QuotidianoPIÙ

consulenti PRIVACY srl

Venerdì 03/05/2024 • 06:00

IMPRESA DATA BREACH

Attacchi informatici: la gestione tra cybersecurity e adempimenti

L'aumento degli **attacchi informatici** alle aziende italiane preoccupa per la sicurezza ICT nel Paese. Prevenire e reagire richiede un approccio integrato tra sicurezza informatica e **adempimenti legali**: formazione del personale, idonee misure di ***cybersecurity***, tempestiva valutazione dell'impatto e notifica delle violazioni.

di Fabio Pari - Avvocato - Resp. area legale www.skema.it

di Lucia Inzerilli - Avvocato – Privacy Officer www.iconsulentiprivacy.it

Secondo l'ultimo "*Rapporto Clusit sulla sicurezza ICT in Italia*", negli ultimi cinque anni il numero degli attacchi informatici alle aziende italiane è aumentato in maniera esponenziale sia in termini di frequenza che di gravità. Nel 2023 gli attacchi a livello mondiale sono aumentati dell'11%, mentre **in Italia sono aumentati addirittura del 65%.** Ma non solo: la frequenza di attacchi "critici" o "gravi" è passata dal 47% del 2019 al 56% del 2023. Ciò significa che un attacco su due causa ingenti danni all'azienda che lo subisce, come ad esempio il totale blocco operativo.

I dati relativi al 2023 attestano che **l'Italia rappresenta un bersaglio particolarmente facile**, avendo ricevuto ben l'11% di tutti gli attacchi rilevati a livello globale (contro un 3,4% del 2021 e un 7,6% del 2022). Il primo bersaglio sono i siti istituzionali/governativi, **seguiti dall'industria** (13%): è significativo che un quarto del totale degli attacchi rivolti al settore "*manufacturing*" a livello globale riguardi realtà manifatturiere italiane.

Dati che fanno riflettere se pensiamo al fatto che, dopo cinque anni dall'entrata in vigore del GDPR, la compliance aziendale in materia di protezione dei dati personali rimane spesso "sulla carta", sostanziandosi in meri adempimenti formali che non incidono su processi e cultura aziendale.

Già, la cultura aziendale: nell'ultimo report ENISA ("*Identifying Emerging Cyber Security Threats And Challenges For 2030*") viene previsto che l'aumento della tecnologia, dell'utilizzo dell'AI e delle tecniche avanzate di deepfake determineranno un significativo aumento degli attacchi cyber di tipo ransomware. Tra le cause principali viene indicato "**l'errore umano**", ponendo quindi l'attenzione sulle attività di sensibilizzazione e formazione del personale.

Spesso il management non è pienamente consapevole del fatto che la gestione di un attacco può avere un costo pesantissimo per l'azienda, sotto molti punti vista:

- sanzione che potrebbe comminare il Garante Privacy;
- *business continuity,* con ingenti costi connessi al blocco operativo, alla perdita dei dati ed alla rimessa in opera aziendale;
- perdita di dati riservati componenti il *know how* aziendale;
- danno di immagine (*brand reputation*).

L'attacco informatico è il *data breach* per eccellenza, che il GDPR definisce all'art. 4 comma 1 n. 12): "*Violazione dei dati personali = la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*".

Non a caso partiamo dalla definizione. La difficoltà più grande che riscontriamo nella nostra esperienza quotidiana parte proprio dalle basi: saper riconoscere un **data breach** per poi attuare ottimali strategie sia per gli stringenti adempimenti legali da porre in essere tempestivamente, sia in termini di cyber sicurezza informatica. Nella maggior parte dei casi la scarsa o addirittura assente formazione privacy e di cyber sicurezza del management e del personale, non solo è causa dell'incidente informatico, ma è anche motivo di ritardo nel riconoscimento e nella reazione all'evento.

Gestione della sicurezza informatica

Dal punto di vista della cyber sicurezza, è fondamentale che le aziende implementino una metodologia di analisi del rischio e adottino le conseguenti misure di sicurezza (**gestione dei rischi**), nonché stabiliscano un piano di risposta che permetta di rilevare, gestire e segnalare tempestivamente gli incidenti (**gestione degli incidenti**). Inoltre, la crescita dell'87% degli attacchi di phishing

ed ingegneria sociale, insieme alle previsioni ENISA sull'aumento futuro degli attacchi informatici al 2030, impongono alle aziende di **investire senza ritardi sulla formazione della governance e del personale**, le cui condotte sono quasi sempre la principale porta di ingresso per i criminali informatici (**gestione della governance**). Questi interventi, assieme a quelli necessari per la gestione della continuità operativa e la sicurezza della supply chain, dal **18 ottobre 2024 s**aranno obbligatori per una vasta categoria di aziende, come richiesto dalla **Direttiva NIS2.**

La valutazione del rischio

Dal punto di vista strettamente legale, l'azienda che subisce un attacco deve essere pronta ad effettuare gli adempimenti richiesti dalla normativa, *in primis* la **valutazione del rischio per i diritti e le libertà delle persone fisiche**, ossia quando la violazione può comportare un danno fisico, materiale o immateriale, per le persone fisiche i cui dati sono stati violati.

Qualora il rischio venga ritenuto improbabile, la violazione può non essere notificata all'autorità di controllo competente, ma il titolare del trattamento non è esentato da adempimenti.

Infatti, è necessario riportare nei propri disciplinari interni una descrizione puntuale della violazione, comprese le circostanze ad esse relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio, come disposto dall'art.33 del regolamento. Questa non è solo una prescrizione normativa, ma anche metro di giudizio dell'**Autorità Garante** nel comminare le sanzioni.

Ad esempio, si riporta il provvedimento sanzionatorio del 21 marzo 2024 riguardante la società LAZIOcrea S.p.a., responsabile del trattamento per conto della Regione e di diversi enti del servizio sanitario regionale. Detta società - oggetto di un attacco informatico, determinato da un malware di tipo ransomware - non ha fornito adeguata documentazione sulle decisioni assunte e sulle valutazioni svolte, in grado di comprovare che, con riferimento a tali trattamenti, fosse improbabile che la violazione presentasse un rischio per i diritti e le libertà degli interessati: detta mancanza è stata determinante nell'irrogazione della sanzione.

Diversamente, nel caso in cui la **violazione comporti un rischio per i diritti e le libertà degli interessati** scatta l'obbligo di notifica all'autorità garante entro 72 ore dalla conoscenza della violazione. Non è richiesta la ricostruzione integrale dell'evento (dati coinvolti, numero record, rischi per gli interessati), ciò che conta è notificare senza ritardo: è prevista infatti la possibilità di effettuare una notifica preliminare, integrabile successivamente.

In caso di notifica tardiva (oltre le 72 ore) occorrerà indicare i motivi del ritardo. Spesso, come sopra anticipato, la mancanza di rodate procedure interne e scarsa formazione del personale comporta ritardi nella notifica. Il ritardo andrà opportunamente argomentato con solidi motivi, in quanto l'art. 168 del Codice privacy "Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante" dispone che "*salvo che il fatto non costituisca più grave reato, chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito con la reclusione da sei mesi a tre anni*".

Inoltre, è indispensabile poter illustrare sin dalla notifica preliminare **i correttivi operati e le misure di sicurezza, tecniche e organizzative in essere** (ex art. 32 GDPR), che dovrebbero essere già state correttamente mappate nei registri del trattamento.

Se la violazione presenta un **rischio elevato** per i diritti e le libertà delle persone fisiche, sarà necessario darne comunicazione all'interessato senza ingiustificato ritardo, perciò il prima possibile. La soglia per la comunicazione delle violazioni alle persone fisiche è più elevata rispetto a quella della notifica alle autorità di controllo ed ha come obiettivo fornire loro informazioni specifiche sulle misure che questi possono prendere per proteggersi da eventuali conseguenze negative della violazione.

Misure organizzative

Un'azienda che ha agito proattivamente in termini di cyber sicurezza, di implementazione di idonee misure organizzative e sul piano della formazione, non solo sarà efficiente negli adempimenti legali, ma potrebbe scongiurare la necessità di notifica all'autorità di controllo ed evitare le notifiche agli interessati, non subendo ripercussioni sulla propria **brand reputation**, potendo anche arginare i costi nella rimessa in opera dei processi aziendali.

COSA POSSONO FARE LE IMPRESE?

È fondamentale che le organizzazioni implementino una metodologia di analisi del rischio e adottino le conseguenti misure di sicurezza (**gestione dei rischi**), nonché stabiliscano un piano di risposta che permetta di rilevare, gestire e segnalare tempestivamente gli incidenti (**gestione degli incidenti**). Inoltre, la crescita dell'87% degli attacchi di phishing ed ingegneria sociale, insieme alle previsioni ENISA sull'aumento futuro degli attacchi informatici al 2030, impongono alle aziende di **investire senza ritardi sulla formazione della governance e del personale**, le cui condotte sono quasi sempre la principale porta di ingresso per i criminali informatici (**gestione della governance**).

Questi interventi, assieme a quelli necessari per la gestione della continuità operativa e la sicurezza della supply chain, **dal 18 ottobre 2024 saranno obbligatori per una vasta categoria di aziende, come richiesto dalla Direttiva NIS2.**

Tuttavia, mai come in questi tempi **i dati esaminati richiedono alle aziende di investire** nella propria sicurezza informatica non per adempiere ad un obbligo normativo, ma **per tutelare il proprio business e la sicurezza dei propri dati.**

IL DATA BREACH STRESS TEST ®

Anche in questa sfida organizzazioni pubbliche e private potranno contare su di noi: visto il grande successo del nostro "Privacy Stress Test", abbiamo il piacere di presentare il "**Data Breach Stress Test**". Il servizio si compone di 3 moduli, interconnessi ma acquistabili separatamente, che hanno come obiettivo quello di **individuare le criticità aziendali nella gestione di una data breach**:

- **MODULO A**: legal audit sul rischio di data breach svolto attraverso l'analisi di: documenti (registro trattamenti, nomine responsabili ecc.); procedure operative (es. gestione data breach); misure di sicurezza dichiarate; analisi dei rischi:
- **MODULO B**: analisi cyber con emissione di report sulle criticità riscontrate, quali ad esempio: perimetro violato, risorse raggiunte, configurazioni mancanti;
- **MODULO C**: simulazione di attacco phishing basata sulle campagne attualmente in corso in Italia e costruita ad hoc mediante invio massivo di e-mail al personale aziendale.

Al termine delle attività, sulla base dei moduli acquistati, sarà prodotto un **REPORT** che evidenzierà che le lacune riscontrate in ambito legale, organizzativo e IT.

PER MAGGIORI INFO

SCRIVICI (commerciale@iconsulentiprivacy.it**) o CHIAMACI (**0541/1798723**)**