishing per Facebook può registrare la posizione degli utenti, l’audio dell’ambiente, scattare foto e screenshot. Può, inoltre, inviare e leggere SMS, effettuare chiamate a numeri specifici, leggendo il registro delle chiamate da memoria ed esfiltrare contatti. Pur tuttavia, specificano i ricercatori, questa variante non è in grado di intercettare messaggi SMS e telefonate. Infine, l’impiego di un protocollo comunicazione di comando e controllo C2 (con lo stesso modello di progettazione previsto nella versione Windows) e la capacità di eseguire una vasta gamma di ulteriori comandi e script rendono Loda4Android abbastanza flessibile.

La nuova versione per Windows

La nuova versione di LodaRAT destinata ai sistemi Windows è la versione 1.1.8, informazione di cui i ricercatori hanno trovato evidenze revisionando il codice malware di un campione. Sebbene questa variante sia per lo più uguale alle versioni precedenti, sono stati aggiunti nuovi comandi che ne estendono alcune capacità. La struttura presenta:

- Un’utilità di rete denominata “nx.exe” che consente l’accesso remoto al computer di destinazione tramite protocollo RDP (Remote Desktop Protocol) e porta standard 3389. Tale accesso è reso possibile cambiando, preventivamente, alcune impostazioni di sicurezza di Windows su alcune voci di registro e sul firewall predefinito;
- un comando denominato SOUND che, sfruttando una libreria audio BASS “bacb.dll”, consente di catturare l’audio via microfono, senza utilizzare il registratore di suoni

integrato di Windows, meno performante in termini di tempi di registrazione massimi consentiti.

In conclusione

Senza dubbio, la campagna rilevata riflette un cambiamento generale nelle strategie di attacco da parte degli sviluppatori e delle relative affiliazioni di LodaRAT.

È ragionevole pensare che, molto probabilmente, tali attori di minaccia, implementando con funzionalità aggiuntive un malware multipiattaforma di questo tipo e puntando su attività di spying piuttosto che su obiettivi prettamente finanziari, abbiano in mente di espandere, in futuro, il proprio bacino d'azione aumentando con esso anche i relativi livelli di rischio per aziende e privati.

https://www.key4biz.it/lodarat-il-trojan-bancario-affina-lo-spying-e-diventa-multipiattaforma/344584/

EDPB, pubblicate le linee guida su 18 casi d'uso riguardanti la notifica di violazione dei dati

L'*European Data Protection Board* ("EDPB") ha pubblicato, in consultazione, le linee guida 01/2021 sugli esempi relativi alla notifica di violazione dei dati ("data breach"). I

contributi a tali linee guida dovranno pervenire entro il 2 marzo e nel frattempo possiamo analizzare nel dettaglio quanto sviluppato, al riguardo, dall'EDPB.

Si tratta di un documento molto interessante sia per gli esperti *privacy* ma anche per gli operatori della *Cybersecurity*.

Con tali linee guida, l'EDPB ha inteso integrare le linee guida WP250 emanate dal WPG 29 e attualizzarle ai casi pratici oltre che all'intervenuta applicazione quotidiana del GDPR, con lo scopo di fornire utili elementi per la gestione delle violazioni dei dati e quali fattori considerare durante la valutazione del rischio.

Il primo elemento da valutare nell'ambito di qualsiasi di violazione è la possibilità di riconoscerla, per come definito all'art. 4, paragrafo 12 del GDPR.

Nel parere 03/2014 (G29 WP213, del 25 marzo 2014) sulla notifica di violazione e nelle citate linee guida WP 250, il WP29 ha chiarito che le violazioni possono essere classificate in base ai tre principi sulla sicurezza delle informazioni:

· "**Violazione della riservatezza**" – in caso di divulgazione non autorizzata o accidentale o accesso ai dati personali.

· "**Violazione dell'integrità**" – in caso di alterazione non autorizzata o accidentale dei dati personali.

· "**Violazione della disponibilità**" – in caso di perdita accidentale o non autorizzata dell'accesso o la distruzione dei dati personali (pag. 7 linee guida WP250).

Ciascuna violazione, potenzialmente, può avere una serie di effetti negativi significativi, specialmente sugli individui, che possono provocare danni fisici, materiali o immateriali; ciò può significare la perdita di controllo sui loro dati personali, la limitazione dei loro diritti, la

discriminazione, il furto di identità, la frode, perdite finanziarie, l'inibizione non autorizzate della pseudonimizzazione, il danno alla reputazione e la perdita di riservatezza dei dati personali (anche protetti dal segreto professionale) e può anche includere qualsiasi altro significativo svantaggio economico o sociale.

Uno degli obblighi più importanti del titolare del trattamento è valutare questi rischi per i diritti e le libertà degli interessati e attuare adeguate misure tecniche e organizzative per affrontarle.

Il GDPR, ai sensi dell'art. 33, richiede al titolare del trattamento di:

· documentare eventuali violazioni dei dati personali, i suoi effetti e le azioni correttive intraprese;

· notificare la violazione dei dati personali all'autorità di controllo, a meno che sia improbabile che comporti un rischio per i diritti e le libertà delle persone fisiche;

· comunicare la violazione dei dati personali all'interessato quando ciò possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche.

Le violazioni dei dati comportano problemi di vari natura, ma sono anche sintomi di una vulnerabilità, forse per un sistema di sicurezza dei dati obsoleto; indicano, altresì, debolezze del sistema che devono essere risolte.

In generale, è sempre meglio prevenire le violazioni dei dati preparandosi in anticipo, poiché le loro conseguenze sono irreversibili.

Anzitutto, come accennato, andrebbe identificata la causa del problema di vulnerabilità: infatti la notifica di violazione potrebbe essere anticipata all'identificazione del pericolo di vulnerabilità e non dovrebbe essere atteso il relativo

incidente per promuovere quelle azioni correttive; in tal modo si potrebbero ridurre i ritardi connessi all'impatto provocato dalla violazione.

Perciò, la violazione dovrebbe essere notificata quando si ritiene che questa possa comportare un rischio per i diritti e le libertà dell'interessato e prendere coscienza del rischio della violazione, non attendendo un esame forense dettagliato o l'attuazione delle misure di mitigazione.

Ciascun titolare del trattamento dovrebbe disporre di piani e procedure per la gestione di eventuali violazioni dei dati, con chiare linee guida da fornire ai propri dipendenti per garantire il processo di recupero o mantenere la continuità operativa di sistema.

Altro elemento fondamentale sono la formazione (costante e aggiornata) e la sensibilizzazione del personale su tali temi in modo da rendere cosciente e preparato ciascun individuo inserito nella catena di gestione delle violazioni dei dati.

Proprio questo approccio non è altro che la declinazione pratica del principio di "accountability" by design fintanto che venga adottato un "Manuale sul trattamento della violazione dei dati personali" che miri ad identificare i rischi, fornire in anticipo informazioni rapide per consentire di mitigare i rischi e adempiere agli obblighi senza ritardo.

A questo punto l'EDPB condivide quegli esempi di violazione che sono frutto della casistica e letteratura emersa negli ultimi tempi. Si tratta, perciò, di spunti di riflessione che dovrebbero permettere, in via analogica, di comprendere come reagire ad una violazione dei dati secondo le macro categorie di minaccia.

Ransomware

Un attacco *ransomware*, generalmente, prevede che un codice dannoso crittografa i dati personali e successivamente

l’aggressore chieda al titolare un riscatto in cambio del codice di decrittazione.

Questo tipo di attacco di solito può essere classificato come **violazione della disponibilità, ma spesso potrebbe verificarsi anche una violazione della riservatezza**.

CASO N. 01: *Ransomware* con backup adeguato e senza esfiltrazione

I sistemi informatici di una piccola azienda manifatturiera sono stati esposti a un attacco *ransomware* e i dati memorizzati in quei sistemi sono stati crittografati.

Il titolare del trattamento ha utilizzato la crittografia “a riposo”, quindi tutti i dati a cui il *ransomware* accedeva venivano archiviati in forma crittografata utilizzando un algoritmo di crittografia avanzato.

La chiave di decriptazione non è stata compromessa durante l’attacco, ovvero l’aggressore non poteva né accedervi né utilizzarlo indirettamente.

Di conseguenza, l’aggressore aveva accesso solo a dati personali crittografati.

In particolare, né il sistema di posta elettronica dell’azienda, né alcun sistema client utilizzato per l’accesso è stato colpito.

L’azienda ha usufruito della consulenza di una società esterna di sicurezza informatica per indagare sulle dinamiche dell’incidente.

Sono altresì integri e disponibili i registri che tracciano tutti i flussi di dati in uscita dall’azienda (inclusa la posta in uscita).

Perciò, dopo aver analizzato dai sistemi di rilevamento i log

e i dati raccolti, l'indagine interna – supportata dalla società esterna di sicurezza informatica – ha stabilito, *con certezza*, che l'autore del reato ha solo crittografato i dati, senza esfiltrazione.

I registri non hanno mostrato alcun flusso di dati in uscita nel periodo di tempo dell'attacco.

I dati personali interessati dalla violazione riguardano clienti e dipendenti dell'azienda, poche decine di individui in tutto.

Era altresì disponibile immediatamente un *backup* e i dati sono stati ripristinati poche ore dopo l'attacco.

La violazione non ha comportato alcuna conseguenza sull'operatività quotidiana del titolare del trattamento né sono stati registrati ritardi nei pagamenti dei dipendenti o nella gestione delle richieste dei clienti.

In questo caso, la violazione ha comportato l'alterazione illecita dei dati personali e l'accesso non autorizzato ai dati medesimi.

Misure preventive e valutazione del rischio

Come per tutti i rischi posti da agenti esterni, la probabilità che un attacco *ransomware* abbia successo può essere drasticamente ridotto rafforzando la sicurezza dell'ambiente di controllo dei dati.

La maggior parte di queste violazioni possono essere prevenute garantendo adeguate misure organizzative, fisiche e tecnologiche.

Esempi di tali misure sono la corretta gestione delle *patch* e l'utilizzo di un appropriato sistema di rilevamento *antimalware*.

Avere un adeguato *backup*, gestito separatamente al sistema informatico, aiuterà i sistemi medesimi di una piccola azienda ad essere gestiti nel miglior modo per mitigare le conseguenze di un attacco.

Inoltre, utile a tal fine è il programma di sicurezza, istruzione, formazione e sensibilizzazione rivolto ai dipendenti (*security, education, training and awareness program*, SETA) che può aiutare a prevenire e riconoscere questo tipo di attacco.

Tra queste misure, come detto, una gestione adeguata di aggiornamento della *patch* garantisce che i sistemi siano appunto aggiornati visto che la maggior parte degli attacchi *ransomware* sfruttano vulnerabilità ben note.

Nel valutare i rischi, il titolare del trattamento dovrebbe indagare sulla violazione e identificare il tipo di

codice dannoso per comprendere le possibili conseguenze dell'attacco.

Tra questi rischi, dovrebbe essere considerato il rischio che i dati siano stati esfiltrati senza lasciare traccia nei *log* dei sistemi.

In questo caso, l'autore dell'attacco ha avuto accesso ai dati in forma crittografata e questi sono stati compromessi. Tuttavia, tutti i dati che potrebbero essere stati esfiltrati non possono essere letti o utilizzati dall'autore, almeno per il momento.

La tecnica di crittografia utilizzata dal titolare del trattamento è conforme all'attuale stato dell'arte della tecnologia disponibile sul mercato.

Inoltre la chiave di decriptazione non è stata compromessa e, presumibilmente, neppure con altri mezzi. Di conseguenza, il rischio che i diritti e le libertà delle persone fisiche siano

compromessi è ridotto al minimo.

In generale, vieppiù, il titolare del trattamento dovrebbe anche considerare l'impatto e la gravità della violazione.

In questo caso, la mancanza di disponibilità dei dati oltre che la loro riservatezza non sono compromessi.

Gli effetti negativi della violazione sono stati mitigati celermente dopo la violazione stessa visto che il *backup* ha attutito le conseguenze ulteriori poiché i dati interessati dall'attacco sono stati ripristinati in poche ore, la violazione non ha comportato alcuna conseguenza sul funzionamento quotidiano del titolare del trattamento e non ha avuto effetti significativi sugli interessati (es. pagamenti dei dipendenti o gestione delle richieste dei clienti).

Mitigazione e obblighi

Senza un *backup*, alcune misure per porre rimedio alla perdita di dati personali possono essere intraprese dal titolare e i dati dovrebbero essere raccolti di nuovo.

Tuttavia, sempre in questo caso, l'attacco ha avuto un perimetro contenuto e il sistema è stato ripristinato da un *backup* "pulito" (privo di codice dannoso).

Infatti, le procedure di *backup* dovrebbero essere strutturate, coerenti e ripetibili.

Esempi di procedure di backup sono i file Metodo 3-2-1 e metodo nonno-padre-figlio.

Qualsiasi metodo dovrebbe sempre essere testato per verificarne l'efficacia, soprattutto per la capacità di ripristino. La verifica dovrebbe essere ripetuta a intervalli programmati e verificarne l'integrità del sistema.

Si comprende bene che senza un *backup* adeguato, i dati vengono persi e la gravità degli effetti dell'attacco possa aumentare,

con proporzionale aumento del rischio relativo e degli impatti per le persone fisiche.

La tempestività di ripristino dei dati dal *backup* è una variabile "chiave", anche al fine di analizzare gli impatti della violazione stessa.

Altrettanto rilevante, quindi, è l'intervallo di tempo impiegato per ripristinare i dati compromessi.

Come noto, il GDPR afferma che una violazione dei dati personali debba essere comunicata senza indebito ritardo e, ove possibile, non oltre 72 ore.

Pertanto, potrebbe essere stabilito che il superamento del limite di 72 ore è, in ogni caso, sconsigliabile ma quando si tratta di casi di livello ad alto rischio, anche il rispetto di questa scadenza può essere considerato insoddisfacente.

In questo caso, a seguito di una dettagliata valutazione d'impatto e di un processo di risposta all'incidente, il titolare del trattamento ha stabilito che è improbabile che la violazione abbia comportato un rischio per i diritti e le libertà delle persone fisiche, pertanto non è stata necessaria alcuna comunicazione agli interessati, né è stata necessaria la notifica all'Autorità Garante.

Tuttavia, poiché tutte le violazioni dei dati dovrebbero essere documentate ai sensi dell'articolo 33, paragrafo 5, GDPR, il titolare dovrebbe poter dare traccia dell'accaduto laddove si renda necessario a seguito di accesso da parte dell'Autorità Garante e per dimostrare che le misure di sicurezza sia state aggiornate e implementate in base all'attacco subito.

Azioni necessarie in base ai rischi

individuati

Nessun rischio (registro interno)	Rischio (comunicazione all'Autorità)	Alto rischio (comunicazione agli interessati)
✓	**X**	**X**

CASO N. 02: *Ransomware* senza *backup* adeguato

Uno dei computer utilizzati da un'azienda agricola è stato esposto ad un attacco *ransomware* e i suoi dati sono stati crittografati dall'aggressore. L'azienda si avvale dell'esperienza di società esterna di sicurezza informatica per monitorare la propria rete.

I *log* che tracciano tutti i flussi di dati in uscita dall'azienda (inclusa la posta in uscita) sono disponibili.

A seguito delle indagini interne coadiuvate dalla società di *cybersecurity* si è stabilito che l'autore dell'attacco ha solo crittografato i dati, senza esfiltrarli.

I registri non mostrano flussi di dati in uscita nel periodo di tempo dell'attacco. I dati personali interessati dalla violazione si riferiscono a poche decine di dipendenti e clienti dell'azienda.

No sono state coinvolte categorie particolari di dati.

Non era disponibile un *backup* in formato elettronico.

La maggior parte dei dati sono stati ripristinati da *backup* cartacei in 5 giorni lavorativi e ha comportato lievi ritardi nella consegna degli ordini ai clienti.

Misure preventive e valutazione del rischio

Il titolare del trattamento avrebbe dovuto adottare le stesse misure preventive menzionate nel paragrafo precedente. La principale differenza rispetto al caso precedente è la mancanza di un *backup* elettronico e la mancanza di crittografia "a riposo".

Le differenze sono le seguenti: nel valutare i rischi, il titolare del trattamento dovrebbe indagare sul metodo di infiltrazione e identificare il tipo di codice dannoso per comprendere le possibili conseguenze dell'attacco. In questo esempio il *ransomware* ha crittografato i dati personali senza esfiltrarli. Di conseguenza, sembra che i rischi per i diritti e le libertà degli interessati siano derivati dalla mancanza di disponibilità dei dati personali, e la riservatezza dei dati personali non è stata compromessa.

Un esame approfondito dei log del firewall e le sue implicazioni sono essenziali per determinare il rischio. Il titolare dovrebbe indagare sull'accaduto poiché, in caso di attacco più sofisticato, il *malware* potrebbe modificare i file di registro e rimuovere le tracce dell'attaco. Quindi, il titolare del trattamento non potrebbe affermare con certezza che il registro dei log potrebbe dimostrare l'assenza di esfiltrazione, quindi la probabilità di una violazione della riservatezza non può essere del tutto archiviata.

Bisognerebbe verificare se l'aggressore ha avuto accesso ai dati.

Durante la valutazione del rischio, il titolare del trattamento dovrebbe anche prendere in considerazione la natura, la sensibilità, il volume e il contesto dei dati personali interessati dalla violazione.

In questo caso nessuna categoria particolare di dati personali

sono oggetto dell’attacco e la quantità di dati violati e il numero di interessati è basso.

Bisogna, inoltre, raccogliere informazioni esatte sull’accesso non autorizzato per determinare il livello di rischio e prevenire un nuovo attacco o il prolungamento dello stesso attacco.

Se i dati fossero stati copiati dal database, andrebbe registrato un aumento del rischio.

Mitigazione e obblighi

Senza un *backup*, alcune misure per porre rimedio alla perdita di dati personali possono essere intraprese dal titolare del trattamento e i dati devono essere raccolti di nuovo, a meno che non sia disponibile un’altra fonte.

Senza un *backup*, i dati potrebbero andare persi e la gravità dipenderà dall’impatto per gli interessati medesimi.

Il ripristino dei dati non dovrebbe rivelarsi eccessivamente problematico se i dati sono ancora disponibili su cartaceo, ma data la mancanza di un *backup* elettronico, viene presa in considerazione una notifica all’Autorità di controllo in quanto il ripristino dei dati ha richiesto del tempo e potrebbe causare alcuni ritardi negli ordini di consegna ai clienti e una notevole quantità di metadati potrebbero non essere recuperabili (ad esempio log, timestamp).

Informare gli interessati della violazione può anche dipendere dalla durata di conservazione dei dati personali non più disponibili e della difficoltà di ripristinare la linea di business del titolare (es. ritardi nel trasferimento dei pagamenti dei dipendenti).

Tali ritardi nei pagamenti e nelle consegne possono comportare problemi finanziari per gli interessati e di conseguenza possono comportare un rischio elevato agli stessi.

Inoltre, non si può evitare di informare gli interessati nel caso in cui il loro contributo si renda necessario per ripristinare i dati crittografati.

Il caso in esame, attacco *ransomware* con rischio non elevato per i diritti e le libertà dei dati degli interessati soggetti, necessita comunque di comunicazione all'Autorità visto che lo stesso può avere riflessi sugli aspetti rilevati quali l'integrità dei dati

Azioni necessarie in base ai rischi individuati

Nessun rischio (registro interno)	Rischio (comunicazione all'Autorità)	Alto rischio (comunicazione agli interessati)
✓	✓	**X**

CASO N. 03: *Ransomware* con *backup* e senza esfiltrazione in un ospedale

Il sistema informativo di un ospedale è stato esposto ad un attacco *ransomware* e una parte significativa dei suoi dati è stata crittografata dall'aggressore. L'azienda sanitaria si avvale di una società di sicurezza informatica esterna per monitorare la propria rete.

Sono disponibili *log* che tracciano tutti i flussi di dati (inclusa la posta in uscita).

Dopo aver analizzato i log e i dati di altri sistemi è stato stabilito che l'autore del reato ha solo crittografato i dati senza esfiltrarli.

I registri non mostrano alcun flusso di dati in uscita nel periodo di tempo dell'attacco.

I dati personali interessati dalla violazione si riferiscono ai dipendenti e ai pazienti (migliaia di individui). Sono disponibili *backup* in formato elettronico.

La maggior parte dei dati è stata ripristinata ma questa operazione è durata 2 giorni lavorativi ed ha comportato notevoli ritardi nel trattamento dei pazienti con annullamento e rinvio di interventi chirurgici,

abbassando il livello di servizio per indisponibilità dei sistemi.

Misure preventive e valutazione del rischio

La particolarità del caso riguarda l'elevata gravità delle conseguenze per gli interessati.

La quantità di dati violati e il numero di interessati sono elevati, soprattutto per gli ospedali che di solito elaborano grandi quantità di dati.

L'indisponibilità dei dati ha un impatto elevato sugli interessati.

Inoltre, esiste un rischio residuale rispetto alla elevata gravità per la riservatezza dei dati del paziente.

Il tipo di violazione, la natura, la sensibilità e il volume dei dati personali interessati dalla violazione sono

importanti.

Anche se esisteva un *backup* per i dati e poteva essere ripristinato in pochi giorni, un rischio elevato esiste ancora a causa della gravità delle conseguenze per gli interessati derivanti dalla mancanza di disponibilità dei dati al momento dell'attacco e nei giorni successivi.

Mitigazione e obblighi

Si ritiene necessaria una notifica all'Autorità in quanto si tratta di categorie particolari di dati personali e

il ripristino dei dati potrebbe richiedere molto tempo, con conseguenti notevoli ritardi nella cura del paziente.

È necessario, inoltre, informare gli interessati della violazione a causa dell'impatto per i pazienti, anche dopo il ripristino dei file dati crittografati.

Infatti, il sistema informatico non era disponibile e sono stati compromessi i trattamenti dei pazienti che dovevano essere trattati in ospedale durante il periodo di attacco.

Il titolare del trattamento dovrebbe comunicare la violazione dei dati a quei pazienti direttamente coinvolti.

Potrebbe essere omessa la comunicazione diretta agli altri pazienti (alcuni dei quali potrebbero non essere stati ricoverati in ospedale per più di vent'anni) in ragione dell'eccezione di cui all'articolo 34, paragrafo 3, lettera c), GDPR.

Sarà, invece, opportuna una comunicazione pubblica o un provvedimento simile con cui gli interessati vengano informati in modo altrettanto efficace dell'attacco.

Tale scenario, inoltre, è il classico esempio di attacco *ransomware* ad alto rischio per i diritti e le libertà degli interessati.

Pertanto deve essere data comunicazione all'Autorità ai sensi dell'articolo 33, paragrafi 1 e 5, e data comunicazione agli interessati ai sensi dell'articolo 34, paragrafo 1.

Il titolare dovrebbe aggiornare i sistemi di sicurezza, aggiornarli e implementare misure organizzative e di mitigazione del rischio.

Azioni necessarie in base ai rischi individuati

Nessun rischio (registro interno)	Rischio (comunicazione all'Autorità)	Alto rischio (comunicazione agli interessati)
✓	✓	✓

CASO N. 04: *Ransomware* senza *backup* e con esfiltrazione

Il server di un'azienda di trasporto pubblico è stato esposto a un attacco *ransomware* e ai suoi dati sono stati crittografati.

Secondo i risultati dell'indagine interna l'autore ha crittografato i dati e li ha anche esfiltrati.

Il tipo di dati violati riguardano i dati personali di clienti e dipendenti (diverse migliaia di persone che utilizzano i servizi dell'azienda, quali ad es. per l'acquisto di biglietti online).

Sono stati inoltre esfiltrati i dati di identità di base, i numeri di carta d'identità e i dati finanziari come pure i dettagli della carta di credito.

Il *backup* esistente è stato crittografato dall'aggressore.

Misure preventive e valutazione del rischio

Sebbene il backup fosse disponibile lo stesso è stato oggetto di attacco.

Ciò pone in forte discussione il livello e la qualità delle misure di sicurezza IT adottate dal titolare del trattamento e ciò dovrebbe essere esame di ulteriore indagine, poiché l'architettura del sistema di *backup* deve essere ben protetta,

ben archiviata senza accesso dal sistema principale (altrimenti, come è accaduto, il *backup* potrebbe essere compromesso nello stesso attacco).

Questa violazione riguarda non solo la disponibilità dei dati, ma anche la riservatezza, poiché l'attaccante potrebbe aver modificato e/o copiato i dati dal server.

Pertanto, il tipo di violazione comporta un rischio elevato.

La natura, la sensibilità e il volume dei dati personali aumentano ulteriormente i rischi, perché il numero delle persone interessate è elevato, così come la quantità complessiva di dati personali degli interessati. Inoltre, i dati oggetto di attacco riguardano i dati identificativi di "base", i documenti di identità e dati finanziari come i dettagli della carta di credito.

Una violazione del genere presenta di per sé un rischio elevato e, se elaborati insieme, i dati esfiltrati potrebbero essere utilizzati, tra l'altro, per perpetrare casi di furto di identità o frode.

A causa di una architettura logica del *server* difettosa o dei controlli organizzativi, i file di *backup* sono stati coinvolti nell'attacco *ransomware*, impedendo il ripristino dei dati e aumentando il rischio.

Questa violazione dei dati presenta un rischio elevato per i diritti e le libertà delle persone, perché potrebbe comportare sia danni patrimoniali (es. perdita finanziaria) che danni non patrimoniali (es. furto di identità o frode).

Mitigazione e obblighi

La comunicazione agli interessati è essenziale, in modo che possano compiere i passi necessari per evitare ulteriori danni patrimoniali (ad esempio bloccare le loro carte di credito).

Come detto, il *server* è stato crittografato assieme al backup di riferimento ed i dati dettagliati di migliaia di interessati sono stati esfiltrati.

Perciò è necessario notificare l'accaduto all'Autorità ai sensi dell'articolo 33, paragrafi 1 e 5, e dare comunicare della violazione ai singoli interessati (articolo 34, paragrafo 1); inoltre il titolare dovrebbe dare notizia dell'attacco pubblicamente soprattutto per quei casi in cui sia difficile comunicare direttamente con il singolo interessato.

Il titolare potrebbe anche aver bisogno di aggiornare e correggere i propri dati personali organizzativi e tecnici gestione della sicurezza e misure e procedure di mitigazione del rischio.

Azioni necessarie in base ai rischi individuati

Nessun rischio (registro interno)	Rischio (comunicazione all'Autorità)	Alto rischio (comunicazione agli interessati)
✓	✓	✓

Misure organizzative e tecniche per prevenire/mitigare gli impatti di attacchi *ransomware*

Il fatto che possa aver avuto luogo un attacco *ransomware* è solitamente un segno di una o più vulnerabilità nel sistema di sicurezza adottato dal titolare.

Ciò vale anche nei casi in cui i dati personali siano stati crittografati ma non esfiltrati.

Indipendentemente dall'esito e dalle conseguenze dell'attacco,

l’importanza di una valutazione onnicomprensiva del sistema di sicurezza dei dati – con particolare enfasi sulla sicurezza IT – è imprescindibile.

I punti deboli e le falle della sicurezza informatica o organizzativa devono essere identificati, documentati e affrontati senza indugio.

Misure consigliate:

(l’elenco fornito dall’EDPB sulle seguenti misure non è in alcun modo esaustivo o completo. Piuttosto, l’obiettivo è fornire idee per la prevenzione del rischio e possibili soluzioni. Ogni attività di trattamento è diversa, da qui il titolare dovrebbe prendere la decisione su quali misure si adattano maggiormente alla situazione del caso concreto).

· Mantenere il *firmware*, il sistema operativo e il *software* applicativo su server, macchine *client*, componenti di rete attivi e qualsiasi altra macchina sulla stessa LAN (inclusi i dispositivi Wi-Fi) aggiornati. Garantire che tutte le misure di sicurezza IT siano in atto, assicurandosi che siano efficaci e siano continuamente aggiornati e mantenuti all’evoluzioni tecnologiche. Ciò include la conservazione di registri dettagliati di quali *patch* vengono applicate e in quale *timestamp*.

· Progettare e organizzare i sistemi e le infrastrutture informatiche in modo da segmentare o isolare i sistemi di raccolta e gestione dei dati e delle reti per evitare la propagazione di *malware* all’interno dell’organizzazione e verso sistemi esterni.

· Bisogna adottare e implementare una corretta procedura di *backup,* aggiornata, sicura e testata.

La gestione del *backup* dovrebbe essere tenuta separata rispetto alla raccolta e al sistema di archiviazione dei dati, con esclusione all’accesso da parte di personale non

autorizzato.

· Disporre/adottare un *software anti-malware* appropriato, aggiornato, efficace e integrato.

· Disporre di un *firewall* appropriato, aggiornato, efficace e integrato, con rilevamento delle intrusioni e sistema di prevenzione. È necessario sempre filtrare il traffico di rete attraverso il *firewall.*

· Erogare formazione ai dipendenti sui metodi per riconoscere e prevenire gli attacchi IT e segnalarli immediatamente al responsabile della sicurezza.

· Identificare il tipo di attacco per essere in grado di adottare le giuste misure per mitigare il rischio.

· Ridondare i registri sui flussi dati a un server di registro centrale (possibilmente includendo la firma o

marcatura temporale crittografica delle voci di registro).

· Adottare un tipo di crittografia e autenticazione avanzate, in particolare per l'accesso amministrativo ai sistemi IT (2FA), con chiavi appropriate e validi sistemi di gestione delle *password*.

· Effettuare periodici test di vulnerabilità e penetrazione.

· Istituire un CSIRT (*Computer Security Incident Response Team*) o un *Computer Emergency Response Team* (CERT) o prevedere un *team* collettivo.

· Quando si valutano le contromisure, l'analisi del rischio dovrebbe essere rivista e aggiornata.

Attacchi con esfiltrazioni di dati

Attacchi che sfruttano le vulnerabilità nei servizi offerti dal titolare del trattamento a terzi su Internet (es. commesso

tramite attacchi *injection* [*SQL injection, path traversal*], compromissione del sito web e metodi simili), possono assomigliare ad attacchi *ransomware* in quanto il rischio deriva dall'azione su di un file ad opera di terzi non autorizzati. Questi attacchi in genere mirano a copiare, esfiltrare e utilizzare i dati personali per finalità illecite.

Si tratta quindi principalmente di violazioni della riservatezza e, possibilmente, anche dell'integrità dei dati. Allo stesso tempo, se il titolare del trattamento è a conoscenza delle caratteristiche di questo tipo di violazioni, possono essere messe in atto misure in grado di ridurre il rischio derivante da un attacco.

CASO N. 05: Esfiltrazione di dati relativi alle candidature di lavoro da un sito *web*

Un'agenzia di collocamento è stata vittima di un attacco informatico, tramite codice malevolo inserito facendo breccia sul suo sito web. Questo codice dannoso rendeva le informazioni personali inviate tramite domanda di lavoro online (moduli memorizzati sul server web) accessibile a persone non autorizzate. Dall'esame dell'accaduto è stato constatato che non erano presenti categorie particolari di dati colpiti dalla violazione. Il particolare *toolkit malware* installato aveva funzionalità che ha consentito all'attaccante di rimuovere qualsiasi cronologia di esfiltrazione e ha anche consentito l'acquisizione dei dati personali. Il *toolkit* è stato scoperto solo un mese dopo il suo installazione.

Misure preventive e valutazione del

rischio

Le misure di sicurezza, come detto in precedenza devono essere costantemente aggiornate, i dati sensibili devono essere crittografati e le applicazioni devono essere sviluppate secondo *standard* di sicurezza elevati (*strong autentication*).

A tal fine sono inoltre necessari *audit* periodici della sicurezza IT, valutazioni delle vulnerabilità e test di penetrazione per rilevare in anticipo questi tipi di vulnerabilità e risolverli.

In questo caso particolare.

Il titolare del trattamento dovrebbe sempre indagare sulla violazione identificando il tipo di attacco e i sui metodi, al fine di valutare le misure da adottare.

Per essere veloci ed efficienti, il titolare dovrebbe disporre di un piano di risposta agli incidenti che specifichi i passaggi rapidi e necessari per gestire l'incidente.

In questo caso particolare, il tipo di violazione ha un fattore di rischio alto poiché è stata compromessa sia la riservatezza dei dati oltre che l'integrità visto che l'attaccante ha potuto acquisire i dati e modificarli.

Occorre sempre valutare la natura, la sensibilità e il volume dei dati personali interessati dalla violazione per determinare in che misura la violazione ha coinvolto gli interessati.

Sebbene nessuna categoria particolare di dati personali è stata coinvolta nell'attacco, i dati a cui si ha avuto accesso contengono considerevoli informazioni e tali dati potrebbero essere utilizzati in modo improprio in diversi modi (*targeting* con *marketing* non richiesto, furto di identità, ecc.), quindi se ne desume la gravità delle conseguenze e del relativo aumento del rischio delle libertà degli interessati.

Mitigazione e obblighi

Dopo aver affrontato l’attacco, il *database* dovrebbe essere confrontato con quello archiviato in un *secure*

backup. Dovrebbero essere aggiornate le infrastrutture IT e implementarle per evitare simili violazioni dei dati in futuro (ad esempio con controlli di integrità dei file e controlli di sicurezza).

Se i dati personali non sono stati solo esfiltrati, ma anche cancellati, il titolare deve porre rimedio a tale situazione cercando recuperare i dati personali nello stato in cui si trovavano prima della violazione.

Può essere necessario rivedere il metodo di archiviazione e le politica di conservazione dei dati per aumentare il livello di *data recovery*.

La violazione, che dovrà essere debitamente documentata, ha perciò comportato un rischio elevato per i diritti e le libertà degli interessati (che dovrebbero esserne assolutamente informati ai sensi dell’articolo 34, paragrafo 1), il che ovviamente significa andrà effettuata anche la comunicazione all’Autorità ai sensi dell’articolo 33, paragrafo 5, del GDPR.

Azioni necessarie in base ai rischi individuati

Nessun rischio (registro interno)	Rischio (comunicazione all’Autorità)	Alto rischio (comunicazione agli interessati)
✓	✓	✓

N. 06: Esfiltrazione di *password* con *hash* da un sito web

Una vulnerabilità *SQL Injection* è stata sfruttata per ottenere l'accesso a un *database* del *server* di un sito *web* dedicato alla cucina. Gli utenti potevano, come nomi utente, scegliere solo pseudonimi arbitrari. L'uso della posta elettronica era disincentivato.

Le *password* archiviate nel *database* sono state sottoposte ad *hashing* con estensione algoritmo forte e il sale non è stato compromesso.

Dati interessati: password con *hash* di 1.200 utenti.

Per motivi di sicurezza, il titolare del trattamento ha informato gli interessati della violazione tramite e-mail e ha chiesto loro di modificare le password, soprattutto se la stessa password è stata utilizzata per altri servizi.

Misure preventive e valutazione del rischio

In questo caso particolare la riservatezza dei dati è compromessa, ma le password nel *database* erano state impostate con metodo *hash* aggiornato, con ciò riducendo il rischio dell'attacco.

Questo caso non presenta rischi per i diritti e le libertà degli interessati.

Inoltre, le informazioni di contatto (ad esempio indirizzi e-mail o numeri di telefono) degli interessati non sono state compromesse, il che significa che non vi è alcun rischio significativo per gli interessati per altri tentativi fraudolenti (es. ricezione di e-mail di phishing o messaggi di testo e telefonate fraudolenti). Non sono stati attinte altre categorie di dati personali.

Alcuni nomi utente potrebbero essere considerati dati personali, ma la struttura del sito web non lo consentiva.

Bisogna considerare che la valutazione del rischio può cambiare se il tipo di sito web raccoglie o potrebbe rivelare categorie particolari di dati personali (es. sito web di alcuni partiti politici o di sindacati).

In generale, l'utilizzo di una crittografia all'avanguardia potrebbe mitigare gli effetti negativi di violazione. Inoltre, prevedere un numero limitato di tentativi di accesso impedirà eventuali attacchi *brute force*, riducendo così i rischi di attacco se si conosce già il nome utente.

Mitigazione e obblighi

La comunicazione agli interessati in alcuni casi potrebbe essere considerata un fattore attenuante, poiché gli interessati sono inoltre in grado di compiere i passi necessari per evitare ulteriori danni da violazione (ad esempio modificando la *password*).

In questo caso, la notifica non è obbligatoria, ma può essere considerata una buona pratica.

Il titolare del trattamento dei dati dovrebbe correggere la vulnerabilità e attuare nuove misure di sicurezza per evitare violazioni di dati simili in futuro come, ad esempio, controlli di sicurezza sistematici sul sito web.

La violazione dovrebbe essere documentata ai sensi dell'articolo 33, paragrafo 5, ma nessuna notifica o comunicazione all'Autorità sarà necessaria.

Inoltre, è fortemente consigliabile comunicare in ogni caso agli interessati una violazione delle *password*

anche quando le *password* sono state memorizzate utilizzando un *salt hash* con un algoritmo di ultima generazione.

Per ciò che attiene il *server,* è preferibile l'uso di metodi di autenticazione che elaborano *password* randomiche.

Inoltre, gli interessati dovrebbero avere la possibilità di scegliere le misure appropriate per le proprie *password*.

Azioni necessarie in base ai rischi individuati

Nessun rischio (registro interno)	Rischio (comunicazione all'Autorità)	Alto rischio (comunicazione agli interessati)
✓	**X**	**X**

CASO N. 07: Attacco di *credential stuffing* a un sito *web* bancario

Una banca ha subito un attacco informatico contro uno dei suoi siti *web* di *online banking*.

L'attacco mirava a enumerare tutti i possibili ID utente di accesso utilizzando una *password* banale fissa. Le password sono costituite da 8 cifre.

A causa di una vulnerabilità del sito *Web*, in alcuni casi sono trapelate delle informazioni degli interessati

(nome, cognome, sesso, data e luogo di nascita, codice fiscale, codici identificativi dell'utente), anche se la *password* utilizzata non era corretta o il conto corrente bancario non è più attivo.

Ciò ha interessato circa 100.000 soggetti. Di questi, l'attaccante si è connesso con successo a circa 2.000 account che utilizzavano l'accennata *password* banale.

Dopo il fatto, il titolare è stato in grado di identificare

tutti i tentativi di accesso illegittimi.

Inoltre, dopo ulteriori controlli antifrode, durante l'attacco nessuna transazione è stata eseguita da questi conti.

La banca era a conoscenza della violazione dei dati perché il suo centro operativo di sicurezza ha rilevato un numero elevato di richieste di *login* dirette al sito *web*.

In risposta, il titolare ha disabilitato la possibilità di accedere al sito spegnendolo e forzando il ripristino delle *password* degli account compromessi.

Il titolare ha comunicato la violazione solo agli utenti con gli account compromessi, ovvero agli utenti le cui password sono state compromesse o i cui dati erano stati divulgati.

Misure preventive e valutazione del rischio

È importante ricordare che i titolari del trattamento che trattano dati sensibili, informazioni finanziarie, ecc. hanno una responsabilità in termini di fornitura di un'adeguata sicurezza dei dati, ad esempio avere un centro operativo di sicurezza e altre misure di prevenzione, rilevamento e risposta agli incidenti.

Il mancato rispetto di questi *standard*, più elevati del normale, verrà valutato dall'Autorità in sede di indagini.

La violazione riguarda i dati finanziari oltre che l'identità e le informazioni sull'ID utente, rendendo la violazione particolarmente insidiosa.

Inoltre, il numero di interessati colpiti è elevato.

Il fatto che una violazione possa verificarsi in un ambiente così sensibile indica una significativa falla nella sicurezza dei dati e può essere un indice della necessità di revisione e

aggiornamento delle misure di sicurezza “adeguate” in linea con gli articoli 24 (1), 25 (1) e 32 (1) del GDPR.

I dati violati consentono l’identificazione univoca degli interessati e contengono altre informazioni su di essi (inclusi sesso, data e luogo di nascita), inoltre possono essere utilizzati dall’aggressore per fini ulteriori (quali una campagna di *spear phishing* diretta ai clienti della banca).

Per questi motivi, la violazione dei dati ha comportato un rischio elevato per i diritti e le libertà di tutti gli interessati e i danni patrimoniali e non patrimoniali non sono realmente ponderabili.

Mitigazione e obblighi

Le misure adottate dal titolare nel caso di specie sono adeguate.

Inoltre, durante l’attacco, sono state corrette le vulnerabilità del sito *Web* e sono state adottate altre misure per prevenire violazioni simili in futuro, come l’aggiunta dell’autenticazione a due fattori al sito *Web* e l’autenticazione “forte” del cliente.

In questo scenario, però, è necessario documentare la violazione ai sensi dell’articolo 33, paragrafo 5, GDPR e informarne l’Autorità. Inoltre, il titolare del trattamento dovrebbe notificare la violazione a tutti i 100.000 interessati (inclusi i dati soggetti i cui account non sono stati compromessi) ai sensi dell’articolo 34 GDPR.

Azioni necessarie in base ai rischi individuati

Nessun rischio (registro interno)	Rischio (comunicazione all'Autorità)	Alto rischio (comunicazione agli interessati)
✓	✓	✓

Misure organizzative e tecniche per prevenire / mitigare gli impatti di attacchi di hacker

Proprio come nel caso degli attacchi *ransomware*, indipendentemente dal risultato e dalle conseguenze dell'attacco, la rivalutazione della sicurezza informatica è obbligatoria per i titolari del trattamento in casi simili.

Misure consigliate:

(l'elenco fornito dall'EDPB sulle seguenti misure non è in alcun modo esaustivo o completo. Piuttosto, l'obiettivo è fornire idee per la prevenzione del rischio e possibili soluzioni. Ogni attività di trattamento è diversa, da qui il titolare dovrebbe prendere la decisione su quali misure si adattano maggiormente alla situazione del caso concreto).

· Crittografia e gestione delle chiavi secondo lo stato dell'arte vigente, soprattutto per quanto riguarda le *password* in merito alla gestione di dati sensibili o di dati finanziari. E' sempre preferito impiegare la crittografia all password *(hash* e *salting* crittografati per informazioni confidenziali. E' inoltre preferibile evitare l'elaborazione di *password* dal lato *server*.

· Mantenere aggiornato il sistema (*software* e *firmware*). Garantire che tutte le misure di sicurezza IT siano regolarmente aggiornate, cangianti ed evolute al caso di specie. Per poter dimostrare la conformità con l'articolo 5, paragrafo 1, lettera f) e paragrafo 2, del GDPR, il titolare del trattamento dovrebbe conservare un registro di tutti gli

aggiornamenti eseguiti, compreso anche il momento in cui sono stati applicati.

· Adottare una politica delle password *aggiornata* con uso di metodi di autenticazione "forte" (come autenticazione a due fattori e server di autenticazione).

· Adottare standard di filtraggio dell'*input* utente (come la limitazione del numero massimo di tentativi ovvero fare uso di "*Web Application Firewall*").

· Adottare forme di privilegi utente e criteri di gestione del controllo dell'accesso.

· Utilizzare firewall di rilevamento delle intrusioni aggiornato, efficace e integrato con i sistemi di difesa perimetrale.

· Effettuare audit sistematici della sicurezza informatica e valutazioni delle vulnerabilità (test di penetrazione). Revisioni e test regolari per garantire che i *backup* possano essere utilizzati per ripristinare i dati di cui l'integrità o la disponibilità è stata compromessa.

· Nessun ID di sessione nell'URL in testo normale.

Errore Umano

Il ruolo dell'errore umano nelle violazioni dei dati personali deve essere sempre evidenziato, a causa del suo comune verificarsi.

Poiché questi tipi di violazioni possono essere sia intenzionali che non intenzionali, è molto difficile per i titolari del trattamento identificare le vulnerabilità e adottare misure per evitarle.

L'*International Conference of Data Protection and Privacy Commissioners* ha riconosciuto l'importanza di affrontare la questione del fattore umani e ha adottato nell'ottobre 2019

(http://globalprivacyassembly.org/wp-content / uploads / 2019/10 / AOIC-Resolution-FINAL-ADOPTED.pdf) una risoluzione per affrontare il ruolo dell'errore umano nelle violazioni dei dati personali.

Questa risoluzione sottolinea che dovrebbero essere adottate adeguate misure di salvaguardia per prevenire errori umani e fornisce un elenco non esaustivo di tali tecniche di prevenzione.

CASO N. 08: Esfiltrazione di dati aziendali da parte di un ex dipendente

Durante il periodo di preavviso per le dimissioni, il dipendente di una società copia i dati aziendali dal *database* della società a cui è autorizzato ad accedere per ragioni del suo lavoro. Mesi dopo, dopo aver lasciato il lavoro, utilizza i dati così acquisiti (principalmente dati di contatto di base) per contattare i clienti dell'azienda per invogliarli alla sua nuova attività.

Misure preventive e valutazione del rischio

In questo caso particolare non sono state prese misure preventive per impedire al dipendente di copiare i contatti e le informazioni della clientela dell'azienda, poiché il lavoratore aveva accesso legittimo a queste informazioni.

Poiché la maggior parte degli impieghi relativi alle relazioni con i clienti richiede un qualche tipo di accesso dei dipendenti ai dati personali, queste violazioni dei dati possono essere più difficili da prevenire.

Le limitazioni all'accesso, infatti, possono limitare il

lavoro che il dipendente dovrebbe eseguire.

Tuttavia, le politiche di accesso ben ponderate e il controllo costante possono aiutare a prevenire tali violazioni.

Come al solito, durante la valutazione del rischio devono essere presi in considerazione il tipo di violazione, la natura, sensibilità e volume dei dati personali coinvolti.

Questi tipi di violazioni sono generalmente violazioni di riservatezza, poiché il *database* viene solitamente lasciato intatto, il suo contenuto viene "semplicemente" copiato per un ulteriore utilizzo.

Anche la quantità di dati interessati è generalmente bassa o media.

In questo caso particolare nessuna categoria particolare dei dati personali è stata attinta dalla violazione, il dipendente aveva bisogno solo delle informazioni di contatto dei clienti per mettersi in contatto con loro dopo aver lasciato l'azienda. Pertanto, i dati in questione non sono possono considerarsi dati "sensibili".

Sebbene l'unico obiettivo dell'ex dipendente, che ha maliziosamente copiato i dati, era limitato all'ottenimento delle informazioni di contatto della clientela della società per propri scopi commerciali, il titolare del trattamento non è in una posizione per considerare basso il rischio per gli interessati, dal momento che lo stesso non ha alcun tipo di rassicurazione sulle intenzioni del dipendente.

Pertanto, mentre le conseguenze della violazione potrebbero essere limitate all'utilizzo per auto-marketing non richiesto dell'ex dipendente, non è escluso che i dati rubati vengano comunque trattati illecitamente.

Mitigazione e obblighi

L’attenuazione degli effetti negativi della violazione nel caso di cui sopra è difficile. Potrebbe essere necessario promuovere un’azione legale immediata per impedire ulteriori impieghi dei dati parte dell’ex dipendente, come detto per trattarli illecitamente o diffonderli.

Come passo successivo, l’obiettivo dovrebbe essere quello di evitare situazioni future simili.

Il titolare potrebbe diffidare l’utilizzo abusivo di questi dati ma tale avviso non costituirebbe un valido deterrente.

Ad ogni modo, non esiste una soluzione valida per questo tipo di casi, ma un approccio sistematico può aiutare a prevenirli.

Ad esempio, l’azienda può implementare il sistema dei *log* di accesso in modo che l’accesso indesiderato possa essere registrato e contrassegnato.

Inoltre, il contratto di lavoro dei dipendenti dovrebbe includere clausole che proibiscono tali azioni di captazione maliziosa.

In questo specifico caso, però, visto che la violazione in questione non ha comportato un rischio elevato per i diritti e le libertà delle persone fisiche, sarà sufficiente la sola notifica all’Autorità.

Tuttavia, sarebbe più saggio provvedere alla comunicazione verso gli interessati per evitare che in futuro gli stessi possano apprendere della violazione, all’epoca tenuta nascota.

Inoltre, sarà necessario documentare la violazione ai sensi dell’articolo 33, paragrafo 5.

Azioni necessarie in base ai rischi individuati

Nessun rischio (registro interno)	Rischio (comunicazione all'Autorità)	Alto rischio (comunicazione agli interessati)
✓	✓	**X**

CASO N. 09: Trasmissione accidentale di dati a una terza parte (fidata)

Un agente assicurativo senza alcuno specifico motivo ha notato che, tramite le impostazioni errate di un file Excel ricevuto da una *e-mail*, è possibile accedere a informazioni relative a due dozzine di clienti.

Egli è vincolato dal segreto professionale ed è l'unico destinatario dell'*e-mail*.

L'accordo tra il titolare del trattamento e l'agente assicurativo obbliga l'agente a segnalare al titolare del trattamento ogni violazione dei dati personali senza ingiustificato ritardo.

Pertanto, l'agente immediatamente ha segnalato l'errore al titolare, che a sua volta ha corretto il file e lo ha rispedito, chiedendo all'agente di eliminare il messaggio precedente.

L'agente, poi, ha dato conferma dell'avvenuta cancellazione del messaggio "errato".

Le informazioni ottenute dall'agente non includono dati particolari ma solo dati di contatto e dati sull'assicurazione stessa (tipo di assicurazione, importo).

Dopo aver analizzato i dati personali interessati dalla violazione il titolare ha constatato che non vi è stato alcun impatto significativo sul livello di rischio o sui diritti e le libertà degli interessati.

Misure preventive e valutazione del rischio

A differenza del caso precedente, qui la violazione non deriva da una deliberata azione di un dipendente, ma da un errore umano involontario causato dalla disattenzione.

Questi tipi di violazioni possono essere evitati:

a) imponendo programmi di formazione, istruzione e sensibilizzazione in cui i dipendenti comprendano l'importanza della protezione dei dati personali;

b) tramite la riduzione dello scambio di *file* tramite posta elettronica, sarebbe opportuno utilizzare invece sistemi dedicati per l'elaborazione dei dati dei clienti;

c) prevedere un doppio controllo dei *file* prima dell'invio;

d) separando la creazione dall'invio dei *file*.

Questa violazione dei dati ha riguardato solo la riservatezza dei dati, mentre l'integrità e l'accessibilità di non sono stati compromessi.

La violazione dei dati ha riguardato solo circa due dozzine di clienti, da cui la quantità dei dati interessati può essere considerato basso.

Inoltre, i dati personali interessati non contengono dati particolari.

Il fatto che il responsabile del trattamento (l'agente) abbia contattato immediatamente il titolare del trattamento dopo essere diventato consapevole della violazione dei dati può

essere considerato un fattore di attenuazione del rischio (La possibilità che i dati siano stati inviati ad altri agenti assicurativi dovrebbe essere valutato e, se confermato, dovrebbero essere adottate misure adeguate).

In ragione dell'adozione di misure appropriate dopo la violazione dei dati, la violazione non avrà probabilmente alcun impatto sui diritti e le libertà degli interessati.

La combinazione del basso numero di persone interessate, l'individuazione immediata della violazione e le misure adottate per ridurre al minimo i suoi effetti rendono questo caso particolare senza rischi.

Mitigazione e obblighi

Nel caso in questione, sono in gioco anche altre circostanze di attenuazione del rischio: l'agente è vincolato dal segreto professionale; lui stesso ha segnalato il problema al titolare e ha cancellato il *file* su richiesta.

Implementando la consapevolezza del rischio e inserendo ulteriori passaggi nel controllo dei documenti che coinvolgono i dati personali potrebbe evitare casi simili in futuro.

Oltre a documentare la violazione ai sensi dell'articolo 33, paragrafo 5, non sono necessarie altre azioni.

Azioni necessarie in base ai rischi individuati

Nessun rischio (registro interno)	Rischio (comunicazione all'Autorità)	Alto rischio (comunicazione agli interessati)
✓	**X**	**X**

Misure organizzative e tecniche per prevenire/mitigare gli impatti di fonti interne di rischio umano

La combinazione delle misure sotto indicate – applicate a seconda delle caratteristiche del caso di specie – dovrebbe aiutare a ridurre la possibilità che una violazione simile si ripresenti nuovamente.

Misure consigliate:

(l'elenco fornito dall'EDPB sulle seguenti misure non è in alcun modo esaustivo o completo. Piuttosto, l'obiettivo è fornire idee per la prevenzione del rischio e possibili soluzioni. Ogni attività di trattamento è diversa, da qui il titolare dovrebbe prendere la decisione su quali misure si adattano maggiormente alla situazione del caso concreto).

· Attuazione periodica di programmi di formazione, educazione e sensibilizzazione per i dipendenti sui propri obblighi sulla *privacy*, sulla sicurezza, sul rilevamento e la segnalazione di minacce alla sicurezza dei

dati personali. È utile sviluppare una campagna di sensibilizzazione per ricordare ai dipendenti gli errori più comuni nelle violazioni dei dati personali e come evitarle.

· Istituzionalizzare solide ed efficaci pratiche, procedure e protocolli sulla *privacy* e sulla protezione dei dati.

· Valutazione delle pratiche, delle procedure e dei sistemi in materia di *privacy* per garantire l'efficacia continua degli stessi.

· Definizione di adeguati criteri di controllo degli accessi e definizione degli obblighi da seguire da parte di ciascun utente/dipendente.

· Implementazione di tecniche di autenticazione dell'utente

durante l’accesso ai dati personali particolari/sensibili.

· Disattivazione dell’*account* dell’utente in seno alla società non appena questi lascia l’azienda.

· Controllo del flusso di dati insolito tra il *file* server e le *workstation* dei dipendenti.

· Configurazione della protezione dell’interfaccia I/O nel BIOS o tramite l’uso di *software* che ne controlla l’utilizzo dell’interfacce del computer (blocco o sblocco, ad esempio USB / CD / DVD, ecc.).

· Revisione della politica di accesso dei dipendenti (ad es. Registrazione dell’accesso a dati sensibili e richiesta all’utente di inserire un motivo per il trattamento/consultazione, in modo che sia disponibile per gli audit).

· Disabilitazione dei servizi *cloud* aperti.

· Proibire e impedire l’accesso servizi di posta “aperti”.

· Disattivazione della funzione di stampa dello schermo nel sistema operativo.

· Applicazione di una politica della “scrivania pulita” (*clean desk policy*).

· Blocco automatico di tutti i computer dopo un certo periodo di inattività.

· Utilizzare meccanismi (ad esempio *token* (*wireless*) per accedere/aprire *account* bloccati) per il passaggio rapido degli utenti in ambienti condivisi.

· Utilizzo di sistemi dedicati per la gestione dei dati personali che applicano un adeguato meccanismo di controllo degli accessi e che prevengono l’errore umano, come l’invio di comunicazioni a destinatari sbagliati. L’uso di fogli di

calcolo e altri documenti d’ufficio non è un mezzo appropriato per gestire i dati dei clienti.

Dispositivi e documenti su carta smarriti o rubati

Un caso frequente è lo smarrimento o il furto di dispositivi portatili.

In questi casi, il titolare deve prendere in considerazione alcune circostanze del trattamento, come il tipo di dati memorizzati sul dispositivo, nonché le risorse di supporto e le misure adottate prima della violazione per garantire un adeguato livello di sicurezza.

Tutti questi elementi influenzano i potenziali impatti della violazione dei dati.

La valutazione del rischio potrebbe essere difficile, poiché il dispositivo non è più disponibile.

Questi tipi di violazioni possono sempre essere classificate come violazioni della riservatezza.

Tuttavia, se non c’è *backup* per il *database* rubato o smarrito, questo tipo di violazione può anche essere considerata come violazione della disponibilità e dell’integrità.

Gli scenari seguenti dimostrano come le circostanze sopra menzionate influenzano la probabilità e gravità della violazione dei dati.

CASO n. 10: materiale rubato contenente dati personali crittografati

Durante un’irruzione in un asilo nido per bambini, sono state

rubati due *tablet*.

I *tablet* in questione contenevano un'*app* che a sua volta deteneva i dati personali dei bambini che frequentano l'asilo nido (nome, data di nascita, dati personali sull'educazione dei bambini).

Entrambi i tablet avevano i file crittografati, erano spenti al momento dell'irruzione e l'*app* era protetta da un forte password.

I dati di *backup* erano effettivamente e prontamente disponibili.

Poco dopo il furto, l'asilo ha attivato a distanza un comando per "ripulire" i dati contenuti nei *tablet*.

Misure preventive e valutazione del rischio

In questo caso particolare, il titolare del trattamento ha adottato misure adeguate per prevenire e mitigare gli impatti di una potenziale violazione dei dati utilizzando la crittografia del dispositivo, introducendo un'adeguata protezione tramite *password* forte e con un *backup* dei dati memorizzati sui *tablet*.

Dopo essere venuto a conoscenza di una violazione, il titolare del trattamento dovrebbe valutare la fonte del rischio, valutare i sistemi di supporto, il tipo di dati personali coinvolti e il potenziale impatto della violazione dei dati rispetto alle persone interessate.

La violazione dei dati sopra descritta riguarderebbe la riservatezza, la disponibilità e l'integrità dei dati in questione, tuttavia grazie all'adeguatezza delle contromisure attuate dal titolare del trattamento prima e dopo la violazione dei dati nessuno di questi rischi si è verificato.

Mitigazione e obblighi

La riservatezza dei dati personali sui dispositivi non è stata compromessa dovuta alla predisposizione di una *password* complessa a protezione dei *tablet* oltre che dell'*app*.

I *tablet* sono stati impostati con una *password* e i sui dispositivi sono stati anche crittografati.

Si aggiunga che il titolare ha attivato da remoto un sistema di cancellazione dei dati contenuti nei dispositivi rubati.

In ragione delle misure adottate, anche la riservatezza dei dati è stata mantenuta intatta.

Inoltre, il *backup* ha garantito la continua della disponibilità dei dati personali, quindi nessun potenziale impatto negativo dovrebbe essersi verificato.

Quindi è improbabile che la violazione dei dati sopra descritta comporti un rischio per i diritti e libertà degli interessati, quindi nessuna notifica all'Autorità o agli interessati interessati andrà effettuata.

Tuttavia, anche questa violazione dei dati dovrà essere documentata ai sensi dell'articolo 33, paragrafo 5.

Azioni necessarie in base ai rischi individuati

Nessun rischio (registro interno)	Rischio (comunicazione all'Autorità)	Alto rischio (comunicazione agli interessati)
✓	**X**	**X**

CASO n. 11: materiale rubato

contenente dati personali non crittografati

Il *notebook* di un dipendente di una società di servizi è stato rubato.

Il dispositivo in questione conteneva nomi, cognomi, sesso, indirizzi e date di nascita di oltre 100000 clienti. A causa dell'indisponibilità del dispositivo rubato non è stato possibile identificare se sono state interessate anche altre categorie di dati personali. L'accesso al disco rigido del *notebook* era non protetto da alcuna *password*. I dati personali potrebbero essere ripristinati dai *backup* giornalieri (disponibili).

Misure preventive e valutazione del rischio

Nessuna misura di sicurezza preventiva è stata adottata dal titolare del trattamento, quindi i dati personali memorizzati sul *notebook* sono facilmente accessibile per il ladro o qualsiasi altra persona che, in seguito, è entrata in possesso del dispositivo.

Questa violazione dei dati riguarda la riservatezza dei dati archiviati sul dispositivo rubato.

Il *notebook* contenente i dati personali era, in questo caso, vulnerabile perché non possedeva alcuna protezione tramite *password* o crittografia.

La mancanza di misure di sicurezza di base aumenta il livello di rischio per i soggetti interessati.

Inoltre, è anche alto e problematico il rischio di identificazione degli interessati e ciò aumenta anche la gravità della violazione.

Il numero considerevole di interessati aumenta il rischio nonostante non siano stati attinti dalla violazione dati personali particolari.

Durante la valutazione del rischio, il titolare del trattamento dovrebbe prendere in considerazione le potenziali conseguenze e gli effetti negativi della violazione della riservatezza.

A seguito della violazione gli interessati possono subire frodi di identità in ragione dei dati disponibili sul dispositivo rubato, quindi il rischio è considerato elevato.

Mitigazione e obblighi

L'attivazione della crittografia del dispositivo e l'uso di una *password* complessa di protezione del *database* avrebbero impedito che la violazione dei dati comportasse un rischio per i diritti e le libertà degli interessati.

A causa di queste circostanze è richiesta la notifica all'Autorità, oltre che la comunicazione agli interessati

Azioni necessarie in base ai rischi individuati

Nessun rischio (registro interno)	Rischio (comunicazione all'Autorità)	Alto rischio (comunicazione agli interessati)
✓	✓	✓

CASO N. 12: *File* cartacei rubati con dati sensibili

Un registro cartaceo è stato rubato da una struttura di riabilitazione per tossicodipendenti.

Il registro conteneva l’identità di base e i dati sanitari dei pazienti ammessi alla struttura di riabilitazione. I dati sono stati memorizzati solo su carta e nessun supporto era disponibile per i medici che curano i pazienti. Il registro non era riposto in un luogo sicuro (in un cassetto chiuso a chiave o in una stanza) né era archiviato su di un *file.* Il titolare del trattamento non aveva adottato né una gestione di controllo degli accessi né alcun altra misura di salvaguardia della documentazione cartacea.

Misure preventive e valutazione del rischio

Nessuna misura di sicurezza preventiva è stata adottata dal titolare del trattamento, ne consegue che i dati personali memorizzati in questo registro erano facilmente accessibili per la persona che l’ha trovato. Inoltre, la natura dei dati personali conservati nel registro oltre che la mancanza di *backup* dei dati contribuiscono a descrivere il fattore di rischio molto alto.

Questo caso serve da esempio per una violazione dei dati ad alto rischio.

A causa della totale assenza di adeguate misure di sicurezza, i dati sanitari sensibili ai sensi dell’articolo 9, paragrafo 1, del GDPR sono andati persi.

Trattandosi di dati particolari il rischio potenziale è alto.

Questa violazione riguarda la riservatezza, la disponibilità e l’integrità dei dati personali coinvolti dalla violazione.

Invero, possono essere conosciute, da terzi estranei, importanti e private informazioni mediche dei pazienti e ciò può avere un grave impatto sulla vita personale del paziente.

La violazione della disponibilità può anche compromettere la continuità dei trattamenti medici dei pazienti.

Dal momento che non può essere esclusa la modifica e la cancellazione dei dati contenuti nel registro, l’integrità dei dati stessi è compromessa.

Mitigazione e obblighi

Durante la valutazione delle misure di sicurezza da adottare dovrebbe essere considerata anche l’attività (trattamento dei dati) che si intende svolgere.

Poiché il registro dei pazienti era un documento fisico, la sua custodia avrebbe dovuto essere predisposta in modo diverso. Ad esempio avrebbe potuto impedire la violazione dei dati la pseudonimizzazione dei nomi dei pazienti, la conservazione del registro in un locale custodito e chiuso in un cassetto a chiave o una stanza o l’adozione del controllo degli accessi con autenticazione.

La violazione dei dati sopra descritta può avere un grave impatto sugli interessati; quindi sono necessarie sia la notifica all’Autorità oltre che la comunicazione della violazione agli interessati.

Azioni necessarie in base ai rischi individuati

Nessun rischio (registro interno)	Rischio (comunicazione all’Autorità)	Alto rischio (comunicazione agli interessati)
✓	✓	✓

Misure organizzative e tecniche per prevenire/mitigare gli impatti di perdita o furto di dispositivi

Misure consigliate:

(l'elenco fornito dall'EDPB sulle seguenti misure non è in alcun modo esaustivo o completo. Piuttosto, l'obiettivo è fornire idee per la prevenzione del rischio e possibili soluzioni. Ogni attività di trattamento è diversa, da qui il titolare dovrebbe prendere la decisione su quali misure si adattano maggiormente alla situazione del caso concreto).

· Predisporre sistemi di crittografia del dispositivo (come Bitlocker, Veracrypt o DM-Crypt).

· Usare *passcode/password* complessa su tutti i dispositivi.

· Utilizzare l'autenticazione a più fattori.

· Attivare le funzionalità dei dispositivi altamente mobili che consentono di localizzarli in caso di smarrimento o furto (utilizzare il *software/app* MDM (*Mobile Devices Management*).

· Se possibile, salvare i dati personali non su un dispositivo mobile ma su un *server back-end* centrale.

· Se la *workstation* è connessa alla LAN aziendale, eseguire un *backup* automatico.

· Utilizzare una VPN sicura (ad esempio, che richiede una chiave di autenticazione a due fattori separata) per connettere i dispositivi mobili ai server *back-end*.

· Fornire serrature fisiche ai dipendenti per consentire loro di proteggere fisicamente i dispositivi mobili mentre rimangono incustoditi.

· Regolamentare adeguatamente l'utilizzo del dispositivo all'esterno dell'azienda.

· Corretta regolamentazione dell'utilizzo dei dispositivi all'interno dell'azienda.

· Utilizzare il *software/app* MDM (*Mobile Devices Management*) e abilitare la funzione di cancellazione remota.

· Utilizzare la gestione centralizzata dei dispositivi con “beneficio minimo” per gli utenti finali per l’installazione del *software*.

· Predisporre controlli di accesso fisico.

· Evitare di archiviare informazioni sensibili su dispositivi mobili o dischi rigidi. Se è necessario accedere al file sistema interno dell’azienda, è necessario utilizzare canali ben protetti.

Errore postale

Anche in questo frangente la fonte del rischio è un errore umano interno, senza però comportare una violazione dei dati. È solo il risultato della disattenzione. In questi casi, più che in altri tipi di violazione, il titolare del trattamento può fare ben poco, quindi la prevenzione è ancora più importante.

CASO N. 13: errore di posta ordinaria

Due ordini di scarpe sono stati confezionati da un’azienda di vendita al dettaglio. A causa di un errore umano due fatture di imballaggio sono state confuse con il risultato che sia i prodotti che le relative fatture di imballaggio sono stati inviati ai destinatari in modo sbagliato. Ciò significa che i due clienti hanno ricevuto gli ordini l’uno dell’altro, comprese le fatture di imballaggio contenente i dati personali.

Il titolare del trattamento, venuto a conoscenza della violazione, ha recuperato gli ordini e li ha inviati ai destinatari corretti.

Misure preventive e valutazione del rischio

Le fatture contenevano i dati personali necessari per una corretta consegna (nome, indirizzo, più l’articolo

acquistato e relativo prezzo).

È importante identificare come potrebbe essere accaduto l’errore umano e, se in qualche modo, avrebbe potuto essere prevenuto.

Nel caso in questione il rischio è basso, non vi sono dati particolari, non vi potrebbero essere abusi nel trattamento illecito né vi sono effetti negativi sulle persone coinvolte e la violazione non è il risultato di un errore sistemico da parte del titolare avendo riguardato solo due individui sono preoccupati.

Non è stato possibile identificare alcun effetto negativo sugli interessati.

Mitigazione e obblighi

Il titolare del trattamento, oltre che prevedere la restituzione gratuita degli articoli e delle fatture di accompagnamento, dovrebbe richiedere ai destinatari sbagliati di distruggere/cancellare tutte le eventuali copie delle fatture contenenti i dati personali di altre persone.

Anche se la violazione in sé non rappresenta un rischio elevato per i diritti e le libertà delle persone interessate (quindi la comunicazione agli interessati non è prevista dall’art. 34 GDPR), la comunicazione della loro violazione non può essere evitata, poiché la loro collaborazione è necessaria per mitigare il rischio.

Azioni necessarie in base ai rischi individuati

Nessun rischio (registro interno)	Rischio (comunicazione all’Autorità)	Alto rischio (comunicazione agli interessati)
✓	**X**	**X**

CASO n. 14: Dati personali sensibili inviati per posta per errore

Il dipartimento del personale di un ufficio della pubblica amministrazione ha inviato un messaggio di posta elettronica – riguardo i prossimi corsi di formazione – alle persone registrate nel suo sistema come persone in cerca di lavoro.

Per errore, un documento contenente tutti i dati personali di queste persone in cerca di lavoro (nome, indirizzo e-mail, indirizzo postale, numero di previdenza sociale) è stato allegato a questa e-mail.

Il numero di individui coinvolti è di oltre 60000.

Successivamente l’ufficio ha contattato tutti i destinatari chiedendo loro di cancellare il *file* contenuto nel messaggio precedentemente inviato e di non utilizzare le informazioni in esso contenute.

Misure preventive e valutazione del rischio

Si sarebbero dovute attuare regole più severe per l’invio di tali messaggi. È necessario prendere in considerazione meccanismi di controllo degli invii.

Il numero di persone colpite è considerevole come è altrettanto elevato il numero di dati diffusi, il che conseguentemente aumenta il livello di rischio.

L’eventuale ed ulteriore diffusione dei dati da parte di uno qualsiasi dei destinatari non può essere contenuta dal titolare.

Mitigazione e obblighi

Come accennato in precedenza, i mezzi per mitigare efficacemente i rischi di una violazione simile sono limitati.

Sebbene il titolare abbia richiesto l’eliminazione del messaggio, non può obbligare i destinatari a farlo, e di conseguenza, non può essere certo che quest’ultimi soddisfino la richiesta.

Per tale ragione dovrebbe la violazione dovrebbe essere documentata, notificata all’Autorità e comunicata agli interessati coinvolti.

Azioni necessarie in base ai rischi individuati

Nessun rischio (registro interno)	Rischio (comunicazione all’Autorità)	Alto rischio (comunicazione agli interessati)
✓	✓	✓

CASO N. 15: Dati personali inviati per posta per errore

Un elenco dei partecipanti a un corso di inglese giuridico che si svolge in un hotel per 5 giorni è stato inviato per errore al posto dell’hotel a 15 ex partecipanti al corso.

L’elenco contiene nomi, e-mail, indirizzi e preferenze alimentari dei 15 partecipanti.

Solo due partecipanti hanno compilato le proprie preferenze

alimentari, affermando che sono intolleranti al lattosio. Non è stata protetta l'identità dei partecipanti. Il titolare del trattamento scopre l'errore subito dopo aver inviato l'elenco e informa i destinatari dell'errore e chiede loro di eliminare l'elenco.

Misure preventive e valutazione del rischio

Si sarebbero dovute attuare regole più rigorose per l'invio di tali messaggi. È necessario prendere in considerazione meccanismi di controllo degli invii. Il rischio, rispetto al caso precedente, è basso.

I dati personali includono dati sensibili sulle preferenze alimentari di soli due dei partecipanti. Infatti, anche se si tratta di dati sanitari (il che può comportare solitamente un rischio elevato per l'interessato, cfr. Linee guida WP 250, p. 23.), il rischio che questi dati vengano utilizzati in maniera illecita dovrebbe essere considerato relativamente basso vista la bassa probabilità che tali informazioni sull'intolleranza al lattosio vengano divulgate con impatti patrimoniali e non patrimoniali: di solito l'intolleranza al lattosio normalmente non può essere collegata a nessuna informazione a carattere religiosa o filosofica.

Inoltre, la quantità dei dati violati e il numero di interessati è molto basso.

Mitigazione e obblighi

In sintesi, si può affermare che la violazione non ha avuto effetti significativi sugli interessati. Il fatto che il titolare del trattamento abbia contattato immediatamente i destinatari dopo essere venuto a conoscenza dell'errore può essere considerato un fattore attenuante.

Se viene inviata una *e-mail* ad un destinatario errato/non

autorizzato, il titolare del trattamento dovrebbe appore al messaggio di posta elettronica un messaggio di *follow-up* rispetto ai casi di inoltro errato laddove, scusandosi dell'accaduto, si diano istruzioni affinché l'*e-mail* i questione venga eliminata con avviso di non utilizzare ulteriormente il contenuto della stessa.

In questo caso, infatti, è improbabile che questa violazione dei dati comporti un rischio per i diritti e le libertà degli interessati, quindi non è necessaria alcuna notifica all'Autorità e agli interessati. Però, anche questa violazione dei dati deve essere documentata ai sensi dell'articolo 33, paragrafo 5.

Azioni necessarie in base ai rischi individuati

Nessun rischio (registro interno)	Rischio (comunicazione all'Autorità)	Alto rischio (comunicazione agli interessati)
✓	**X**	**X**

CASO N. 16: Errore di posta ordinaria

Un gruppo assicurativo offre assicurazioni auto. A tal fine, invia tramite posta ordinaria le polizze assicurative. Oltre al nome e all'indirizzo dell'assicurato, la lettera contiene il numero di immatricolazione del veicolo, le tariffe assicurative dell'anno in corso e del prossimo anno, il chilometraggio annuo approssimativo e data di nascita dell'assicurato. Non sono inclusi dati sanitari ai sensi dell'art. 9 GDPR, i dati di pagamento (coordinate bancarie), i dati economici e finanziari. Le lettere vengono imballate con macchine avvolgitrici automatiche. A causa di un errore meccanico, due lettere di diversi assicurati vengono inseriti

in una busta e inviati per posta ad un altro assicurato.

Il contraente apre la lettera e controlla sia la sua lettera oltre a quella inviata erratamente.

Misure preventive e valutazione del rischio

La lettera consegnata in modo errato contiene nome, indirizzo, data di nascita, numero di targa e la classificazione del tasso di assicurazione dell'anno in corso e del successivo. Se il tasso di assicurazione aumenta nell'anno successivo, indica che un sinistro automobilistico è stato presentato alla compagnia di assicurazione. Gli effetti sulla persona interessata devono essere considerati di media portata, poiché le informazioni, normalmente non disponibili al pubblico, come la data di nascita o il numero di immatricolazione del veicolo hanno un peso non irrilevante visto che, ad esempio, se un eventuale reclamo aumenta il tasso di assicurazione potrebbe significare anche che si sia verificato un incidente e tale informazione potrebbe essere divulgata ad un destinatario non autorizzato. La probabilità di un uso improprio di questi dati è valutata tra bassa e media.

Tuttavia, mentre molti dei destinatari probabilmente smaltiranno la lettera erroneamente ricevuta nella spazzatura, non è possibile escludere in maniera categorica che la lettera venga affissa, ad esempio, sui social *network* o che l'assicurato venga contattato direttamente.

Mitigazione e obblighi

Il titolare del trattamento dovrebbe ottenere la restituzione del documento originale a proprie spese. Il destinatario sbagliato deve inoltre essere informato che non può utilizzare impropriamente le informazioni acquisite per errore.

Probabilmente non sarà mai possibile impedire completamente un

errore di consegna postale in un invio di massa utilizzando macchine completamente automatizzate. Tuttavia, in caso di aumento della frequenza, è necessario controllare se le macchine avvolgitrici sono impostate e mantenute abbastanza correttamente, o se qualche altro problema al sistema può comportare una simile violazione.

Azioni necessarie in base ai rischi individuati

Nessun rischio (registro interno)	Rischio (comunicazione all'Autorità)	Alto rischio (comunicazione agli interessati)
✓	✓	**X**

Misure organizzative e tecniche per prevenire / mitigare gli impatti di errato

Misure consigliate:

(l'elenco fornito dall'EDPB sulle seguenti misure non è in alcun modo esaustivo o completo. Piuttosto, l'obiettivo è fornire idee per la prevenzione del rischio e possibili soluzioni. Ogni attività di trattamento è diversa, da qui il titolare dovrebbe prendere la decisione su quali misure si adattano maggiormente alla situazione del caso concreto).

· Stabilire *standard* precisi – senza spazio per l'interpretazione – per l'invio di lettere/*e-mail*.

· Adeguata formazione del personale su come inviare lettere/*e-mail*.

· Quando si inviano e-mail a più destinatari, per impostazione predefinita vengono elencati nel campo "Ccn".

· È richiesta una conferma aggiuntiva quando si inviano e-mail a più destinatari, e non sono elencati nel campo “Ccn”.

· Applicazione del principio dei quattro occhi (*four-eyes*).

· Indirizzamento automatico al posto del manuale, con dati estratti da *database* disponibile e aggiornato; il sistema di indirizzamento automatico dovrebbe essere riesaminato regolarmente per verificarne la presenza di errori nascosti e impostazioni errate.

· Applicazione dell’invio del “messaggio differito” (ad esempio, il messaggio può essere cancellato/modificato entro un determinato periodo di tempo dopo aver cliccato sul pulsante).

· Disattivazione del completamento automatico durante la digitazione degli indirizzi di posta elettronica.

· Sessioni di sensibilizzazione sugli errori più comuni che portano a una violazione dei dati personali.

· Sessioni di formazione e consegna di manuali su come gestire gli incidenti che portano a una violazione dei dati personali e chi tenere informato (coinvolgere il DPO).

Altri casi: ingegneria sociale

CASO n. 17: furto di identità

Il *contact center* di una società di telecomunicazioni riceve una telefonata da qualcuno che si presenta come un cliente.

Il sedicente cliente richiede all’azienda di modificare l’indirizzo di posta elettronica a cui le informazioni di fatturazione dovrebbero essere inviate da lì in poi. L’operatore del *contact center* convalida l’identità del cliente richiedendo alcuni dati personali, così come definiti dalle procedure dell’azienda. Il chiamante indica

correttamente il codice fiscale e l'indirizzo del cliente richiesto (perché aveva accesso a questi elementi). Dopo la convalida, l'operatore effettua la richiesta di cambio di informazione di fatturazione. La procedura non prevede alcuna notifica all'ex contatto *e-mail*. Il mese successivo il legittimo il cliente contatta l'azienda, chiedendo perché non riceve la fatturazione al suo indirizzo *e-mail* e nega qualsiasi chiamata da parte sua chiedendo il cambio del contatto *e-mail*. Successivamente, l'azienda si rende conto

che le informazioni sono state inviate a un utente illegittimo e annulla la modifica.

Valutazione, mitigazione e obblighi del rischio

Questo caso serve da esempio sull'importanza delle misure preliminari.

La violazione, dal punto di vista del rischio, presenta un alto livello di rischio, in quanto i dati di fatturazione possono fornire informazioni sulla vita privata dell'interessato (es. abitudini, contatti) e potrebbe causare danni patrimoniali e non (es. *stalking*, rischio per l'integrità fisica). I dati ottenuti durante questo attacco possono essere utilizzati anche per facilitare l'acquisizione illecita dell'*account* presso la stessa azienda attaccata o sfruttare ulteriori misure di autenticazione in altre organizzazioni.

Considerando questi rischi, la misura di autenticazione "appropriata" dovrebbe soddisfare un livello elevato, a seconda di quali dati personali possono essere elaborati a seguito dell'autenticazione.

Di conseguenza, sono necessarie sia una notifica all'Autorità oltre la comunicazione all'interessato da parte del titolare.

Il processo di convalida preliminare del cliente deve essere chiaramente perfezionato alla luce di questo caso. I metodi

utilizzati per l'autenticazione erano infatti insufficienti. Il malintenzionato è stato in grado di fingere di essere l'utente indicato tramite l'uso di informazioni pubblicamente disponibili a cui ha avuto accesso.

L'uso di questo tipo di autenticazione statica, basata sulla conoscenza (dove la risposta non cambia, e dove le informazioni non sono "segrete" come nel caso di una *password*) non è consigliato.

L'organizzazione dovrebbe, invece, utilizzare una forma di autenticazione con un alto grado di sicurezza, in cui l'utente sia in grado di dimostrare che sia la persona designata e non chiunque altro.

L'introduzione di un metodo di autenticazione a più fattori (*out-of-band multi-factor authentication*) risolverebbe il problema (ad esempio la modifica dovrebbe essere recapitata al contatto precedente, o si effettuano domande extra con informazioni visibili solo sulle bollette precedenti).

È responsabilità del titolare del trattamento decidere quali misure adottare, poiché conosce al meglio i dettagli e le esigenze del proprio funzionamento interno.

Azioni necessarie in base ai rischi individuati

Nessun rischio (registro interno)	Rischio (comunicazione all'Autorità)	Alto rischio (comunicazione agli interessati)
✓	✓	✓

CASO N. 18: Esfiltrazione di *e-mail*

Una catena di ipermercati ha rilevato, 3 mesi dopo la sua configurazione, che alcuni *account* di posta elettronica sono

stati compromessi in modo che ogni *e-mail* contenente determinate espressioni (ad es. “fattura”, “pagamento”, “bonifico bancario”, “autenticazione carta di credito”, “coordinate bancarie”) vengano inoltrati in una cartella inutilizzata e anche inoltrati a un indirizzo di posta elettronica esterno. Inoltre, a quel tempo, era già stato realizzato un attacco *social* in cui l’aggressore, fingendosi un fornitore, era riuscito a modificare i dettagli del conto bancario del vero fornitore con i suoi.

A quel punto, diverse fatture false erano state già inviate, con accluso il nuovo conto bancario.

La piattaforma del sistema di monitoraggio della posta elettronica ha fornito un avviso per quanto riguarda alcune cartelle. L’azienda non è stata in grado di rilevare come l’attaccante, sin dal principio, è stato in grado di accedere agli *account* di posta elettronica, ma supponeva che la colpa per aver dato accesso al gruppo di utenti incaricati dei pagamenti era da attribuirsi ad un *file* contenuto in una *e-mail* infetta.

A causa dell’inoltro di *e-mail* basato sull’intercettazione di alcune parole chiave, l’aggressore ha ricevuto informazioni su 99 dipendenti: nome e stipendio di un determinato mese riguardante 89 interessati; nome, stato civile, numero di figli, salario, orario di lavoro e altre informazioni sulla ricevuta dello stipendio di 10 dipendenti, i cui contratti di lavoro erano cessati.

Il titolare del trattamento ha dato comunicazione della violazione ai 10 dipendenti appartenenti a quest’ultimo gruppo.

Valutazione, mitigazione e obblighi del rischio

Anche se l’aggressore probabilmente non mirava a raccogliere

dati personali, poiché la violazione potrebbe comportare danni patrimoniali (ad es. perdita finanziaria) e non patrimoniali (ad es. furto di identità o frode) o potrebbe facilitare altri attacchi (ad esempio *phishing*), la violazione dei dati personali è da considerarsi ad alto rischio per i diritti e le libertà degli interessati.

Pertanto la violazione deve essere comunicata a tutti i 99 dipendenti e non solo ai 10 dipendenti, cui sono trapelate informazioni sullo stipendio.

Dopo essere venuto a conoscenza della violazione, il titolare del trattamento ha forzato la modifica della *password* dell'*account* compromesso, è stato bloccato l'invio di *e-mai*l all'*account e-mail* dell'aggressore, ha comunicato tale modifica al fornitore, ha rimosso le regole impostate dall'aggressore e perfezionato gli *alert* del sistema di monitoraggio per dare un *alert* non appena viene creata una regola automatica.

In alternativa, il titolare potrebbe rimuovere il diritto per gli utenti di impostare regole di inoltro, che necessitano dell'autorizzazione del *team* IT o potrebbe introdurre una politica per cui gli utenti sul trattamento dei dati finanziari.

Il fatto che una violazione possa verificarsi e non venga rilevata per così tanto tempo evidenziano problemi significativi nel sistema di sicurezza informatica del titolare; inoltre, in un lasso di tempo più lungo, tale attacco di ingegneria sociale avrebbe potuto essere utilizzato per compromettere dati ulteriori. Questi problemi dovrebbero essere affrontati senza indugio, come enfatizzare l'automazione delle revisioni e dei controlli delle modifiche, come pure il rilevamento degli incidenti, con adeguate misure di risposta. I titolari che gestiscono dati sensibili, informazioni finanziarie, ecc. hanno una responsabilità maggiore in termini di applicazione e implementazione di

adeguate misure di sicurezza dei dati.

Azioni necessarie in base ai rischi individuati

Nessun rischio (registro interno)	Rischio (comunicazione all'Autorità)	Alto rischio (comunicazione agli interessati)
✓	✓	✓

EDPB, pubblicate le linee guida su 18 casi d'uso riguardanti la notifica di violazione dei dati

---

DanaBot, nuova variante del trojan bancario si nasconde in chiavi software pirata

I ricercatori di Proofpoint hanno di recente individuato delle affiliazioni afferenti ad attori di minaccia che, con almeno un metodo di diffusione, stanno distribuendo una variante del trojan bancario Danabot, il cui aggiornamento risalirebbe a ottobre 2020.

DanaBot, le varianti

Scoperto per la prima volta nel maggio del 2018, al riguardo è memorabile la campagna malspam che ha interessato le PEC di

aziende e PA italiane alla fine dello stesso anno, sarebbero state tre le versioni principali del malware veicolate in vario modo (variante n.1 maggio 2018, variante n.2 ottobre 2019, variante n.3 febbraio 2019).

Nel corso del tempo, DanaBot è stato uno strumento abbastanza impiegato come servizio MaaS, venduto o noleggiato ad altri attori affiliati, in particolar modo, per colpire istituzioni finanziarie dislocate principalmente negli Stati Uniti, Canada, Germania, Regno Unito, Australia, Italia, Polonia, Messico e Ucraina, per poi scomparire dalle scene a giugno 2020 e riapparire in autunno con questa sua quarta variante.

L’analisi di un campione

Il rapporto tecnico pubblicato descrive l’analisi di un campione della nuova variante dalla quale risultano alcuni elementi d’interesse e parzialmente in comune con le precedenti versioni del malware.

L’architettura, implementata in linguaggio di programmazione Delphi, secondo caratteristiche modulari e multithreading, prevede una componente loader (file EXE) deputata alla decrittografia, decompressione ed esecuzione di una componente secondaria (file DLL) operante con quattro modalità di funzionamento predeterminate e codificate.

La revisione del codice ha inoltre permesso agli analisti di rilevare:

- delle specifiche routine anti analisi per ottenere un certo grado di offuscamento e persistenza;
- un protocollo di comunicazione C2 TOR based (hostname: 5jjsgjephjcua63go2o5donzw5x4hiwn6wh2dennmyq65pbhk6qflzyd\ . onion).

DanaBot: una modalità di distribuzione

Lo sfruttamento di vari siti Web che propinano, per una vasta gamma di programmi (antivirus, VPN, editor di grafica e documenti), il download gratuito di tools warez/crack con chiavi software pirata, sarebbe, secondo i ricercatori, uno dei principali metodi di distribuzione individuati.

Infatti la prova download, di un prodotto offerto da uno di questi siti scoperti, ha mostrato che quando un utente scarica ed esegue la chiave software, in realtà avvia un dropper e carica due componenti stealer sul dispositivo target. Una di queste componenti raccoglie informazioni di sistema, dati del browser e wallet di criptovaluta, l'altra installa un miner (implementato in AutoIt script) e il payload principale di DanaBot (hxxp [:] // 45.147.230 [.] 58 / palata.exe).

Come proteggersi

È ragionevole pensare che nei prossimi mesi, come stimato dallo stesso team di ricerca, non si possa escludere che il numero di affiliati che utilizzeranno quest'ultima o altre varianti DanaBot non possa ulteriormente crescere e con esso anche le campagne di phishing e malspam.

Pertanto per proteggersi da questi tipi di minacce, oltre che prestare attenzione allo spam e garantire una protezione antivirus affidabile, occorre senza dubbio usufruire di canali ufficiali e verificati per il download, evitando installazioni di terze parti, link torrent e condivisioni P2P che, in ogni caso, con vari espedienti possono indirizzare verso file malevoli (con estensioni .ZIP, .EXE, .PDF, .DOC e .JS) che, una volta eseguiti, avviano il processo d'infezione.

https://www.key4biz.it/danabot-nuova-variante-del-trojan-bancario-si-nasconde-in-chiavi-software-pirata/343453/

5G, certificazione Enisa per la sicurezza delle reti. Breton: “La cybersecurity al centro”

La Commissione europea ha stabilito che l’**Enisa**, l’Agenzia dell’Unione europea per la sicurezza informatica, avrà il compito di preparare il sistema di certificazione per la sicurezza delle reti 5G.

Lo schema, voluto fortemente dall’Unione, contribuirà a mitigare i rischi connessi alle vulnerabilità tecniche delle reti di quinta generazione e a rafforzarne ulteriormente la sicurezza.

*“La sicurezza è al centro del lancio della tecnologia 5G. La certificazione a livello UE, in combinazione con altri tipi di misure contenute nel **Toolbox 5G dell’UE**, sostiene i nostri sforzi per ottimizzare la sicurezza delle reti 5G e correggere le vulnerabilità tecniche”,* ha dichiarato **Thierry Breton**, commissario europeo per il mercato interno *.”Questo è il motivo per cui è importante che gli Stati membri facciano ulteriori progressi nell’attuazione del pacchetto di strumenti di attenuazione dei rischi cyber, concordato dagli Stati membri dell’UE”.*

In un comunicato l’Enisa ha dichiarato che il nuovo schema di certificazione cyber sarà basato su disposizioni già esistenti e dall’esperienza già acquisita dell’agenzia in ambito delle

certificazioni.

Per **Juhan Lepassaar**, direttore esecutivo dell'Agenzia dell'UE per la sicurezza informatica, *"la certificazione delle reti 5G emerge come il logico passo successivo nella strategia dell'UE sulla sicurezza informatica per il decennio digitale. La nuova iniziativa si basa sulle azioni già intraprese per mitigare i rischi cyber connessi alla tecnologia 5G ".*

Cosa prevede il toolbox della Commissione Ue per rendere sicure le reti 5G?

Il 5G offre una pluralità di vantaggi in diversi settori, ma solo se le reti sono sicure può offrire vantaggi positivi ai cittadini. Con questo principio di base gli Stati membri, tramite il gruppo di cooperazione **NIS**, hanno adottato il pacchetto di strumenti.

Ecco le misure e gli strumenti che gli Stati membri dovrebbero disporre per mitigare i rischi legati al 5G. In particolare dovrebbero affrontare questi aspetti:

- Rafforzare i requisiti di sicurezza per gli operatori di rete mobile;
- Valutare il profilo di rischio dei fornitori; applicare restrizioni pertinenti per i fornitori considerati "ad alto rischio", comprese le esclusioni necessarie per gli asset chiave.
- Assicurare che ciascun operatore disponga di un'adeguata strategia multi-vendor per evitare o limitare qualsiasi grande dipendenza da un unico fornitore ed evitare la dipendenza dai fornitori considerati alto rischio.

L’impegno dell’Enisa

A novembre 2019, l’Enisa, con il supporto degli Stati membri dell’UE, della Commissione europea ed esperti, ha pubblicato il primo 5G Threat Landscape, valutando le minacce legate alle nuove reti di telecomunicazione.

Un mese prima, gli Stati membri dell’UE hanno pubblicato la valutazione del rischio coordinata a livello di UE delle reti 5G, che contiene 10 scenari di rischio di alto livello, basati sulle valutazioni del rischio nazionali degli Stati membri.

Per approfondire

https://www.key4biz.it/5g-certificazione-enisa-per-la-sicurezza-delle-reti-breton-la-cybersecurity-al-centro/343140/

Malware, la botnet Emotet non esiste più

Emotet, la botnet malware più grande al mondo, non esiste più. Grazie ad un’operazione internazionale coordinata dall’Europol e dall’Eurojust in collaborazione con le autorità giudiziarie di Germania, Paesi Bassi, Stati Uniti, Regno Unito, Francia, Lituania, Canada e Ucraina, uno dei servizi di criminalità informatica più professionali e duraturi in circolazione, è stato sconfitto.

Emotet: la botnet attiva dal 2014

Apparsa in natura per la prima volta nel 2014, la botnet si è evoluta nel tempo fino a diventare un vero e proprio framework

criminale multi funzione. Emotet è un malware che si è diffuso nel corso degli anni passati prevalentemente tramite e-mail di phishing contenenti documenti Word infetti con un codice dannoso. Lo scopo di Emotet è quello installare una backdoor sui sistemi Windows così da renderli disponibili a vari scopi: distribuzione di ulteriore malware, ransomware e installazione di strumenti di accesso remoto.

Fonte: Europol

La collaborazione con i CSIRT

“Per interrompere l’infrastruttura Emotet, si legge nel comunicato dell’Europol, *le forze dell’ordine hanno collaborato per creare una strategia operativa efficace. Dato che l’infrastruttura utilizzata da Emotet ha coinvolto diverse centinaia di server dislocati in tutto il mondo, tutti dotati di funzionalità diverse per gestire i computer delle vittime infette, in un’operazione durata una settimana le forze dell’ordine e le autorità giudiziarie hanno acquisito il controllo dell’infrastruttura e l’hanno rimossa dall’interno. Le macchine infette delle vittime sono state reindirizzate*

verso questa infrastruttura controllata dalle forze dell'ordine", ha spiegato l'Europol. *"Un approccio nuovo e unico per interrompere efficacemente le attività dei facilitatori del crimine informatico".*

L'Europol sta infine collaborando con i **Computer Emergency Response Team** (CSIRT) in tutto il mondo per aiutare coloro che hanno subito infezioni da parte di Emotet. L'indagine è comunque ancora in corso per l'identificazione dei responsabili e della loro gestione una volta individuati.

https://www.key4biz.it/malware-la-botnet-emotet-non-esiste-piu/341932/

CSIRT, forze dell'ordine e magistratura. Come cooperare al meglio? Il report ENISA

L'Agenzia dell'Unione europea per la sicurezza informatica (**Enisa**) ha pubblicato un nuovo report per sostenere la cooperazione tra i **Computer Security Incident Response Team (CSIRT**), le forze dell'ordine e la magistratura.

Nel report dell'Enisa sono dettate le linee guida per aiutare ad affrontare le sfide di questa complessa cooperazione multi-stakeholder. Il rapporto, che comprende un manuale ed un set di strumenti per gli esperti, analizza ruoli, doveri, competenze, sinergie e potenziali interferenze tra i gruppi di risposta agli incidenti di sicurezza informatica (CSIRT), in

particolare quelli nazionali e governativi, le forze dll'ordine e magistratura (pubblici ministeri e giudici).

Il rapporto propone una metodologia per analizzare il quadro giuridico e organizzativo definendo i ruoli e i doveri, le competenze richieste dei CSIRT e delle forse dell'ordine. Identifica inoltre le sinergie e le potenziali interferenze che possono verificarsi durante le attività necessarie per rispondere a incidenti cyber e nella lotta alla criminalità informatica.

Il CSIRT in Italia

In Italia il CSIRT è attivo dal 6 maggio 2020. Istituito presso il **Dis**, il Dipartimento delle informazioni per la Sicurezza, e ha il compito di:

- definire le procedure tecniche per la prevenzione e la gestione degli incidenti informativi
- ricevere le notifiche sugli incidenti, fornire a chi ha effettuato la notifica le informazioni per facilitare una gestione efficace dell'evento ed informare gli altri Stati dell'Ue eventualmente coinvolti.
- Garantire la collaborazione nella rete Csirt, attraverso l'individuazione di forme di cooperazione appropriate, lo scambio di informazioni.

Per approfondire

Clicca qui per scaricare il report Enisa **"2020 Report on CSIRT-LE Cooperation"**

https://www.key4biz.it/csirt-forze-dellordine-e-magistratura-come-cooperare-al-meglio-il-report-enisa/341722/

Meetmindful, rubati i dati di 2,28 milioni di utenti (incluse le credenziali di Facebook)

Sono state rubate le informazioni di oltre 2,28 milioni di utenti registrati al sito di incontri **Meetmindful**. Tra questi, nomi, email, indirizzi, date di nascita, indirizzi IP, geolocalizzazioni, preferenze per gli appuntamenti e credenziali per entrare su **Facebook**.

Secondo il sito specializzato **ZDnet**, che ha riportato la notizia, i criminali informatici hanno condiviso un file da 1,2 Gb come download gratuito su un forum di hacking accessibile pubblicamente.

Fonte: Zdnet

Il contenuto di questo file include una grande quantità di informazioni fornite dagli utenti durante la configurazione dei profili sul sito MeetMindful e sulle app per i dispositivi mobili, ma non i messaggi scambiati dagli utenti.

Il file trapelato è stato visualizzato più di 1.500 volte e molto probabilmente scaricato, osserva ZDnet. I dati sono stati rilasciati da **ShinyHunters**, un hacker che all'inizio di questa settimana ha anche fatto trapelare i dettagli di milioni di utenti registrati su **Teespring**, un portale che consente agli utenti di creare e vendere abbigliamento personalizzato.

Allarme Sextortion

La fuga di dati dal sito **Meetmindful** rappresenta un grosso problema per gli utenti del sito e il motivo principale per cui **MeetMindful** deve informare i titolari degli account.

Il rischio infatti è che i criminali informatici possano usare i dati sottratti per attività illecite come il **Sextortion**, in cui i cyber criminali inviano email affermando di possedere informazioni compromettenti sul destinatario e minacciando la segnalazione a familiari o colleghi di lavoro.

https://www.key4biz.it/meetmindful-rubati-i-dati-di-228-milioni-di-utenti-incluse-le-credenziali-di-facebook/341294/