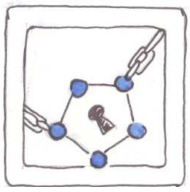

*Allerta Rossa*

# L'angolo della privacy

## *Comunicazione ai Clienti: crescenti attacchi cryptolocker - gestione data breach*

Stiamo assistendo ad un aumento massiccio di attacchi ai sistemi informatici aziendali finalizzati al "sequestro" delle informazioni attraverso la cifratura dei dati con algoritmi quasi impossibili da decifrare senza la relativa chiave di decrittazione.

Gli attacchi possono originarsi da comportamenti ingenui degli utenti (che aprono mail sospette o confermano installazione di programmi o componenti fraudolenti presenti su siti Internet che a loro volta sono stati hackerati o costruiti ad hoc per attirare navigatori inesperti), oppure da attacchi mirati alla rete informatica aziendale, spesso dopo settimane se non mesi di tentativi, studio delle porte aperte sui firewall, server esposti su Internet, software e sistemi operativi non aggiornati ecc.. L'elenco delle vulnerabilità sarebbe molto lungo ed ogni giorno potrebbe arricchirsi di nuovi elementi che vengono scoperti e sfruttati dai malintenzionati.

Sotto il profilo privacy – GDPR (che è l'ambito di nostra competenza e per cui Le scriviamo questo pro-memoria), subire un attacco cryptolocker con o senza esportazione (quindi "furto" di dati), equivale a subire un data breach che ai sensi dell'art. 33 del GDPR deve essere gestito ed eventualmente notificato anche al Garante Privacy ed agli interessati (soggetti cui si riferiscono i dati oggetto del data breach ai sensi dell'art. 34 del GDPR).

Il nostro invito è quindi di sollecitare periodicamente il settore IT (sia esso interno oppure affidato a tecnici esterni) affinché verifichi le misure di protezione attuate in azienda ed evidenzi eventuali criticità o proposte di miglioramento, che sarà poi il Titolare del trattamento a valutarne l'adozione o meno.

Ricordiamo infatti che ai sensi dell'art. 32 del GDPR (sicurezza nei trattamenti) compete al Titolare del trattamento attuare ogni misura ritenuta utile per la protezione del dato, adottando misure di sicurezza che ritiene adeguate rispetto ai trattamenti effettuati; non sono infatti più presenti le misure "minime" di sicurezza come nel precedente codice privacy, ma solo misure "adeguate" che non sono elencate nella norma.

Ci si deve quindi basare su buone prassi dettate anche dal progresso tecnologico e calibrate in funzione degli strumenti elettronici adottati, dando attuazione ai principi di privacy by design e di privacy by default (art. 25 del GDPR), secondo il concetto di "responsabilizzazione" (accountability – art. 24 del GDPR).

Un eventuale data breach, sia nel caso in cui si possa risolvere con il ripristino dei dati (decrittazione, ripristino senza furto dei dati), sia nel caso in cui vada notificato al Garante, comporta la compilazione di relazioni (interne o trasmesse al Garante privacy)

con descrizione di quanto accaduto e relativa documentazione a supporto.

In caso di notifica al Garante, è quasi certa almeno una successiva richiesta di ulteriori informazioni da parte del Garante stesso, ma potrebbe anche comportare una ispezione in azienda: quindi ogni anomalia o incidente sulla sicurezza deve essere comunicato anche al DPO (se nominato) e gestito dal Titolare senza indugi o ritardi.

Tra le informazioni da verificare ed eventualmente trasmettere al Garante entro 72 ore dal verificarsi della violazione, vi sono anche le misure di sicurezza adottate, che unitamente all'analisi del rischio sono contenute nella documentazione che andiamo a redigere con la conclusione dell'impostazione del piano privacy.

Alla luce di quanto sopra, ricordiamo al Titolare del trattamento che è suo onere verificare costantemente sia l'effettiva applicazione delle misure dichiarate, sia la valutazione (diretta o con il supporto dei tecnici informatici) del fatto che siano ancora attuali e sufficienti, ed eventualmente implementarle, rivedendo ed adeguando di conseguenza la documentazione privacy.

Ovviamente tutta la documentazione (registri dei trattamenti, lettere di nomina e autorizzazione, formazione al personale ecc.) deve essere presente ed aggiornata in quanto potrebbe essere richiesta dal Garante.

In occasione di audit periodici sul piano privacy adottato, alcuni dei controlli sulle misure di sicurezza dovrebbero vedere il coinvolgimento dell'amministratore di sistema (se presente) o del settore IT, il quale è chiamato ad esprimersi sull'idoneità o meno di quanto impostato dall'azienda a protezione del dato, consentendo al Titolare di avere gli elementi per effettuare una valutazione sul grado di sicurezza dei trattamenti effettuati e sulle eventuali carenze rilevate dall'IT. Potrebbero essere utili, per incrementare ulteriormente gli elementi di prova a favore del Titolare, audit tecnici da parte di personale IT non abitualmente coinvolto nella gestione delle infrastrutture IT e penetration test sia interni che esterni, le cui risultanze possono evidenziare eventuali falle nei sistemi installati.

Nel restare quindi a disposizione per eventuali chiarimenti o supporto nella valutazione di eventuali data breach, raccomandiamo ancora di verificare con regolarità il corretto funzionamento dei processi di backup e verificare (anche attraverso il personale IT) l'adeguatezza dei backup rispetto ad attacchi di tipo criptolocker (es. modalità di backup non attaccabili dai crypto, conservazione su supporti off line, ridondanza dei processi di backup, cloud backup ecc.), comunicandoci anche in questo caso eventuali variazioni nelle procedure censite nella documentazione privacy.

In ultimo, durante l'imminente periodo feriale, considerando che molti attacchi mirati partono nei week end o in occasione di chiusura delle normali attività proprio per avere maggiori chances di non essere scoperti, un'utile contromisura potrebbe essere quella di spegnere server, modem, firewall ecc. durante il periodo di chiusura per ferie.

**Fonte: Pentha s.r.l.**