PREPARAZIONE AL GENERAL DATA PROTECTION REGULATION (GDPR)

WHITE PAPER

SOMMARIO

PREPARAZIONE AL GENERAL DATA PROTECTION REGULATION (GDPR)

INTRODUZIONE

CHE COS'È IL GDPR?

La continua digitalizzazione e globalizzazione della nostra economia fa sempre più affidamento sul controllo e l'elaborazione dei dati personali. Da una parte ciò offre enormi opportunità di business, dall'altra si accompagna a una crescente sensibilizzazione e preoccupazione pubblica relativamente all'importanza della protezione dei dati personali.

Un recente sondaggio condotto da KPMG International su scala mondiale ha rivelato che più della metà (il 55%) dei consumatori ha affermato di aver abbandonato gli acquisti online a causa di preoccupazioni sulla privacy. Il sondaggio indica anche che meno del 10% degli intervistati ritiene attualmente di avere il controllo sul modo in cui le organizzazioni gestiscono e utilizzano i loro dati personali.

Il General Data Protection Regulation (GDPR) dell'Unione Europea nasce in risposta a queste preoccupazioni. Riconoscendo il valore di tali dati, il regolamento impone un costo sulla loro raccolta, conservazione e utilizzo, attribuendo alle organizzazioni la responsabilità della loro protezione e obbligandole a restituirne il controllo e la proprietà alle persone.

A differenza della direttiva esistente sulla protezione dei dati, la 95/46/CE, che è stata recepita nelle singole legislazioni nazionali, GDPR è una disposizione unitaria mirante a rafforzare, unificare e applicare la protezione dei dati personali nell'intera UE. I suoi criteri più rigorosi, obblighi aggiuntivi e sanzioni per mancata conformità più elevate (il valore più grande tra il 4% del fatturato mondiale e 20 milioni di euro) faranno indubbiamente aumentare sia l'impegno richiesto per il raggiungimento della conformità, sia i rischi associati alla mancata conformità. L'aspetto positivo è che si tratta, in gran parte[1], di un'azione unificata tesa a definire le responsabilità delle organizzazioni in merito alla protezione dei dati in tutti gli Stati membri dell'Unione.

[1] I legislatori hanno concesso ai governi locali la possibilità di aggiungere o adattare disposizioni per rispondere a esigenze locali di protezione dei dati.

Il **General Data Protection Regulation (GDPR)** è la risposta dell'Unione Europea al ruolo enormemente esteso che la tecnologia riveste attualmente nella vita di tutti i giorni. Il GDPR è stato ratificato dagli stati membri nell'aprile del 2016 ed **entrerà in vigore il 25 maggio 2018.** Pur essendo un regolamento UE, si applica a qualsiasi organizzazione che raccolga dati personali di residenti dell'UE, indipendentemente dalla sua ubicazione fisica.

Obiettivo del nuovo regolamento è **garantire che nel processo di raccolta di dati personali sia integrata un'adeguata protezione dei dati "per impostazione predefinita fin dalla progettazione".** Ciò ha inizio con una raccolta limitata ai dati minimi necessari per una finalità specifica e con la cancellazione dei dati quando non sono più necessari. Un altro importante aspetto del GDPR è che l'interessato, la fonte dei dati personali, è il proprietario di tali dati. In qualità di proprietario, l'interessato deve avere la possibilità di revocare il proprio consenso alla raccolta dei dati con la stessa facilità con la quale ha concesso l'autorizzazione. L'interessato ha inoltre il "diritto all'oblio" e ad acquisire i propri dati personali.

Il GDPR definisce poi le condizioni che richiedono l'invio di una notifica in caso di violazione dei dati e prevede due livelli di sanzioni a seconda della gravità della violazione.

In considerazione dei rapidi cambiamenti tecnologici, il GDPR attribuisce inoltre l'onere di una "valutazione continuativa dei rischi" all'organizzazione che raccoglie i dati (il titolare del trattamento) e richiede la conformità al regolamento di qualsiasi organizzazione esterna che tratti i dati (responsabile del trattamento).

CHI È INTERESSATO?

Il GDPR si applica a qualsiasi organizzazione, in qualsiasi paese, che raccoglie, conserva o tratta i dati personali di residenti dell'Unione europea. Questi dati possono provenire da dipendenti, business partner, clienti attuali e potenziali. Nella terminologia del regolamento, tali organizzazioni sono dette "titolari del trattamento", che determinano come e perché sono trattati i dati personali, o "responsabili del trattamento", che agiscono per conto dei titolari. Per entrambi il GDPR stabilisce maggiori obblighi e prevede sanzioni in caso di violazione.

QUALI SONO LE IMPLICAZIONI PER LE IMPRESE GLOBALI?

Per la maggior parte delle imprese, le implicazioni sono rilevanti e di ampia portata, con la necessità di cambiamenti che coinvolgono i flussi di elaborazione dei dati, la struttura organizzativa, i processi aziendali, fino alle tecnologie informatiche e di sicurezza.

DIRITTI DELLE PERSONE

L'essenza del GDPR è la definizione dei diritti delle persone in relazione alla protezione dei dati. Tali diritti possono essere sintetizzati in grandi linee come segue:

- **Consenso informato**
  Il diritto di essere chiaramente informato sui motivi che richiedono la comunicazione dei dati e sulle modalità del loro utilizzo. Il consenso deve essere accordato in modo esplicito e può essere ritirato in qualsiasi momento.
- **Accesso**
  Il diritto di accedere gratuitamente a tutti i dati raccolti e di ottenere conferma delle modalità del loro trattamento.
- **Correzione**
  Il diritto di correggere i dati se inaccurati.
- **Cancellazione e "diritto all'oblio"**
  Il diritto di richiedere la cancellazione dei propri dati.
- **Portabilità dei dati**
  Il diritto di recuperare e riutilizzare i dati personali, ai propri scopi, tra diversi servizi.

La prima sfida da affrontare per la conformità al GDPR è quindi quella di controllare e, se necessario, modificare il modo in cui l'organizzazione raccoglie, conserva e tratta i dati personali in base a questi diritti. Parte impegnativa di tale sfida sarà già solo il raggiungimento di un punto in cui l'organizzazione sia in grado di individuare con precisione tutte le istanze dei dati di una persona nell'intera infrastruttura (ossia il problema del "Dove sono i miei dati?").

Per alcune organizzazioni, ciò offrirà l'opportunità di ottimizzare le operazioni, eliminare raccolte di dati non necessari e limitare il trattamento ai soli dati essenziali per gli obiettivi fondamentali dell'impresa. In ogni caso, la transizione alla conformità sarà probabilmente un impegno significativo.

RESPONSABILIZZAZIONE E GOVERNANCE

L'organizzazione deve quindi essere in grado di dimostrare la conformità tramite opportune misure di governance, che includano documentazione dettagliata, registrazione e valutazione continua del rischio. A questo proposito vi è un'aspettativa aggiuntiva di "protezione dei dati fin dalla progettazione e protezione per impostazione predefinita": la sicurezza deve cioè, nella misura maggiore possibile, essere parte integrante di tutti i sistemi sin dall'inizio, piuttosto che qualcosa applicata a posteriori, anche se questo chiaramente presenta una sfida enorme dove sono coinvolti sistemi legacy. Casi del genere rendono evidente il ruolo essenziale, come primo livello di difesa, della sicurezza a livello di rete, che può rappresentare l'unica difesa dalla violazione dei dati per l'enorme numero di sistemi legacy ancora in uso, finché questi non potranno essere riprogettati con misure intrinseche di protezione dei dati.

A causa del rapido ritmo dei cambiamenti tecnologici, che vediamo ad esempio nell'ambito di Internet, dei dispositivi mobili, delle applicazioni e dell'economia digitale, e della conseguente evoluzione delle minacce informatiche che continueranno a sfruttare tali cambiamenti, il regolamento è necessariamente vago riguardo agli specifici interventi tecnologici da attuare per conformarsi a questi criteri. Oltre alle precauzioni più ovvie quali la cifratura dei dati, la pseudonimizzazione[2] e così via, il GDPR usa termini quali "adeguato" e "stato dell'arte" per descrivere il requisito di una continua valutazione del rischio e dell'aggiornamento delle misure di conformità. Con la scoperta di nuove vulnerabilità, per rimanere conformi in futuro può essere necessario cambiare la tecnologia della sicurezza o le pratiche di protezione dei dati considerate oggi conformi. Se da una parte ciò lascia indubbiamente spazio a dispute legali sull'interpretazione della norma, dall'altra le organizzazioni dovranno comunque adottare meccanismi per garantire che le loro iniziative siano allineate alle più recenti innovazioni tecnologiche e alla conseguente evoluzione delle minacce.

[2] La pseudonimizzazione è una procedura che prevede la sostituzione dei campi più identificativi di un record di dati con uno o più identificatori artificiali (o pseudonimi).

NOTIFICA DELLE VIOLAZIONI

Il GDPR introduce inoltre per le organizzazioni un nuovo obbligo di notifica alle autorità competenti di qualsiasi violazione dei dati personali[3] che possa avere come conseguenza un rischio per "i diritti e le libertà delle persone fisiche"[4]. Quando il rischio è considerato "elevato", la notifica deve essere estesa anche agli interessati. La notifica deve essere effettuata "senza ingiustificato ritardo" e, ove possibile, entro 72 ore dalla scoperta dell'evento.

Anche in assenza di riferimenti espliciti a specifiche tecnologie di protezione dei dati e sicurezza di rete, la transizione alla conformità deve iniziare con la verifica che la rete sottostante sia sufficientemente protetta da tutti i possibili vettori di attacco.

SFIDE RELATIVE ALLA SICUREZZA DELLE RETI

MANTENERE DIFESE "ALLO STATO DELL'ARTE"

Tenere il passo con l'evoluzione del panorama delle minacce costituisce una sfida anche senza la condizione posta dal GDPR in merito a difese "allo stato dell'arte". Gli enormi proventi della criminalità informatica, per non parlare del potenziale terrorismo sponsorizzato da stati, assicura un livello di risorse e innovazione che può essere difficile da eguagliare per qualsiasi singola impresa o persino per governi nazionali.

Parte del problema deriva dalle modalità di evoluzione della sicurezza informatica, con la creazione di una soluzione di sicurezza aggiuntiva alla scoperta di ogni nuovo vettore di attacco. Anche se ogni aggiunta di questo tipo può assolvere al compito designato, ciò avviene principalmente in un contesto isolato, con un'interazione scarsa o nulla con il resto dell'infrastruttura di sicurezza. Questo modo di procedere non solo è difficile da gestire, ma può facilmente condurre a lacune e incoerenze nella risposta a nuove minacce, specialmente in un ambiente multi-vendor.

La sfida è resa più complessa dall'adozione di tendenze quali la mobilità, il cloud computing e l'Internet of Things, che espandono tutte la superficie di attacco effettiva, esponendo nuove vulnerabilità ed erodendo il concetto tradizionale di perimetro di rete.

Una risposta alle nuove minacce consiste nel prevedere più processi e controlli ma, come può testimoniare chiunque abbia familiarità con le procedure di sicurezza adottate negli aeroporti e alle frontiere, un aumento dei controlli può presto condurre a caos e ritardi inaccettabili. L'aggiunta di processi aumenta inoltre la complessità, moltiplicando il numero di punti dati da aggregare e interpretare durante la valutazione della risposta migliore da adottare per ogni evento rilevato.

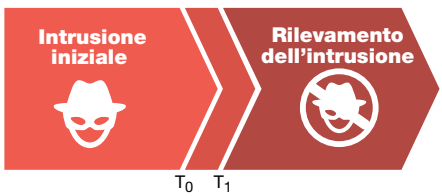
Qualsiasi soluzione meritevole della definizione "stato dell'arte" dovrà non solo superare le sfide descritte, ma adattarsi continuamente ai cambiamenti nell'uso della tecnologia e all'evoluzione del panorama delle minacce.

NOTIFICARE LE VIOLAZIONI ENTRO 72 ORE

La prima sfida comportata dal requisito del GDPR di notifica delle violazioni consiste nel rilevare quando si verifica una violazione che rientra nella definizione e determinare quali risorse possono essere a rischio. Quasi per definizione, qualsiasi violazione esterna della sicurezza che raggiunga il suo scopo deve avere evaso completamente i meccanismi di rilevamento, oppure non essere stata rilevata con sufficiente tempestività. Ciò significa che ha sfruttato un meccanismo di attacco diverso da tutti quelli rilevati in precedenza, oppure che i segnali di allarme che ha generato non sono stati colti.

È un fatto che, nel 2016, il tempo medio impiegato dalle organizzazioni per scoprire una violazione tipica sia stato di quasi cinque mesi[5]. Fortunatamente, la finestra di 72 ore prevista dal GDPR si apre al momento del rilevamento, non al momento dell'intrusione. Tuttavia, poiché l'impatto finanziario di una violazione è fortemente correlato al tempo di cui l'hacker dispone per accedere ai sistemi, l'abbreviazione del tempo di rilevamento resta una necessità fondamentale.

Ovviamente, è impossibile rilevare ciò che non è rilevabile; gli amministratori della sicurezza devono pertanto accettare il fatto che occasionalmente può verificarsi un'intrusione e prepararsi di conseguenza, puntando al tempo stesso alla massima riduzione di tali eventi e all'accelerazione del loro rilevamento con ogni mezzo possibile. Come accennato in precedenza, il GDPR non richiede la notifica di tutte le violazioni della sicurezza, ma solo di quelle che presentano un rischio per i diritti delle persone. Pertanto, se i dati violati sono stati adeguatamente offuscati tramite crittografia o pseudonimizzazione e se la durata dell'accesso non autorizzato è mantenuta breve, il rischio per tali diritti dovrebbe essere minimo.



[3] Una violazione dei dati personali è definita qui come qualsiasi violazione della sicurezza risultante nella distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali.
[4] Articolo 32 GDPR, "Sicurezza del trattamento".
[5] Report M-Trends 2016.

Tuttavia, il fatto che uno specifico profilo di attacco non sia stato rilevato prima non lo rende necessariamente non rilevabile. Con la giusta combinazione di threat intelligence e analisi del traffico distribuite, unite a tecnologie come il sandboxing, è comunque possibile bloccare anche attacchi che si presentano per la prima volta. La sfida che tali tecniche di rilevamento avanzate devono affrontare è quella di distinguere i segnali rilevanti da tutto il rumore di fondo.

Questa sfida è paragonabile a quella affrontata in tutto il mondo dalle organizzazioni antiterroristiche, che devono estrarre i segnali rivelatori di un prossimo attacco dalle azioni e dalle comunicazioni di migliaia di soggetti sotto sorveglianza attraverso più giurisdizioni e confini nazionali. Senza una vasta collaborazione e tecnologie di riconoscimento automatizzato di schemi ricorrenti, il lavoro di tali organizzazioni avrebbe poche possibilità di successo.

Analogamente, l'approccio tradizionale alla sicurezza di rete, che prevede più soluzioni isolate che inviano segnalazioni a un singolo amministratore umano, al quale sono demandate le decisioni da prendere, sta rapidamente diventando insostenibile. L'aumento sia della complessità delle reti che della frequenza degli eventi relativi alla sicurezza rende essenziale l'introduzione nell'infrastruttura di sicurezza di un certo grado di collaborazione e automazione intelligente.

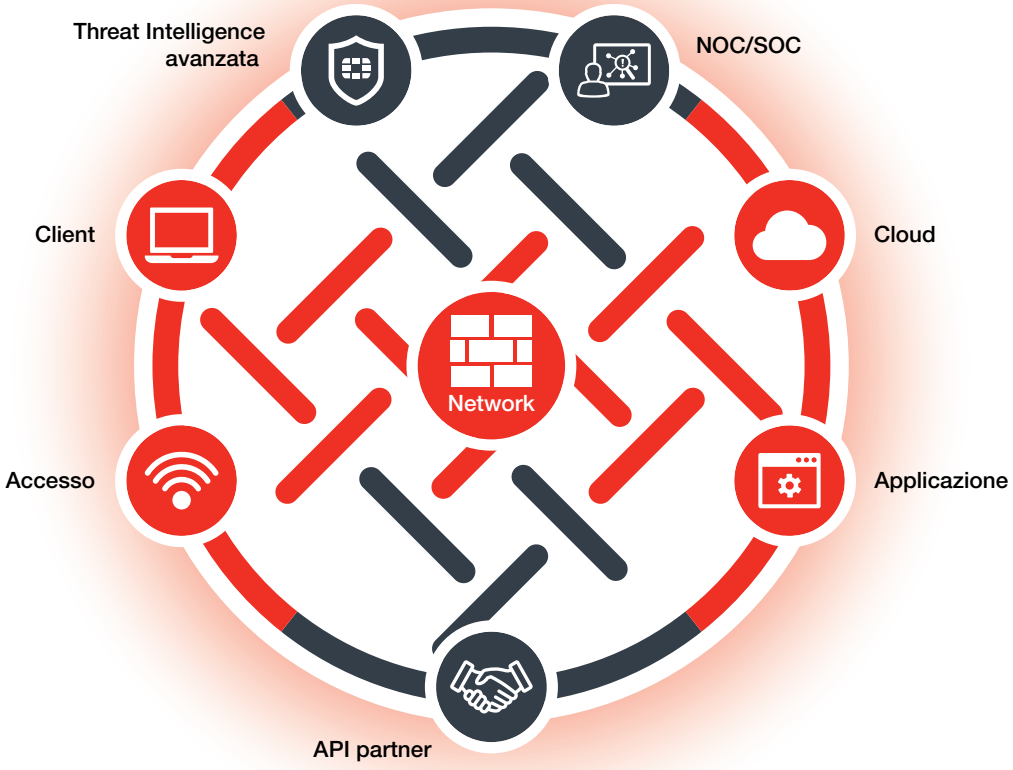
LA SOLUZIONE FORTINET: SICUREZZA FIN DALLA PROGETTAZIONE

Anche se la conformità al GDPR non può essere raggiunta solo attraverso la tecnologia, il requisito di tecnologie di sicurezza di rete "allo stato dell'arte" è chiaramente un primo passaggio essenziale. Per ridurre l'esposizione alle implicazioni potenzialmente paralizzanti di una grave violazione dei dati, è necessario ridurre al minimo sia il numero delle intrusioni nella rete, sia il tempo richiesto per rilevarle. È qui che Fortinet può dare il maggiore contributo all'impegno complessivo di un'organizzazione per conseguire la conformità.

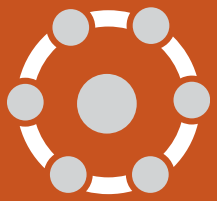
Alla base della soluzione Fortinet vi è un nuovo approccio alla sicurezza, nel quale tutti i componenti chiave dell'infrastruttura di sicurezza sono interconnessi in un sistema coerente.

FORTINET SECURITY FABRIC

Il Fortinet Security Fabric è basato su tre proprietà chiave: **esteso, avanzato e automatizzato**, per-offrire una risposta ottimale alle sfide comportate dalla protezione delle attuali reti complesse a banda larga, senza confini, dalla minaccia in rapida evoluzione degli attacchi informatici.



IL FORTINET SECURITY FABRIC



ESTESO

Progettato per coprire la superficie di attacco in espansione delle moderne reti aziendali, Il Fortinet Security Fabric fornisce protezione, visibilità e controllo per ogni parte dell'ambiente: endpoint cablati e wireless, risorse su cloud pubblico e privato, data center e le applicazioni stesse.

Combinato alla segmentazione dinamica della rete, che separa logicamente dati e risorse, il Fortinet Security Fabric può esaminare la rete in profondità per scoprire nuove minacce che passano da una zona all'altra. Questa distribuzione estesa e visibilità approfondita è un passaggio cruciale per la conformità, consentendo di monitorare il traffico e i dispositivi interni, impedendo l'accesso non autorizzato a risorse sensibili e limitando la diffusione di intrusioni e malware.

Inoltre i vantaggi del Fortinet Security Fabric non sono limitati al portfolio di soluzioni di sicurezza Fortinet. Grazie alle API aperte, alla tecnologia di autenticazione aperta e ai dati di telemetria standardizzati, sta emergendo un crescente ecosistema di partner che offrono integrazioni con il Fabric, consentendo alle organizzazioni di integrare gli investimenti esistenti in sicurezza e rete nel proprio Fortinet Security Fabric.

AVANZATO

La potenza di elaborazione di molte appliance di sicurezza tradizionali non riesce più a tenere il passo con l'aumento della larghezza di banda delle reti e della complessità delle minacce, costringendo spesso le organizzazioni a confrontarsi con un compromesso inaccettabile: ridurre il livello di protezione, con il rischio di un'intrusione attraverso un vettore di attacco non coperto o una parte della rete non protetta, o accettare un calo delle prestazioni delle applicazioni nella rete.

Scaricando i processi riguardanti sicurezza e contenuti su unità di elaborazione della sicurezza (Security Processing Unit, SPU) dedicate e personalizzate, che uniscono accelerazione hardware con firmware altamente ottimizzato, i prodotti Fortinet sono diventati i più veloci del settore, consentendo alle organizzazioni di implementare una sicurezza completa senza compromessi sulle prestazioni.

AUTOMATIZZATO

In aggiunta alla visibilità estesa dell'intera superficie di attacco e a una potenza di elaborazione in grado di analizzare in profondità ogni pacchetto, il Fortinet Security Fabric è anche in grado di combinare le informazioni strategiche raccolte dai propri componenti distribuiti per correlare rapidamente gli eventi e coordinare una rapida risposta automatica appropriata al livello di rischio.

Con la stessa rapidità con cui rileva le nuove minacce, il Fortinet Security Fabric è in grado di isolare automaticamente i dispositivi interessati, partizionare i segmenti della rete, aggiornare le regole, distribuire nuove policy e rimuovere il malware. Di pari passo con la crescita della rete aziendale e con il suo adattamento ai cambiamenti delle esigenze del business, il Fortinet Security Fabric cresce e si adatta di conseguenza, estendendo automaticamente le policy di sicurezza più recenti ai nuovi dispositivi, carichi di avoro e servizi, man mano che vengono distribuiti, che sia in ambiente locale, remoto o cloud.

IN SINTESI

Per molte organizzazioni, la transizione iniziale alla conformità al GDPR sarà con tutta probabilità un processo lungo e impegnativo. Inoltre, poiché il procedere inarrestabile della rivoluzione digitale porta progressi tecnologici a entrambi i campi della guerra informatica, tale conformità richiederà un riesame regolare, basato su una continua rivalutazione dei rischi.

Fondamentale per questo continuo processo sarà il ruolo della sicurezza di rete nella prevenzione delle intrusioni e nella riduzione del rischio di violazioni gravi, attraverso la riduzione del tempo necessario per rilevare le nuove minacce. Il raggiungimento di questo obiettivo richiede un approccio alla sicurezza esteso, avanzato e automatizzato.

Il Fortinet Security Fabric concretizza una visione tecnologica collaborativa che integra la potenza e intelligenza collettive del portfolio di soluzioni di sicurezza Fortinet per offrire vantaggi maggiori della semplice somma delle sue parti.

Le soluzioni di sicurezza Fortinet sono progettate secondo criteri di sicurezza scalabile interconnessa, elevate capacità di riconoscimento, threat intelligence efficiente e standard API aperti, per offrire una protezione integrata agli ambienti aziendali più complessi, guadagnandosi le certificazioni più indipendenti per efficacia e prestazioni nel settore della sicurezza. Queste soluzioni, che realizzano la visione del Fortinet Security Fabric, colmano le lacune lasciate dai prodotti tradizionali non integrati e forniscono la protezione end-to-end estesa, avanzata e automatizzata richiesta attualmente dalle organizzazioni nei loro ambienti fisici, virtuali e cloud.

Italia - Roma
Via del Casale Solaro, 119
00143 Roma
Italia
Vendite: +39 06-51573-330

Italia - Milano
Centro Torri Bianche Palazzo Tiglio
20871 Vimercate (MB)
Italia
Tel: +39 039 687211

SEDI GLOBALI
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
Stati Uniti
Tel: +1.408.235.7700
www.fortinet.com/sales

UFFICIO VENDITE EMEA
905 rue Albert Einstein
06560 Valbonne
Francia
Tel: +33.4.8987.0500

UFFICIO VENDITE APAC
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

AMERICA LATINA SEDE CENTRALE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

67717 0 1 IT