3M | The experts in screen privacy.

La preparazione al GDPR - FAQ (domande frequenti)

Enza Iannopollo, Forrester Research

Enza è un'analista del team Security & Risk, specialista certificata CIPP/E (Certified Information Privacy Professional). Presso la Forrester, Enza si occupa di protezione e riservatezza dei dati, dei sistemi di analisi dei dati e dell'Internet of Things, curando in particolare le procedure e le relative tecnologie.

Il regolamento GDPR rappresenta una delle più significative evoluzioni normative degli ultimi vent'anni sulla privacy dei dati. Il regolamento stabilisce le procedure mediante le quali le organizzazioni devono gestire i dati personali dei propri clienti, dipendenti e partner commerciali su base continuativa. 3M ha recentemente incontrato Enza Iannopollo della Forrester Research per discutere le misure di sicurezza e le politiche e i programmi di compliance in materia di privacy adottati dalle organizzazioni per conformarsi alle nuove normative come il GDPR. Enza ha analizzato l'adeguatezza dell'ambiente di lavoro evidenziando la necessità di protezioni fisiche per tutelare i dati contro le minacce alla privacy.

Ascoltiamo cosa ha detto.

Qual è la vera posta in gioco?

Le organizzazioni rischiano multe fino al 4 per cento del fatturato globale annuo o

€20 M

D. Il personale delle aziende è pronto a conformarsi al GDPR?

R. Secondo i dati che abbiamo raccolto, solo una su tre aziende nel mondo è pronta per la conformità al regolamento generale sulla protezione dei dati (GDPR). Poiché il regolamento GDPR entrerà in vigore il 25 maggio 2018, è chiaro che molte imprese dovranno impegnarsi rapidamente per completare il lavoro di adeguamento.

In particolare, abbiamo notato che le imprese hanno problemi nel soddisfare i requisiti necessari a documentare e attuare la formazione sulla privacy e i programmi di sensibilizzazione dei dipendenti. Le autorità di regolamentazione dell'UE hanno segnalato che questi programmi sono essenziali per la conformità al GDPR. D'altro canto abbiamo rilevato che le organizzazioni che sono state capaci di soddisfare tali requisiti hanno talmente migliorato la cultura della privacy a livello aziendale e le prassi adottate, che talvolta hanno superato gli standard previsti dalle normative.

D. Le imprese sono più pronte in alcune regioni specifiche rispetto ad altre?

R. Il 34 per cento delle imprese statunitensi afferma di essere pronto rispetto al 26 per cento delle imprese europee.[1] Le imprese che non hanno raggiunto la conformità al regolamento GDPR, che ne siano consapevoli o meno, corrono un grosso rischio dal punto di vista commerciale e imprenditoriale. Le aziende che si ritengono pronte ma che in realtà non lo sono, corrono un rischio ancora maggiore.

È interessante notare che un numero maggiore di imprese statunitensi ritiene di essere conforme rispetto a quelle europee. Questo dato ha a che fare con gli effetti extraterritoriali del regolamento GDPR. Il regolamento si applica infatti a tutte le imprese che elaborano o custodiscono dati personali dei cittadini residenti nell'Unione Europea, indipendentemente dalla loro ubicazione. Questo significa che non solo le imprese europee ma anche quelle che hanno sede centrale negli USA sono tenute a rispettare queste rigorose norme sulla privacy.

Abbiamo il sospetto che una lettura superficiale della normativa, combinata con aspettative ingannevoli e infondate relative all'incapacità di fare osservare il regolamento GDPR, potrebbe aver distorto la percezione delle aziende in merito alla propria conformità.

D. Quali sono le misure di sicurezza fisica e della privacy previste dal GDPR?

R. Il GDPR è un regolamento basato su principi. Ciò significa che il regolamento non fornisce alle organizzazioni un insieme di azioni precise da seguire. È compito delle imprese riflettere sui requisiti del GDPR come su una sorta di "condizione desiderata" per le loro procedure di gestione dei dati. Ciò significa anche che le organizzazioni devono identificare e valutare i rischi specifici che devono essere ridotti in modo da conformarsi con i requisiti previsti dal regolamento GDPR.

Nell'identificazione dei rischi, le imprese devono considerare quelli correlati all'elaborazione dei dati, in particolare quelli associati alla perdita accidentale o illecita, alla divulgazione non autorizzata o all'accesso a dati personali trasmessi, memorizzati o elaborati in qualsiasi modo. Non importa se la divulgazione non autorizzata dei dati avviene a causa di un ben orchestrato attacco cibernetico da parte di hacker su un sito web aziendale o perché un estraneo scatta una foto di dati sensibili visualizzati sullo schermo del computer portatile di un dipendente. Entrambi i casi rappresentano rischi gravi e richiedono adeguate strategie di mitigazione.

D. L'hacking visivo rappresenta un rischio?

R. Assolutamente sì. Basta ricordare che Le "chiavi del paradiso" per molte organizzazioni prendono la forma di un nome utente e una password. Basta una rapida occhiata su uno schermo non protetto per consentire a un individuo non autorizzato di ottenere tali chiavi e accedere al dispositivo. E il rischio aumenta col crescere della sofisticazione delle tecniche di "social engineering".

Un anno fa un giornalista ha subito una violazione mentre lavorava su un aereo.[2] Il pirata informatico è stato in grado di descrivere i particolari di un articolo che il giornalista stava scrivendo, dei messaggi di posta elettronica personali che aveva inviato e dei successivi incontri di lavoro - tutte informazioni che ha detto di aver ottenuto hackerando la rete wi-fi dell'aeromobile. O forse il pirata informatico potrebbe semplicemente aver dato uno sguardo allo schermo del computer portatile del giornalista. Il giornalista si è indignato, ma ha capito il messaggio: quando si lavora su un articolo sensibile - in questo caso si trattava di un'analisi delle vaste e profonde implicazioni per la privacy del rifiuto della Apple di accettare la richiesta dell'FBI di decrittare il telefono di un terrorista - è necessario tutelare la privacy e la proprietà intellettuale sul proprio dispositivo. Come il giornalista, molte organizzazioni fanno lo stesso errore di sottovalutazione del rischio dell'hacking visivo e informatico.

D. Quali sono i vantaggi dell'adozione di protezioni fisiche low-tech?

R. Viste le incessanti notizie di violazioni dei dati su larga scala, oggi è facile dimenticare che le aziende che operano in un mondo digitalizzato devono pur sempre fare i conti con la sicurezza fisica. L'adozione di protezioni fisiche, come ad esempio le telecamere per la videosorveglianza, le serrature per le custodie dei notebook e i filtri per la privacy per monitor, laptop, tablet e smartphone, offre molteplici vantaggi. I filtri per la privacy, ad esempio, costituiscono una solida strategia di riduzione del rischio per le violazioni della privacy e dei dati. Basta che alcuni dati sensibili dei clienti o dei dipendenti vengano esposti alla

visione delle persone sbagliate per generare una violazione dei dati che potrebbe rappresentare una situazione potenzialmente molto dannosa e oggetto di pubblicità negativa per l'organizzazione.

I filtri inoltre contribuiscono a incrementare la conformità con regolamenti diversi dal GDPR. Ad esempio, pochi anni fa un operatore sanitario è stato licenziato da un ospedale annesso alla University of Iowa per aver violato la normativa sulla protezione dei dati dei pazienti. L'operatore è stato accusato di aver violato visivamente la cartella medica del paziente mentre veniva esaminata da un collega, e questa è una violazione della legge HIPAA.[3]

Le protezioni fisiche, come i filtri per la privacy, rappresentano un promemoria visivo per i dipendenti affinché le migliori pratiche per la sicurezza e la privacy divengano una priorità per l'organizzazione. E, come sempre in caso di privacy visiva, non si tratta solo di soddisfare i requisiti di conformità. Si tratta di proteggere il patrimonio più prezioso dell'impresa.

D. In che modo le imprese possono sfruttare la privacy per poter instaurare con il cliente relazioni di qualità superiore?

R. Le imprese che adottano il regolamento GDPR e rigorosi programmi sulla privacy, oltre alla conformità ottengono una serie di vantaggi. Una migliore esperienza del cliente è uno di questi. Il modo in cui un'organizzazione protegge i dati dei propri clienti può avere un impatto diretto nella costruzione, o distruzione, del sottostante sentimento di fiducia che i clienti hanno nella stessa organizzazione.

Per esempio, sappiamo bene che in seguito a una violazione della privacy i clienti passano a un concorrente.[4] Inoltre il nostro studio sugli atteggiamenti dei consumatori verso la privacy rileva che il 30 percento delle persone rifiuta di completare una transazione online se legge qualcosa di ambiguo nell'informativa sulla privacy di tale organizzazione.[5]

Se vi impegnerete a proteggere i dati dei vostri clienti e i vostri dipendenti riconosceranno e adotteranno lo stesso impegno nelle loro interazioni con il cliente, potreste distinguervi dalla concorrenza.

D. Ci sono aziende che si distinguono per il loro impegno verso la privacy e la sicurezza?

il 23% delle imprese Fortune 100

ha inserito la privacy tra le iniziative prioritarie volte al miglioramento della responsabilità sociale d'impresa (CSR).

R. Il tema della privacy è cambiato sensibilmente, da un argomento di nicchia riservato agli uffici legali è diventato un valore fondamentale per molte organizzazioni. Oggi i CIO e i CMO sono i funzionari aziendali più convinti che la protezione del patrimonio di dati dagli attacchi e dell'uso improprio sia tra le priorità di un'azienda. Il nostro studio ha evidenziato che il 23% delle imprese Fortune 100 ha inserito la privacy nelle proprie iniziative volte al miglioramento della responsabilità sociale d'impresa (CSR).[6] Circa il 70 percento ha incluso la sicurezza nei propri rapporti sulla CSR.

Abbiamo anche notato che le imprese impegnate nella tutela della privacy e della sicurezza traggono vantaggio dal dimostrarsi aperte e trasparenti sulle modalità di gestione dei dati personali. Questo può essere un modo estremamente valido per dare valore al rapporto con i clienti, i dipendenti e i partner commerciali. Tuttavia, operare in conformità con tale impegno non è semplice. Spesso le organizzazioni, per evidenziare il loro impegno nel costruire una cultura aziendale che riconosca privacy e sicurezza come valori essenziali, devono cambiare il loro modo di operare.

D. Sono previste altre normative come il GDPR in un prossimo futuro?

R. Non vi è alcun dubbio: il regolamento GDPR indica solo una tendenza. Di recente abbiamo completato una nuova ricerca che analizza le procedure e le normative sulla privacy in 54 Paesi.[7] È evidente che in alcune zone, come la regione Asia-Pacifico, ci si aspetta che il GDPR rappresenti un'evoluzione delle locali normative sulla privacy. In altre regioni, come l'America Latina e la Russia, elementi del GDPR, come la custodia dei dati, vengono integrati nelle normative sulla privacy. Infine il Parlamento Europeo sta lavorando per aggiornare i requisiti dell'attuale direttiva ePrivacy. I particolari sono ancora in fase di definizione, ma il proposito è quello di normalizzare i requisiti della normativa ePrivacy con quelli del regolamento GDPR.

[1]Forrester Technographics Business Security Survey, 2017
[2]Digital Trends, "Apple vs FBI shown in different light as journalist hacked mid-flight," 25 gennaio 2016
[3]Veriphyr, "Medical Assistant Fired for "Shoulder Surfing" and Breaching Patient Data Privacy," 2011
[4]Ponemon Institute, "The Impact of Data Breaches on Reputation and Share Value", maggio 2017
[5]Forrester Research Consumer Technographics European Online Benchmark Survey (Parte 2), 2016
[6]Forrester Report "The Future of Data Security and Privacy: Growth And Competitive Differentiation," 2017
[7]Forrester "Interactive Data Privacy Heat Map," 2017

FORRESTER®