mare consulting

I tuoi dati sensibili sono al sicuro?

mareconsulting.net
info@mareconsulting.net

Dicembre 2021

I tuoi dati sensibili sono al sicuro?

I **dati sensibili** sono per ogni azienda una **grande risorsa** che va custodita e protetta.
Tra essi si annoverano dati personali come e-**mail**, numeri di telefono, **indirizzi**, **dati bancari**, per citarne alcuni.

Gli **attacchi hacker** ai database delle aziende sono sempre più diffusi proprio per questa ragione. Ogni impresa, ora più che mai, ha la necessità e il dovere di **aumentare la sicurezza** per tenere i **dati sensibili dei propri clienti** al sicuro da possibili furti.

Cos'è il GDPR, General Data Protection Regulation?

Si tratta del **Regolamento europeo sulla protezione dei dati** che disciplina il modo in cui le aziende e le altre organizzazioni trattano i dati personali. È il provvedimento più significativo degli ultimi 20 anni in materia di **protezione dei dati** e ha implicazioni importanti per qualsiasi organizzazione al mondo che si rivolga ai **cittadini dell'Unione Europea**.

La legislazione ha lo scopo di dare a ogni persona il **controllo sull'utilizzo dei propri dati sensibili**, così da tutelare "i diritti e le libertà fondamentali delle persone fisiche". Per questa ragione il Regolamento GDPR stabilisce **requisiti precisi** e **rigorosi** per il trattamento dei dati, la trasparenza, la documentazione da produrre e conservare e il consenso degli utenti.

Il GDPR impone **l'obbligo di test di sicurezza con una cadenza di almeno 12 mesi** sui sistemi informativi che gestiscono i dati personali. Tale obbligo è assolto mediante l'**esecuzione di un VAPT**, Vulnerability Assessment and Penetration Test.

Sanzioni GDPR

La **mancata esecuzione del VAPT** annuale è soggetta, in caso di ispezione del garante, a infrazione civile e cioè a **multe salate** e in alcuni casi anche a **responsabilità penale**.

Il GDPR ha un grosso potere di esecuzione, arrivando a multe fino al 4% del fatturato globale annuo di un'azienda o a multe che ammontano a **20 milioni di euro**, questo dipende da quale dei due valori è il più alto, perché in alcuni casi la cifra può raggiungere cifre molto alte.

Tra le più elevate multe GDPR inflitte a partire dal maggio 2018, data di entrata in vigore del Regolamento, si segnalano:

50.000.000 € contro Google in Francia;

35.258.708 € contro H&M in Germania;

27.800.000 € contro TIM in Italia;

22.046.000 € contro British Airways nel Regno Unito.

Le ammende GDPR sono stabilite in tutta l'UE su base quasi giornaliera e la maggior parte delle multe non è rappresentata da ingenti somme a grandi aziende, ma da somme comprese tra i **4.000** e i **50.000** euro **nei confronti delle piccole imprese**, dei **comuni**, dei **negozi online** e altre realtà.

Trattare i dati personali in piena conformità con il GDPR è fondamentale, indipendentemente dalle dimensioni della propria azienda.

Che cos'è la certificazione ISO27001?

Si tratta di una certificazione che richiede l'**esecuzione ogni 6 mesi dei test di sicurezza**, mediante VAPT, Vulnerability Assessment e Penetration Test, sulla propria infrastruttura.

Senza VAPT non è possibile ottenere la certificazione e la si perde nel caso i test non vengano effettuati con la periodicità prevista.

Ottenere una certificazione accreditata ISO 27001 permette di dimostrare che la tua azienda sta **seguendo le best practice sulla sicurezza delle informazioni**. Inoltre, fornisce un **controllo indipendente e qualificato** in grado di attestare che la sicurezza delle informazioni è gestita in linea con le best practice internazionali e con gli obiettivi aziendali.

Report VAPT.

In entrambi i casi, sia di compliance normativa al GDPR che di certificazione alla ISO27001, l'esecuzione del VAPT è dimostrato mediante un executive summary e un allegato tecnico in cui sono descritte le vulnerabilità riscontrate e le soluzioni per risolverle.

Le attività di VAPT si dividono in due test che verificano la sicurezza informatica dell'azienda:

- il **Vulnerability Assessment:** un test di cyber security che serve all'azienda per scoprire quali sono i punti deboli del sistema informatico e dove intervenire per risolverli;

- un **Penetration Test**: un test di sicurezza informatica che serve a simulare un attacco informatico mirato e controllato al sistema informatico di un'azienda, utile per sapere come un hacker potrebbe attaccare il sistema informatico.

Contatta il nostro referente

Antonio Negro
Innovation Consultant
T. +39 081 8036677 | M. +39 344 0148164
antonio.negro@mareconsulting.net

Katya Capozzoli
Innovation Consultant
T. +39 081 8036677 | M. +39 348 8301387
katya.capozzoli@mareconsulting.net

Dove siamo
Via Ex Aeroporto s.n.c. c/o Consorzio Il Sole Lotto XI – 80038 Pomigliano d'Arco (NA)
Telefono: 081 803 6677, **Email:** info@mareconsulting.net,
Web: mareconsulting.net