Fulcri Privacy

NEWSLETTER

novembre 2019

Gentile Cliente,
torna il consueto appuntamento mensile con gli aggiornamenti in relazione alle novità rilevanti in tema privacy, sicurezza e GDPR.

Questa newsletter si divide in tre parti:

- Minacce informatiche ed in particolare il fenomeno, sempre più diffuso, degli attacchi informatici condotti tramite i c.d. “ransomware”;
- L’attività ispettiva programmata dal Garante per il periodo luglio-dicembre 2019 con particolare riferimento all’attività di fidelizzazione (cd. fidelity card);
- Le perplessità del Garante sulle modalità di applicazione della fatturazione elettronica.

Minacce informatiche

Diverse associazioni che si occupano di sicurezza informatica (come ad esempio il Clusit - Associazione Italiana per la Sicurezza Informatica) hanno reso disponibili le statistiche relative agli attacchi informatici per il 2019.

Tale fenomeno è in preoccupante ascesa, soprattutto per quanto riguarda gli attacchi veicolati tramite i c.d. “ransomware”.

Ma cosa sono i ransomware? E come è possibile tutelarsi da tali attacchi?

In parole molto semplici, i ransomware sono particolari tipi di programmi malevoli (*malware*) che, se installati dall’utente, procedono a cifrare tutti i dati presenti sul dispositivo elettronico, rendendoli inaccessibili i dati e richiedendo un riscatto (dal gergo anglosassone “ransom”) per rendere nuovamente accessibili i dati.

Occorre segnalare che tali minacce riguardano tutte le organizzazioni, senza alcuna distinzione relativa al *core business*. Il rapporto Clusit evidenzia però che il settore della sanità (Farmacie, Medici e strutture sanitarie in generale) e finanziario (Istituti di credito e assicurazioni) è particolarmente soggetto a tali attacchi, circostanza da porre in stretta correlazione in relazione alla delicatezza dei dati trattati da tali organizzazioni.

Il canale di diffusione principale di tali minacce è rappresentato dalle email: il soggetto riceverà una comunicazione sul proprio dispositivo con un allegato che, se aperto, procederà alla cifratura di tutti i dati contenuti al suo interno.

La comunicazione a mezzo email inoltrata presenta sempre un contenuto particolarmente allarmante per il destinatario, in modo da spingere quest’ultimo all’apertura dell’allegato.

Quali sono le cautele che possono essere prese in considerazione per scongiurare tali minacce?

Tralasciando l'aspetto strettamente legato alle misure di sicurezza tecniche-informatiche (installazione di antivirus regolarmente aggiornati sulle periferiche, adozioni di firewall hardware e software etc..), occorre formare il proprio personale ed "educarlo" al riconoscimento di tali minacce, in modo da sventare l'apertura di allegati malevoli.

Alcuni consigli molto pratici per prevenire tali infezioni:

- evitare l'apertura di allegati alle comunicazioni provenienti da soggetti sconosciuti;
- verificare con attenzione la correttezza del testo contenuto nei messaggi (molto spesso le comunicazioni accompagnatorie contengono imprecisioni, refusi ed errori in lingua italiana perché tradotte da altre lingue con tool online);
- effettuare una copia di sicurezza dei dati e conservarla su unità di memoria non direttamente collegate alla rete della propria organizzazione (ad esempio, un hard disk portatile conservato in un cassetto chiuso a chiave e non collegato in rete);
- effettuare periodicamente sessioni di formazione destinate al personale delle funzioni aziendali più sensibili (ad esempio autorizzati al trattamento che lavorano nell'amministrazione e hanno possibilità di disporre pagamenti verso i fornitori oppure facenti capo alla funzione commerciale).

Si ricorda che, qualora si subisca una infezione da parte di questo di tipo di software malevolo e l'organizzazione non sia in grado di procedere a ripristinare la disponibilità dei dati cifrati, tale casistica rientra in quelle per le quali è necessario procedere a notificare una violazione dei dati personali (c.d. *data breach*) all'autorità Garante e procedere a dare avviso della violazione anche ai soggetti interessati della violazione.

Dalla lettura del bilancio dell'applicazione del GDPR (periodo 25 maggio 2018 – 30 settembre 2019) reso disponibile dall'Autorità Garante il 29 ottobre 2019, si evince che le notifiche relative alle violazioni dei dati personali sono state 1.520 (una media di circa 3 notifiche al giorno), dato sicuramente che conferma l'attenzione da porre su questo delicato argomento.

Le ispezioni del Garante

Con delibera del 12.9.2019 il Garante ha programmato l'attività ispettiva per il periodo luglio-dicembre 2019, attività ispettive che sono attualmente in corso di svolgimento.

L'Autorità ha specificato su quali aspetti focalizzerà l'attenzione in sede di ispezione. Tra le diverse aree sotto la lente di ingrandimento, occorre segnalare in particolare i trattamenti di dati effettuati in relazione alle attività di profilazione relative ai possessori di carte fedeltà (c.d. fidelity card).

Tali controlli verteranno sul rispetto dell'obbligo dell'**informativa** e sulle condizioni per il rilascio del **consenso** da parte degli interessati, oltre che sulla durata del periodo di **conservazione** dei dati personali raccolti in relazione a tale finalità.

Gli aspetti sopraelencati, oggetto dell'attività ispettiva, sono disciplinati da specifiche domande all'interno del tool, all'interno delle informative e dei moduli di consenso che vengono messi a disposizione dei clienti, oltre che all'interno del registro delle attività di trattamento generato.

La fatturazione elettronica

È di questi ultimi giorni la memoria con cui il Garante ha informato la Commissione Finanze della Camera delle proprie perplessità sollevate dal decreto fiscale al vaglio delle Camere.

In particolare il Garante non ritiene conforme alla normativa privacy l'art. 14 del decreto che al momento consente all'Agenzia delle Entrate e alla Guardia di Finanza di memorizzare i file delle **fatture elettroniche** fino al 31.12 dell'ottavo anno successivo a quello di presentazione della dichiarazione di riferimento o alla conclusione di eventuali giudizi. I dati oggetto di tale memorizzazione includono quelli inerenti **la natura, la qualità e la quantità dei beni e dei servizi oggetto della prestazione di cui alla fattura emessa**.

La ratio della norma è evidentemente quella di coadiuvare la Guardia di Finanza nella lotta all'evasione fiscale e nelle normali funzioni di polizia economica-finanziaria svolte, ma di fatto contrappone l'interesse dell'Agenzia delle Entrate a quello di tutela dei dati personali perseguito dal Garante.

Questa previsione normativa ha infatti risollevato l'attenzione del Garante sulla "***proporzionalità***" del trattamento rispetto al fine rincorso.

Proprio su questo punto emergono le perplessità del Garante: la **memorizzazione** dei dati così **analitica**, il **periodo di memorizzazione più lungo**, i maggiori poteri dei Finanzieri, sono tutti fattori che rischiano di ledere il principio di proporzionalità, come il Garante ha già avuto modo di chiarire e sostenere nei precedenti provvedimenti del 18.11 e 20.12.2018.

Nella memoria trasmessa alle Camere il Garante ha sottolineato come questa modalità di archiviazione dei dati fornisca all'Agenzia delle Entrate anche **informazioni sensibili sui cittadini**, a proposito del loro **stato di salute** o eventuale sottoposizione a **procedimenti giudiziari**, che emergerebbero nel caso di fatture relative a prestazioni in ambito sanitario o forense.

La nota del Garante, al di là del destinatario specifico, ci ricorda uno dei **principi cardine** da tenere sempre presente nel trattamento dei dati personali: secondo il principio di minimizzazione dei dati, **i dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati**. Il trattamento dei dati personali infatti che effettuiamo non deve **mai prescindere dai principi applicabili** al trattamento dei dati personali **di cui all'art. 5 GDPR**.

Il Garante, concludendo, ha ritenuto che la conservazione prevista dall'art. 14 del decreto fiscale sia sproporzionata ed ha pertanto chiesto di valutare l'effettiva necessità dell'archiviazione integrale dei dati di fatturazione per la durata prevista.

Per ulteriori informazioni commerciale@fulcri.it