

Vulnerability Assessment (GDPR Compliant)

Condurre una Vulnerability Assessment è una pratica fondamentale per documentare in maniera inequivocabile l'importanza che viene riconosciuta alla sicurezza e al mantenimento di adeguati livelli di protezione.

VULNERABILITY ASSESSMENT: cos'è

Il "GDPR" non cita esplicitamente nessun prodotto o servizio, come non elenca specifici requisiti di sicurezza, ma ribadisce in più punti la necessità di mettere in campo tutte quelle azioni volte a garantire la sicurezza che normalmente si considerano efficaci per essere in regola.

Benché alle aziende piaccia pochissimo l'incertezza, esse infatti preferirebbero una check-list da smarcare, il **Regolamento europeo** prescinde dal mercato e dalla tecnologia in voga al momento, e **stabilisce dei principi capaci di garantire la sicurezza dei dati in modo duraturo e continuativo senza apparire obsoleti.**

In quest'ottica, il Vulnerability Assessment risulta una componente fondamentale per dimostrare che le problematiche poste dal trattamento e dalla protezione dei dati sono state prese in giusta considerazione dall'azienda.

Il Vulnerability Assessment infatti è uno di quegli strumenti che l'azienda può utilizzare per mantenere in efficienza i sistemi che raccolgono, archiviano e gestiscono dati personali.

Così la volontà di mantenersi a norma con il GDPR spinge le aziende e le organizzazioni che trattano dati personali di cittadini europei a mettere in atto misure adeguate per garantirne la sicurezza e la riservatezza. Inoltre, il GDPR non abroga direttamente altre leggi o provvedimenti in materia di protezione dei dati, se non del tutto incompatibili, ma, in mancanza di appositi interventi legislativi, vi si aggiunge in parallelo.

Il GDPR ha le sue peculiarità, in particolare per quello che riguarda la reportistica e il Vulnerability Assessment è un valido punto di partenza per essere in regola con tutti i requisiti.



GDPR Compliance

Quali gli articoli del GDPR che coinvolgono il Vulnerability Assessment

GDPR

Vulnerability Assessment

Articolo 32 (pag. 51) Sicurezza del trattamento. “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:” b) la capacità di assicurare su base permanente la riservatezza, l’integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento”

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

Articolo 39 (pag. 56) – Compiti del responsabile della protezione dei dati – 1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti: ...b) sorvegliare l’osservanza del presente regolamento.

Articolo 57 (pag. 68) – Compiti [delle Autorità di controllo] – ... sul proprio territorio ogni autorità di controllo: ... h) svolge indagini sull’applicazione del presente regolamento...

Articolo 30 – Registri delle attività di trattamento – “Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la sua responsabilità”

Articolo 35 – Valutazione di impatto sulla protezione dei dati – “7. La valutazione contiene almeno: c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione”.



Usare il Vulnerability Assessment per preparare la GDPR Compliance

Preparandosi per essere conformi al GDPR e alle sue regole, le aziende e le organizzazioni devono osservare una serie di azioni minime di controllo per evitare sanzioni ma soprattutto per non perdere la fiducia dei loro clienti.

Il Vulnerability Assessment offre la possibilità di implementare alcune di queste azioni, quali:

- Uno sguardo all'ambiente IT per scoprire punti ciechi o zone in ombra su cui non si ha pieno controllo
- Continui aggiornamenti sia del controllo sulle vulnerabilità sia, e soprattutto, delle azioni di remediation
- L'individuazione delle priorità sugli asset a rischio
- Un affidabile supporto alla redazione della reportistica per la GDPR Compliance
- Integrazione con i sistemi di "security information and event management"

È evidente che per essere in regola con il GDPR ogni azienda debba avere per prima cosa una visione completa di tutti gli asset informatici che concorrono nelle attività di trattamento dei dati.

Visione tutt'altro che scontata nella realtà dei fatti, poiché nelle aziende di una certa dimensione esistono sempre numerosi punti ciechi o zone d'ombra difficili da individuare o a cui non si pensa.

Il Vulnerability Assessment ricerca in maniera obbiettiva le minacce e le vulnerabilità anche negli ambiti a cui non si pensa o in cui non si crede possano annidarsi problemi, per poi fornire tutti gli strumenti opportuni e necessari per ripristinare il corretto livello di sicurezza.

I 20 controlli critici per la sicurezza secondo il SANS Institute V6

CS1	Inventario dei dispositivi autorizzati e non autorizzati	SI	CS11	Configurazioni sicure per dispositivi di rete come firewall, router e switch	SI
CS2	Inventario del software autorizzato e non autorizzato	SI	CS12	Difesa dei confini	SI
CS3	Configurazione sicura di hardware e software su dispositivi mobili, laptop, workstation e server	SI	CS13	Protezione dei dati	SI
CS4	Valutazione e correzione continue delle vulnerabilità	SI	CS14	Accesso controllato basato sul principio del "need to know"	SI
CS5	Uso controllato dei privilegi amministrativi	SI	CS15	Controllo wireless degli accessi	SI
CS6	Manutenzione, monitoraggio e analisi dei registri di audit	SI	CS16	Monitoraggio e controllo degli account	SI
CS7	Protezioni per e-mail e browser web	SI	CS17	Valutazione delle competenze di sicurezza e appropriata formazione per colmare le lacune	SI
CS8	Difese contro il malware	SI	CS18	Sicurezza del software applicativo	SI
CS9	Limitazione e controllo di porte, protocolli e servizi di rete	SI	CS19	Risposta e gestione degli incidenti	SI
CS10	Capacità di recupero dati	SI	CS20	Test di penetrazione ed esercizi per il Team RED	SI

SEDE LEGALE

One Off Services S.C.P.A
Viale XXIV Maggio, N°5
34170 - Gorizia (GO)

SEDE OPERATIVA VENETO

Via XIII Martiri, N°88
Tel./Fax. +39 0421 - 223661
30027 - San Donà Di Piave (VE)
kibsstudio@kibsstudio.com

SEDE OPERATIVA EMILIA - ROMAGNA

Via Armando Gnani, N°54
Tel. +39 0544 502170
48124 - Ravenna (RA)