# COME OTTENERE LA CONFORMITÀ GDPR CON LA GESTIONE DELLE VULNERABILITÀ

Whitepaper F-Secure

F-Secure

# RIEPILOGO GENERALE

Dopo la scoperta di Spectre e Meltdown nel gennaio 2018, il responsabile della technology policy di ICO[1] ha avvertito che, ai sensi del regolamento generale UE sulla protezione dei dati (GDPR)[2], le società potrebbero essere punite per le vulnerabilità presenti nei loro protocolli di protezione dei dati.

Per essere conforme al GDPR UE, qualsiasi entità che acceda, controlli o elabori informazioni di identificazione personale (PII) di cittadini UE deve adottare misure sufficienti a garantire la sicurezza e la riservatezza dei dati. Questo comprende tra l'altro:

**GDPR ARTICOLO 32 (PAGINA 52): SICUREZZA DEL TRATTAMENTO**

"1. [...] dovranno mettere 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 (PAGINA 56): COMPITI DEL RESPONSABILE DELLA PROTEZIONE DEI DATI**

"Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti: [...] b) sorvegliare l'osservanza del presente regolamento."

"2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo."

Per ottenere il livello di protezione dei dati richiesto dal GDPR UE, le organizzazioni devono:

1. Valutare costantemente le vulnerabilità dei loro sistemi
2. Stabilire la priorità delle vulnerabilità in funzione del livello di rischio
3. Correggere e contenere le vulnerabilità in modo rapido ed efficace
4. Documentare tutte le misure adottate per correggere le vulnerabilità.

Mettendo in atto queste azioni, le organizzazioni saranno in grado di soddisfare i livelli di protezione dei dati richiesti dal GDPR. Mitigheranno inoltre il rischio e la severità delle penali imposte in caso di violazioni e potranno dimostrare davanti al tribunale UE di aver seguito la due diligence.

Utilizzare una soluzione di gestione delle vulnerabilità (VM - Vulnerability Management) è il modo più efficace per raggiungere il livello di protezione richiesto. Può aiutarti a individuare, valutare, definire le priorità, stilare dei report, correggere e porre rimedio alle vulnerabilità e alle configurazioni errate dei tuoi asset digitali. Questi asset possono comprendere processi aziendali, app web, sistemi di reti dati e i relativi software.

**Questo documento spiega in che modo una soluzione di gestione delle vulnerabilità può aiutare la tua organizzazione a ottenere il livello di protezione dei dati richiesto dal GDPR.**

# LA GESTIONE DELLE VULNERABILITÀ TI AIUTA A RISPETTARE IL GDPR

La scoperta di Spectre e Meltdown, nel gennaio del 2018, ha sconvolto il mondo dell'informatica. Dopo la pubblicazione di quel fatale rapporto del Project Zero di Google, si è fatto sentire il responsabile della technology policy di ICO, Nigel Houlden.

In un post pubblicato sul sito ICO[1], Houlden ha avvertito che, ai sensi del regolamento generale UE sulla protezione dei dati (GDPR)[2], le società potrebbero essere punite per le vulnerabilità presenti nei loro protocolli di protezione dei dati.

Ha affermato: "Possono esserci circostanze in cui le società potrebbero essere ritenute responsabili di una violazione di sicurezza a causa di misure, come le patch, che avrebbero dovuto essere adottate prima."

Questa dichiarazione sottolinea l'importanza di sistemi di gestione efficaci delle vulnerabilità e della sicurezza delle informazioni, in particolare relativamente alle violazioni di dati.

Houlden ha dichiarato inoltre: "La mancata correzione di vulnerabilità note è un fattore che ICO prende in considerazione per determinare se una violazione del settimo principio dell'Atto sulla Protezione dei Dati è sufficientemente seria da giustificare una sanzione pecuniaria civile."

Il GDPR conferisce alle autorità il potere di comminare multe elevate alle organizzazioni che non hanno adottato le misure necessarie a proteggere le loro informazioni. Per infrazioni gravi, la multa può arrivare fino a un massimo di 20 milioni di euro o al 4% del fatturato annuo globale se superiore. Le carenze nella cyber security sono tuttavia in genere punite con multe del livello inferiore: fino a 10 milioni di euro o al 2% del fatturato annuo globale. Nel 2018, a Carphone Warehouse è stata comminata una multa di £400.000[3] per una violazione che ha messo a rischio i dati personali di oltre 3 milioni di persone.

"Possono esserci circostanze in cui le società potrebbero essere ritenute responsabili di una violazione di sicurezza a causa di misure, come le patch, che avrebbero dovuto essere adottate prima."

ICO. (2018). Meltdown and Spectre – cosa dovrebbero fare le organizzazioni per proteggere i dati personali?

Sebbene sia probabile che l'ICO utilizzi le multe come ultima risorsa, qualsiasi azione disciplinare può risultare molto onerosa. Queste azioni possono comprendere indagini sulle prassi di sicurezza dei dati della società non conforme, seguite dall'ordine di correggere tutti gli elementi che non soddisfano i requisiti del GDPR.

In un mondo post GDPR, una gestione delle vulnerabilità insufficiente diventa un rischio aziendale diretto. Tuttavia, cercare di risolvere allo stesso tempo centinaia di singoli problemi di sicurezza dei dati non è una strategia efficace.

**RIEPILOGO DEL GDPR**

Il 25 maggio 2018 è entrato in vigore il GDPR, ovvero il regolamento generale UE sulla protezione dei dati che prevede che tutte le società che controllano o elaborano informazioni di identificazione personale (PII) di cittadini UE debbano adottare misure sufficienti a garantire la riservatezza e sicurezza dei dati loro affidati.

Il GDPR, che si affianca a HIPAA e SOX, è la prima norma sulla conformità della protezione dati a comminare sanzioni economiche alle società che perdono o non gestiscono in modo adeguato i dati dei propri clienti. Il GDPR contiene degli elementi che ampliano l'ambito della due diligence nelle prassi di sicurezza dei dati, in particolare in aree quali i requisiti di documentazione.

Le multe del GDPR sono suddivise in due livelli e si applicano a qualsiasi organizzazione che gestisca dati di cittadini UE. Il livello di multe superiore si applica a infrazioni gravi e può arrivare fino a 20 milioni di euro o al 4% del fatturato globale annuo. Il livello di multe inferiore riguarda violazioni di minore importanza e arriva fino a 10 milioni di euro l'anno o al 2% del fatturato globale annuo.Qualora una società violi più norme del GDPR, la multa sarà calcolata in base all'infrazione più grave.

Queste multe sono più pesanti e vengono assegnate con maggiore probabilità rispetto a qualsiasi altra norma esistente. Vengono calcolate in funzione di tre fattori principali:

1. Quanti dati personali di cittadini UE sono stati gestiti male o persi
2. Quali misure sono state adottate prima dell'incidente per evitare la perdita
3. Quali misure sono state adottate dopo la perdita

Il GDPR avrà un impatto ridotto o irrilevante su un'azienda che:

- Non gestisce o gestisce un numero limitato di dati di cittadini UE
- Implementa protocolli di sicurezza adeguati, ben documentati e puntualmente aggiornati
- Rispetta gli ordini del GDPR dopo la scoperta della violazione

**Le società devono stabilire delle priorità e correggere le vulnerabilità in ordine di gravità ed estensione invece di adottare interventi di massa.**

# LA GESTIONE DELLE VULNERABILITÀ RIDUCE I COSTI DELLA VIOLAZIONE DEI DATI

Lo studio Cost of a Data Breach 2018 di Ponemon[4], che ha coinvolto oltre 2200 professionisti IT e di sicurezza di 477 aziende, ha determinato che il costo medio di una violazione dei dati si aggira intorno ai 125€ per record cliente globalmente o oltre 176€ per record negli Stati Uniti.

Sono molti i fattori che influiscono sul costo di una violazione dei dati, come ad esempio:

- La perdita inaspettata di clienti a seguito di una violazione dei dati
- Le dimensioni della violazione e il numero di record persi o rubati
- Il tempo necessario a individuare e contenere la violazione dei dati
- I costi di una gestione efficace di rilevazione ed escalation
- I costi di una gestione efficace della violazione dei dati

**VALUTAZIONE DEI COSTI DELLA VIOLAZIONE DEI DATI**

Il GDPR non specifica un metodo di calcolo diretto per le sanzioni. Il costo reale di una violazione dipende da numerose variabili, che non possono essere determinate con precisione prima di un incidente.

Il Ponemon Institute fornisce i migliori dati disponibili per la valutazione del costo reale di una violazione nel suo studio annuale "Cost of a Data Breach"[4].

Questo studio rappresenta una preziosa risorsa per chiunque sia responsabile di protezione dati, sicurezza IT e/o conformità.

È consigliabile, se non necessario, leggerlo per la due diligence generale per la protezione dei dati.

Complessivamente, i costi delle misure proattive per la protezione dalle violazioni, come rilevazione, escalation, notifica e risposta possono essere eclissati dall'impatto della violazione. Non solo si rischia la perdita di business causata dal tempo di inattività del sistema, ma anche la defezione dei clienti e una significativa interruzione delle attività. In generale, il modo migliore per ridurre i costi legati alle violazioni dei dati consiste nell'individuarle e contenerle rapidamente.

Il GDPR prevede per le organizzazioni globali che controllano o elaborano dati di identificazione personale (PII) dei cittadini UE delle multe calcolate in base ai seguenti criteri:

- Quanti dati personali di cittadini UE sono stati gestiti non correttamente o persi?
- Quali misure sono state adottate prima dell'incidente per evitare la perdita?
- Quali misure sono state adottate dopo la perdita?

Sebbene l'ICO non abbia indicato alcun metodo di calcolo diretto, le società che applicano la due diligence possono drasticamente ridurre l'importo delle multe. In sostanza, occorre che la società dimostri davanti al tribunale UE di aver protetto i dati del cliente oltre ogni "ragionevole misura".

La gestione delle vulnerabilità è considerata dai professionisti di security e dalle entità legiferanti, inclusa l'ICO, una misura di protezione dei dati essenziale. In assenza di questa non si può affermare di aver soddisfatto, per non dire superato, queste ragionevoli misure di protezione dati.

In sostanza, senza la gestione delle vulnerabilità, sarà difficile convincere un tribunale UE di aver adottato tutte le misure idonee ad evitare una violazione dei dati.

**In assenza di una gestione delle vulnerabilità (VM - Vulnerability Management) efficace si rischiano le sanzioni più severe ai sensi del GDPR.**

# LA GESTIONE DELLE VULNERABILITÀ MITIGA I RISCHI DI VIOLAZIONE DEI DATI

Quando viene scoperta e resa pubblica una vulnerabilità nella sicurezza dei dati, si scatena una corsa tra chi deve correggerla e chi vuole sfruttarla. E molto spesso sono gli hacker che cercano di sfruttare le falle di sicurezza a vincerla. Se un hacker riesce a sferrare il suo attacco prima che venga implementata la patch, la probabilità che i dati vengano violati è molto alta. Secondo lo studio di Ponemon Cost of a Data Breach[4] del 2018:

Il 57% degli intervistati che hanno riferito di una violazione ha affermato che era stata causata da una vulnerabilità nota che avrebbe potuto essere corretta.

Fonte: 2018 Cost of a Data Breach - Ponemon

- Il 57% degli intervistati che hanno riferito di una violazione ha affermato che era stata causata da una vulnerabilità nota che avrebbe potuto essere corretta
- Il 34% degli intervistati ha affermato che sapeva di essere vulnerabile prima che si verificasse la violazione
- Il 56% delle società che non avevano eseguito la scansione delle vulnerabilità ha subito una violazione

Un numero considerevole di organizzazioni che trattano informazioni di identificazione personale (PII) non esegue la scansione delle vulnerabilità, lasciando libero accesso ai sistemi vitali non controllati e alle vulnerabilità non individuate. E se sono consapevoli di problemi di sicurezza, non dispongono di un sistema adeguato per risolverli in ordine di priorità.

La scansione delle vulnerabilità è un modo semplice ed efficace per aumentare le probabilità di evitare una violazione, può infatti ridurre subito il rischio del 20% prima ancora di iniziare ad applicare le patch o ad adottare altre misure di sicurezza.

Lo studio Cost of a Data Breach[4] 2018 di Ponemon ha individuato due capacità chiave nelle società che hanno evitato violazioni dei dati. Le loro prestazioni medie erano superiori relativamente a:

- La capacità di rilevare rapidamente le vulnerabilità (superiore del 19%)
- La capacità di correggere tempestivamente le vulnerabilità (superiore del 41%)

Queste società hanno evitato le violazioni, e le conseguenti infrazioni al GDPR, utilizzando prassi di gestione delle vulnerabilità efficaci. In generale, la rilevazione e la correzione delle vulnerabilità si sono sempre dimostrate fattori chiave per le organizzazioni che hanno evitato le violazioni.

Dopo essere state mappate, le vulnerabilità devono essere corrette tempestivamente e in base alla priorità. Questo può essere un compito arduo vista la lunga lista di vulnerabilità accertate dalla maggior parte delle organizzazioni.

Il report State of Vulnerability Response 2018 di Ponemon[5] rivela che il 65% dei professionisti di cyber security trova difficile stabilire la priorità delle correzioni. Una vulnerabilità critica sul laptop di un addetto al marketing ad esempio non dovrebbe avere una priorità maggiore rispetto a una vulnerabilità media su un server che contiene dati PII.

Per poter definire con precisione le priorità, occorre valutare il rischio aziendale reale costituito da una vulnerabilità. Definire la priorità delle attività di mitigazione dei rischi mediante il CVSS (Common Vulnerability Scoring System)[6] è un inizio, ma da solo non è sufficiente. Dovrebbe piuttosto essere un componente di una strategia di valutazione dei rischi articolata.

Sfortunatamente per molte organizzazioni, le informazioni necessarie a stabilire una priorità basata sui rischi sono dislocate in molti punti diversi dei reparti IT, protezione dati e conformità. Questo rende l'intero processo estremamente difficile, specie se eseguito senza uno strumento appositamente studiato.

L'articolo 32 del GDPR stabilisce: "...dovranno mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso."

Morale della favola? Se un'organizzazione non riesce a identificare e correggere le vulnerabilità in modo rapido ed efficace, ha sempre più probabilità di essere vittima di una violazione. Non sorprende quindi che l'ICO abbia sottolineato l'importanza della gestione delle vulnerabilità per soddisfare i livelli di sicurezza imposti dal GDPR.

**CASO DI STUDIO: LA TEMPESTIVITÀ È ESSENZIALE NELLA PREVENZIONE DELLA VIOLAZIONE DEI DATI**

L'attacco del ransomware WannaCry che ha paralizzato le reti dati di tutto il mondo è un esempio da manuale del perché la tempestività sia così essenziale per gestire le vulnerabilità critiche. Nel maggio del 2017, WannaCry si è diffuso utilizzando un exploit per una vulnerabilità di Windows (MS17-010) chiamato EternalBlue. Microsoft aveva individuato e corretto con una patch l'MS17-010 nel marzo di quell'anno e l'aveva segnata come vulnerabilità "critica" a causa dell'elevata possibilità per gli hacker di eseguire il codice da remoto nei sistemi colpiti.

Se i responsabili della protezione dei dati delle organizzazioni internazionali avessero individuato, dato priorità e corretto questa vulnerabilità immediatamente, o anche un mese dopo che la patch era stata resa disponibile, WannaCry avrebbe potuto essere evitato.

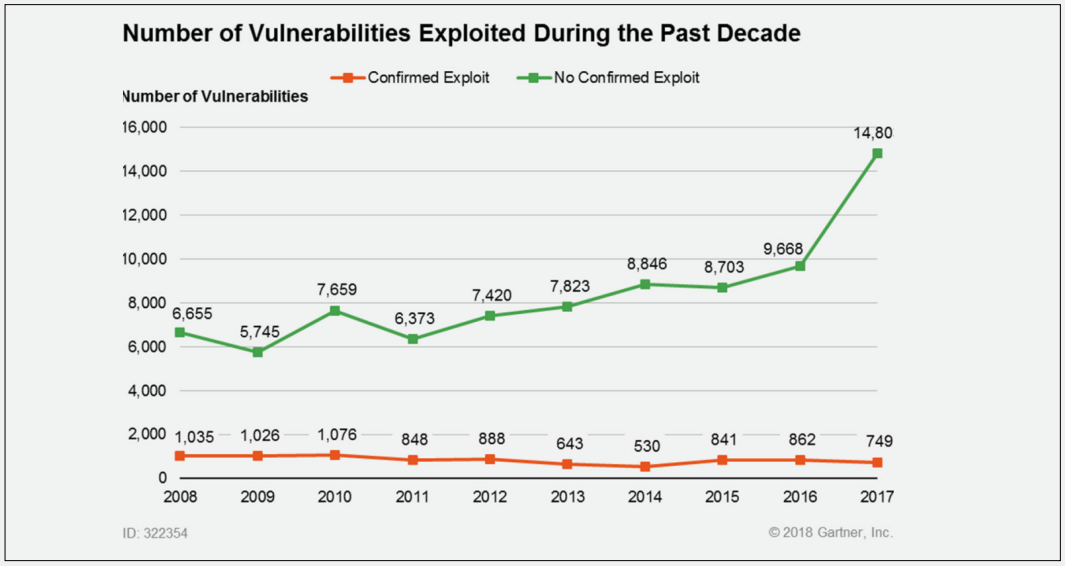
Nel 2017 WannaCry ha infettato centinaia di migliaia di computer in tutto il mondo, con conseguenze devastanti per società di telecomunicazione, agenzie governative, istituti finanziari, servizi pubblici, ospedali, impianti di produzione e gestori dei trasporti. Si stima che abbia causato in totale perdite per circa 4 miliardi di dollari, oltre ad aver messo a rischio innumerevoli vite umane.

WannaCry e il caos che ha causato sono stati ampiamente coperti dai media di tutto il mondo eppure, quattro mesi dopo la sua scoperta e la successiva emissione della patch, i ricercatori hanno trovato oltre 50.000 macchine su cui la patch non era stata installata e che erano a rischio a causa di EternalBlue.

Questo è solo un esempio tra tanti che dimostra quanto sia importante una efficace gestione delle vulnerabilità per un'adeguata sicurezza delle informazioni.

## ASSEGNAZIONE DELLE PRIORITÀ ALLE VULNERABILITÀ

Source: IBM X-Force/Analysis Gartner (giugno 2018)




Un rapporto di Gartner del 2018 mostra che "nonostante le oltre 92.000 vulnerabilità scoperte pubblicamente nello scorso decennio, solo circa 8500 (quindi circa un ottavo) sono state sfruttate 'allo stato naturale'."

Gartner prosegue affermando: "Tuttavia sono state ampiamente utilizzate e riutilizzate da un gran numero di famiglie di malware." Gartner afferma inoltre "Sebbene non tutti i malware abbiano bisogno della presenza di una vulnerabilità, la maggior parte di essi oggi opera in questo modo."

Gartner, Market Guide for Vulnerability Assessment, Craig Lawson and Prateek Bhajanka, 19 giugno 2018.

Gartner non promuove alcun vendor, prodotto o servizio raffigurato nelle proprie pubblicazioni di ricerca, e non suggerisce agli utenti della tecnologia di optare soltanto per quei vendor che possiedono la classificazione più alta o altre valutazioni. Le pubblicazioni di ricerca di Gartner comprendono le opinioni delle organizzazioni di ricerca di Gartner e non dovrebbero essere interpretate come dati di fatto. Gartner disconosce tutte le garanzie, espresse o implicite, rispetto a questa ricerca, inclusa ogni garanzia di commerciabilità o di idoneità per un determinato obiettivo.

**Il software di gestione delle vulnerabilità è fondamentale per una efficace classificazione delle priorità dei rischi nei sistemi che contengono o elaborano informazioni di identificazione personale dei cittadini UE.**

# IN CHE MODO F-SECURE RADAR TI AIUTA A SODDISFARE I REQUISITI GDPR

Considerato l'approccio alla sicurezza basato sui rischi di F-Secure, possiamo dire, senza rischio di smentita, di avere una soluzione per i tuoi problemi relativi alla conformità, in particolare quando si stratta della gestione delle vulnerabilità all'interno di sistemi che contengono, trattano o trasferiscono dati PII. F-Secure Radar, il nostro strumento per la gestione delle vulnerabilità, è appositamente progettato per aiutarti a mappare la tua superficie di attacco e impedire violazioni dei dati.

La sicurezza è tuttavia solo un aspetto della conformità GDPR. Ci rendiamo conto che per soddisfare tutti i requisiti del GDPR, oltre a eseguire molteplici valutazioni ed esami dei processi, devi ricorrere a più vendor. Se non l'hai ancora fatto, è bene che tu ti rivolga a un partner per la sicurezza di indubbie capacità.

Non fraintendere — non abbiamo una formula magica — ma comprendiamo le complessità della conformità GDPR. E, cosa più importante, possiamo aiutarti a districarti tra di esse in modo efficace ed efficiente.

Ecco in che modo F-Secure Radar ti aiuterà a soddisfare i requisiti GDPR:

| **GDPR 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 propria responsabilità. Tale registro contiene tutte le seguenti informazioni: [...],<br><br>(g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1. | F-Secure Radar è appositamente concepito per assicurare la gestione delle vulnerabilità mediante un metodo di delivery continua basata su processo.<br><br>I contributi comprendono informazioni sul processo generale di gestione delle vulnerabilità, strumenti e attività di remediation pianificate oltre alla documentazione delle misure correttive adottate. |

| GDPR ARTICOLO 32: SICUREZZA DEL TRATTAMENTO | |
|---|---|
| "1. [...] dovranno mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: [...], | La gestione delle vulnerabilità offerta da F-Secure Radar misura e quantifica il rischio per sistemi che contengono, elaborano o trasferiscono dati PII, in modo che possano essere tempestivamente adottate le idonee misure correttive.<br><br>Alla luce del ruolo chiave della gestione delle vulnerabilità nella sicurezza IT e della dichiarazione dell'ICO sulla sua importanza, questa dovrebbe essere considerata uno dei componenti tecnici 'minimi' per ottenere un adeguato livello di sicurezza.<br><br>Il metodo di delivery continua basata su processo di F-Secure Radar è una base preziosa per le misure di sicurezza organizzative, così come l'implementazione di un idoneo processo di gestione delle vulnerabilità. |
| "1. [...] dovranno mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: [...],<br><br>(b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; [...] | F-Secure Radar è appositamente progettato per offrire una valutazione continua delle vulnerabilità che è essenziale per assicurare riservatezza, integrità, disponibilità e resilienza dei servizi e sistemi di trattamento dati.<br><br>I contributi comprendono valutazioni continue delle vulnerabilità stesse, rischi ai dati PII individuati, definizione delle priorità delle azioni per correggere o mitigare i rischi, storico sulla riservatezza, integrità e resilienza dei sistemi e documentazione delle azioni correttive adottate. |
| (d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. | F-Secure Radar è appositamente progettato per eseguire la gestione delle vulnerabilità secondo una modalità continua basata su processo.<br><br>È essenziale per realizzare un processo di controllo, valutazione e verifica dell'efficacia delle misure tecniche e organizzative adottate per migliorare la sicurezza.<br><br>I contributi comprendono un processo continuo di correzione delle vulnerabilità, la risoluzione degli errori di configurazione e il rinnovo dei certificati scaduti.<br><br>F-Secure Radar fornisce inoltre report sullo storico e le modifiche a livello di riservatezza, integrità e resilienza dei sistemi e la documentazione delle azioni correttive adottate. |

| GDPR ARTICOLO 35: VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI | |
|---|---|
| "2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno." | I report di valutazione delle vulnerabilità forniti da F-Secure Radar possono essere trasmessi ai DPO (Data Protection Officer) insieme ad altri documenti, in modo che questi possano fornire una consulenza corretta nel corso della valutazione d'impatto sulla protezione dati.<br><br>I report forniranno tra l'altro ai DPO:<br><br>1. Una migliore comprensione dell'efficacia delle misure tecniche e organizzative adottate per garantire la sicurezza.<br>2. Documentazione e base logica per valutare efficacemente il rischio attuale nei sistemi con dati PII.<br>3. Storico e modifiche nella riservatezza, integrità e resilienza dei sistemi.<br>4. Documentazione sulle misure correttive adottate. |
| "7. La valutazione contiene almeno:<br><br>c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e<br><br>(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, [...]". | I report forniti da F-Secure Radar possono essere utilizzati per contribuire alla preparazione delle valutazioni d'impatto sulla protezione dei dati.<br><br>I contributi comprendono:<br><br>1. La capacità di misurare e quantificare il rischio per sistemi che contengono, elaborano o trasferiscono dati PII, in modo che possano essere tempestivamente adottate le idonee misure correttive.<br>2. La capacità di dimostrare che è stato adottato un processo per testare, valutare e verificare regolarmente l'efficacia delle misure tecniche e organizzative.<br>3. La capacità di dimostrare che sono state adottate idonee misure di sicurezza tecniche e organizzative per la protezione del sistema, ad esempio contro vulnerabilità, errori di configurazione e certificati scaduti.<br>4. La capacità di mostrare lo stato corrente del piano di azione per la correzione e la mitigazione dei rischi e la documentazione sulle azioni correttive attuate in precedenza. |

| GDPR ARTICOLO 39: COMPITI DEL RESPONSABILE DELLA PROTEZIONE DEI DATI | |
|---|---|
| "Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti: [...]<br><br>b) sorvegliare l'osservanza del presente regolamento." | I report forniti da F-Secure Radar consentono ai DPO (Data Protection Officer) di monitorare la conformità con i requisiti GDPR.<br><br>I contributi comprendono:<br><br>1. La capacità di misurare e quantificare il rischio per sistemi che contengono, elaborano o trasferiscono dati PII, in modo che possano essere tempestivamente adottate le idonee misure correttive.<br>2. La capacità di dimostrare che è stato adottato un processo per testare, valutare e verificare regolarmente l'efficacia delle misure tecniche e organizzative.<br>3. La capacità di dimostrare che sono state adottate idonee misure di sicurezza tecniche e organizzative per la protezione del sistema, ad esempio contro vulnerabilità, errori di configurazione e certificati scaduti.<br>4. La capacità di mostrare lo stato corrente del piano di azione per la correzione e la mitigazione dei rischi e la documentazione sulle azioni correttive attuate in precedenza. |
| "2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo." | I report forniti da F-Secure Radar forniscono ai DPO (Data Protection Officer) la documentazione e la base logica per valutare efficacemente i rischi, l'efficacia delle misure di sicurezza correnti e i processi di monitoraggio al fine di:<br><br>1. Individuare lacune che potrebbero dover essere colmate in prospettiva GDPR.<br>2. Modificare le priorità nelle misure o processi di sicurezza per meglio garantire il livello di sicurezza adeguato richiesto dal GDPR. |

| GDPR ARTICOLO 57: COMPITI DELL'AUTORITÀ DI CONTROLLO | |
|---|---|
| [...]sul proprio territorio ogni autorità di controllo: [...] h) svolge indagini sull'applicazione del presente regolamento | Nel caso in cui l'autorità di controllo svolga un'indagine dovuta ad una violazione dei dati o a una sospetta non conformità, i report forniti da F-Secure Radar consentono ai DPO (Data Protection Officer) di fornire documentazione su:<br><br>1. La capacità di misurare e quantificare il rischio per sistemi che contengono, elaborano o trasferiscono dati PII, in modo che possano essere tempestivamente adottate le idonee misure correttive.<br>2. La capacità di dimostrare che è stato adottato un processo per testare, valutare e verificare regolarmente l'efficacia delle misure tecniche e organizzative.<br>3. La capacità di dimostrare che sono state adottate idonee misure di sicurezza tecniche e organizzative per la protezione del sistema, ad esempio contro vulnerabilità, errori di configurazione e certificati scaduti.<br>4. La capacità di mostrare lo stato corrente del piano di azione per la correzione e la mitigazione dei rischi e la documentazione sulle azioni correttive attuate in precedenza.<br><br>Fornisce anche log dettagliati per future indagini. |

## NOTE

1 ICO. (2018). Meltdown and Spectre – what should organisations be doing to protect people's personal data?

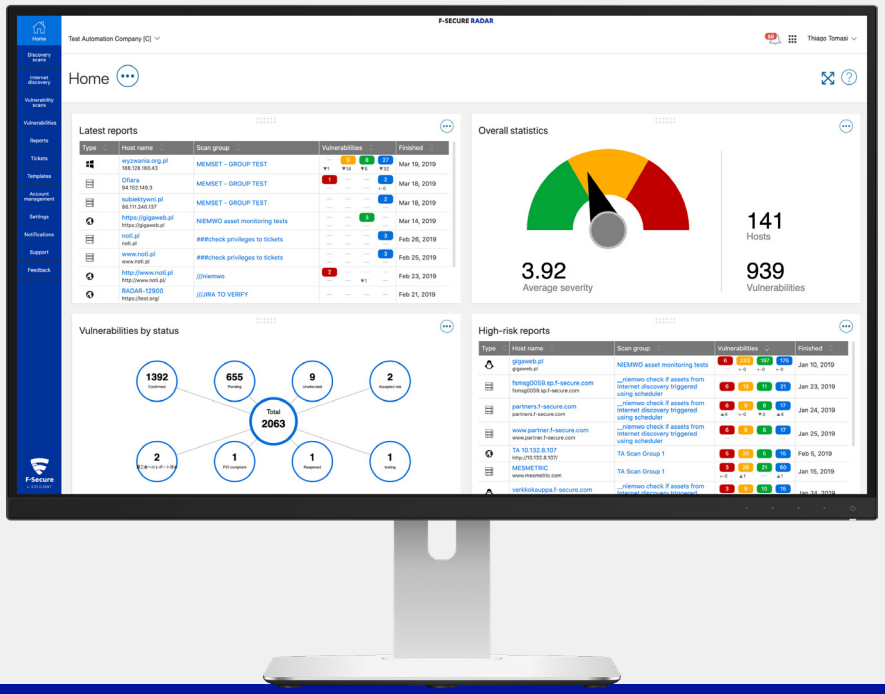
2 F-Secure. (2018). GDPR Playbook.

3 ICO. (2018). Carphone Warehouse fined £400,000 after serious failures placed customer and employee data at risk.

4 Ponemon. (2018). Cost of a Data Breach Study.

5 Ponemon. (2018). Today's State of Vulnerability Response: Patch Work Demands Attention.

6 NIST. (2018). Vulnerability Metrics.




# F-SECURE RADAR

Piattaforma chiavi in mano per la gestione e la scansione delle vulnerabilità. Controlla lo stato della tua conformità GDPR e individua le aree che richiedono miglioramenti.

Scopri altri dettagli e prenota una dimostrazione gratuita dal nostro sito
**f-secure.com/radar**

Nessuno può vantare una visibilità sui cyber attacchi reali maggiore di F-Secure. Stiamo colmando il divario tra rilevamento e risposta, sfruttando l'impareggiabile threat intelligence di centinaia dei migliori consulenti tecnici del settore, milioni di dispositivi che eseguono il nostro pluripremiato software e innovazioni incessanti nell'intelligenza artificiale. Le maggiori banche, compagnie aeree e imprese si affidano a noi per il nostro impegno volto a sconfiggere le minacce più potenti del mondo.

Insieme alla nostra rete costituita dai più importanti partner di canale e da oltre 200 service provider, il nostro obiettivo è fare in modo che ognuno disponga della cyber security di livello enterprise di cui tutti noi abbiamo bisogno. Fondata nel 1988, F-Secure è quotata sul listino NASDAQ OMX Helsinki Ltd.

**f-secure.com | twitter.com/fsecure_it | linkedin.com/ f-secure**

F-Secure