SANS SECURITY AWARENESS

La Newsletter Mensile di sensibilizzazione alla sicurezza informatica per tutti

GDPR

Introduzione

Sicuramente avrete sentito parlare di una nuova legge denominata GDPR, abbreviazione di General Data Protection Regulation. Questa legge è stata emanata dall'Unione Europea e andrà in vigore il 25 maggio 2018. E' rivolta a tutte le organizzazioni o enti che si occupano del trattamento dei dati personali dei cittadini residenti nell'Unione Europea (UE), indipendentemente da dove si trovi l'organizzazione nel mondo. Il GDPR obbliga le organizzazioni ad assicurare la privacy e la sicurezza delle informazioni personali di qualsiasi residente dell'UE. Affinchè si possa garantire la conformità con il GDPR, è importante comprenderne e implementarne i principi fondamentali.

Il diritto alla privacy è insindacabile. Le organizzazioni devono rispettare la privacy dei cittadini limitando i dati personali c1he raccolgono ed elaborano e salvaguardando tali dati. Gli obblighi di riservatezza si applicano a qualsiasi dato, che, da solo o utilizzato con altre informazioni, potrebbe portare ad identificare una persona che vive nell'Unione Europea. Queste informazioni potrebbero essere indirizzi, numeri di passaporto, numeri di patente di guida, dettagli finanziari, dati biometrici, appartenenza sindacale, anamnesi mediche, dati di posizione o informazioni relative all'orientamento sessuale, religioso o politico di una persona. Il regolamento si applica ad una "persona fisica", cioè ad un individuo vivente. Di seguito alcuni dei principali principi del GDPR che dovrebbero essere seguiti:

I dati personali per i singoli cittadini devono essere trattati in modo lecito, equo e trasparente.

Le persone devono essere informate su quali dati verrano raccolti e per quale scopo.

I dati personali devono essere raccolti per scopi specifici, espliciti e legittimi. Non devono essere utilizzati per altri scopi diversi da quelli elencati.

I dati personali saranno conservati e trattati solo e strettamente per il tempo necessario allo scopo comunicato.

I dati personali devono essere tenuti aggiornati e corretti.

Le persone hanno il diritto di ricevere una copia dei propri dati o possono richiedere che i propri dati personali non vengano più utilizzati o, in alcuni casi, cancellati interamente.

Le organizzazioni devono mettere in atto adeguate misure di sicurezza per proteggere i dati personali da eventuale distruzione, perdita, alterazione o divulgazioni accidentali o illecite.

Inoltre, le organizzazioni devono garantire che tutto il personale che gestisce i dati personali abbia una formazione adeguata su come mettere al sicuro e proteggere tali dati.

Le misure di protezione messe in atto per proteggere i dati personali devono garantire un livello di protezione adeguato alla sensibilità dei dati. Se il rischio associato ai dati aumenta, è necessario che anche lo sforzo e la spesa delle misure per proteggere tali dati crescano. Queste misure dovrebbero essere regolarmente riviste e aggiornate in base alle necessità. Dati ben documentati circa decisioni e misure adottate per la privacy e la sicurezza aiutano nel dimostrare la conformità ai requisiti imposti dal GDPR. In aggiunta, le organizzazioni sono legalmente obbligate ad adottare misure, come contratti e le verifiche di due diligence, per proteggere i dati personali quando vengono trasferiti a terzi o in particolare a soggetti al di fuori dell'Unione Europea. Infine, nel caso si verificasse una violazione dei dati personali, le organizzazioni dovranno segnalare la violazione entro 72 ore dopo esserne venuti a conoscenza. La mancata conformità delle organizzazioni al GDPR può portare a multe fino al 4% del loro fatturato globali, rendendo il GDPR una delle normative mondiali economicamente più costose al mondo.

Versione Italiana

Italtel è una società multinazionale che progetta e realizza soluzioni e servizi di Information & Communication Technology basati su prodotti propri e di partner. Offre un ricco catalogo di servizi professionali di ingegneria, di servizi gestiti e soluzioni di Cybersecurity, collaboration, IoT, digitalizzazione delle reti e servizi di comunicazione.
Per maggiori informazioni www.italtel.com e seguici su Twitter (@Italtel)

L'autore di questo numero

Brian Honan *è il CEO di BH Consulting, una società indipendente di consulenza per la sicurezza informatica e la protezione dei dati con sede a Dublino, in Irlanda. Brian ha lavorato come consulente speciale per il Cybercrime Centre di Europol (EC3), è il fondatore del primo CERT irlandese e fa parte del comitato consultivo di diverse compagnie innovative in ambito sicurezza. Puoi seguire Brian su* www.linkedin.com/in/brianhonan *o Twitter* @brianhonan.

Risorse

GDPR Overview For Individuals and Organizations: http://gdprandyou.ie

The GDPR Regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679

OUCH! Translations and Archives: https://www.sans.org/u/D88