Le conseguenze dell'Art.32 del GDPR in caso di attacco

Luigi-Enrico Tomasini
Vertical Software Product Director

CyberExpert

Sicurezza informatica:
come difendersi dalle minacce cyber

Proteggere i tuoi dati è una priorità

GDPR – Art.32 –§1,2

CyberExpert

Sicurezza del trattamento

1. **Tenendo conto** dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e **delle finalità del trattamento**, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, **il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio**, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla **distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati**.

IMPLICAZIONI CON IL GDPR

Mettere al riparo i propri strumenti informatici significa rispettare il principio di garanzia della **sicurezza dei dati** posto in essere dal GDPR, con particolare riferimento all' art. 32, comma 1, lettera D.

Obbligo

«….il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio…»

Adempimento

«una procedura per testare, verificare e valutare *regolarmente* l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.»

Come evidenzia il GDPR ed altre leggi, regolamenti e linee guida in materia di sicurezza informatica, ci si aspetta quindi che le aziende **monitorino e mantengano una consapevolezza sufficiente** delle minacce e delle vulnerabilità della cybersicurezza in modo che possano valutare il rischio e rispondere di conseguenza.

ESEMPIO PRATICO REALE

CyberExpert

Qualche mese fa (novembre) ci contatta un nostro cliente/partner del mondo IT a cui abbiamo fatto una scansione con la nostra piattaforma cyber.expert 3 mesi prima (agosto).

Dal venerdì avevano problemi con i server, la domenica mattina un tecnico si collega per fare un controllo e trova la sua macchina tutta bloccata e cifrata. In sintesi:

- CRYPTATI i Server (impossibile accedere);

- FORMATTATI i NAS (elemento di repository, backup);

- CRYPTATI i client della rete che erano accesi;

Trovato il file dove spiegavano le modalità di riscatto – ransomware infection **BANTA**

Chi ha perpretato la truffa è un criminale e non ci si contratta:
- non è detto che si accontenti della cifra e che permetta realmente di decifrare tutti i dati dopo aver pagato e quindi chiede altri soldi;
- pagando non si è certi che i dati non vengono cmq pubblicati sul web;
- non pagando che reazione potrebbero avere gli hacker?

AZIONI INTRAPRESE

CyberExpert

E' stata fatta intervenire una società specializzata per:

- mettere in sicurezza le macchine, scansionarle;
- Indagare su come sono riusciti a forzare il perimetro, qual'è stata la vulnerabilità che hanno sfruttato;
- Installare degli agent per prevenire nuovi rischi e propagazione;
- Indagare se ci sia stata esfiltrazione di dati;
- Monitoraggio 24x7 dell'intera rete dal SOC per 15 giorni (30k€);
- Provare a ripristinare i NAS formattati per capire se c'era qualcosa di recuperabile (spesa di circa 20k€).

Namirial è stata chiamata come società di supporto sistemistica che ha eseguito le operazioni on situ richieste dalla società specializzata. Il nostro cliente aveva tutti i backup per cui è stato possibile ripristinare in 10 giorni tutto l'ambiente **senza dover pagare il riscatto**.

CHECK CON DPO

Hanno copiato dei Database con i dati degli utenti (ad esempio anagrafiche licenze, gestione ticket)?

Hanno attaccato la contabilità con le informazioni dei clienti?

Dobbiamo procedere con la notifica al garante con il rischio di prendere la sanzione?

- sanzioni amministrative;
- sanzioni penali;
- condanna al risarcimento del danno;
- divieto temporaneo di trattamento dei dati personali (fino a che non venga ripristinata una condizione di conformità alla normativa).

Sanzioni privacy possano arrivare fino a **20 milioni di euro, e colpiscono fino al 2% o al 4% del fatturato annuo** delle imprese non conformi

CONCLUSIONE DEL DPO

Che si tratti di un data breach non vi è dubbio, così come non c'è dubbio sul fatto che questa violazione deve essere documentata nel registro interno delle violazioni e segnalata alla Polizia Postale.

Sul quesito se questo tipo di violazione vada anche notificata al Garante o meno, nel rispetto ovviamente di quanto previsto dal GDPR:

- ai sensi dell' art. 33 del GDPR il data breach va notificato al Garante entro 72 ore dal momento in cui se ne viene a conoscenza ma solo se la violazione può mettere a **rischio i diritti e le libertà degli interessati**.
- l'analisi di tutti i possibili rischi e le possibili conseguenze legate all'evento è stata fatta con riferimento sia all'ipotesi di "non disponibilità del dato" sia di "furto/esfiltrazione dello stesso".

….non si è ritenuto coerente procedere con una notifica al Garante in quanto verificato che non sussistono rischi per i diritti e le libertà delle persone fisiche in quanto da tutti i controlli non ci sono conseguenze di nessun tipo per gli interessati coinvolti.

E LA VULNERABILITA'???

CyberExpert

Risultato della scansione di agosto: evidenza di alcune vulnerabilità, in particolare 2 riferite ad un software di mercato utilizzato per la gestione della documentazione condivisa.

Target	Vulnerabilità	Severity	Soluzione
[redacted]88	[redacted] < 6.13.23 / 6.14 < 7.4.11 / 7.5 < 7.11.6 / 7.12 < 7.12.5 Webwork OGNL Injection (CONFSERVER-67940)	HIGH	Upgrade to [redacted] version 6.13.23, 7.4.11, 7.11.6, 7.12.5 or later.
[redacted].188	[redacted] Server Webwork OGNL Injection (CVE-2021-26084)	HIGH	Upgrade to [redacted] version 6.13.23, 7.4.11, 7.11.6, 7.12.5 or later.

Vulnerabilità già segnalata dal produttore con invito a eseguire l'aggiornamento della versione.

L'indagine ha mostrato che l'attacco è stato fatto utilizzando esattamente la vulnerabilità evidenziata nel report la cui risoluzione il cliente aveva rinviato per motivi di tempo e priorità