CITRIX®

Preparatevi per il GDPR con una distribuzione sicura di applicazioni e dati

Soddisfate le nuove regole europee sulla privacy dei dati in termini di responsabilità, governance e privacy

A partire dal 25 maggio 2018, il Regolamento generale sulla protezione dei dati (GDPR) attuerà un nuovo quadro giuridico nell'Unione europea (UE) per la protezione e la distribuzione dei dati personali. Le organizzazioni di tutto il mondo che servono clienti e individui nell'UE saranno tenute ad adottare politiche in materia di sicurezza per fronteggiare vari rischi e applicarle in modo efficace con l'ausilio di controlli tecnici; in caso contrario potranno incorrere in sanzioni fino a 10 milioni di euro o anche più. Anche se prepararsi al GDPR può rappresentare una sfida significativa per gran parte delle organizzazioni, molti dei requisiti tecnici richiesti sono in linea con le best practice in materia di sicurezza e conformità già supportate dalle soluzioni Citrix.

Citrix semplifica la sicurezza e la conformità consentendo al reparto IT di creare un perimetro software-defined che unisce un accesso sicuro ad applicazioni e dati a controlli contestuali, visibilità e analisi del comportamento per tutti i dispositivi, le reti e i cloud. Estendendo il controllo oltre il datacenter tradizionale per mediare le interazioni degli utenti con applicazioni e dati, il reparto IT può proteggere, rilevare e mitigare i rischi in modo proattivo grazie all'intelligence applicata a ogni singola situazione.

Questo white paper descrive i requisiti del GDPR e come è possibile soddisfarli grazie alle tecnologie Citrix integrate per l'accesso contestuale, la sicurezza della rete, delle applicazioni e dei dati, nonché gli strumenti analitici e di approfondimento.

Che cosa significa il GDPR per la vostra organizzazione

Il GDPR rafforza e armonizza le leggi sulla protezione dei dati nei Paesi appartenenti all'Unione Europea, poiché si applica a tutte le organizzazioni all'interno dell'UE o alle organizzazioni che controllano o elaborano i dati personali degli individui nell'UE. Questo regolamento prevede un elevato livello di accortezza e di responsabilità per queste organizzazioni, dando agli individui un maggiore controllo sui propri dati attraverso misure che includono la pseudonimizzazione, la minimizzazione dei dati e i controlli in materia di raccolta, elaborazione, storage e accessibilità dei dati. L'obiettivo del GDPR è dare agli individui un migliore controllo sui loro dati personali e garantire che le aziende stiano adottando misure per mitigare i rischi di dannose violazioni dei dati, incluso l'accesso non autorizzato all'interno dell'organizzazione.

Secondo il GDPR, gli individui disporranno di diritti quali la possibilità di accedere ai loro dati personali, rettificare imprecisioni od omissioni, richiedere la cancellazione o la rimozione dei dati una volta che non siano più necessari, limitare l'elaborazione dei propri dati e opporsi all'uso dei medesimi. Il GDPR si applica a un ambito ampio e completo di dati che comprende tutte le informazioni relative a una persona fisica identificata o identificabile, indipendentemente dal fatto che i dati siano stati forniti dall'individuo, osservati da sistemi quali browser web e piattaforme di social media, derivati da processi semplici come la cronologia delle transazioni o dedotti attraverso elaborazioni complesse.

Uno studio recente ha rivelato un basso livello di preparazione fra le organizzazioni interessate, accompagnato da un elevato livello di ansia. Secondo lo studio *La necessità di una nuova architettura per la sicurezza IT: uno studio globale sulle sfide della conformità e sull'efficacia della sicurezza sul luogo di lavoro*[1], pubblicato dal Ponemon Institute:

[1] https://www.citrix.com/it-security/resources/ponemon-security-study.html

- Sebbene il 67% degli intervistati sia a conoscenza del GDPR, solo la metà delle organizzazioni prese a campione ha stanziato fondi a bilancio e ha iniziato a prepararsi in vista di queste nuove norme.
- Fra gli intervistati che sono a conoscenza del GDPR, la principale preoccupazione riguarda le potenziali sanzioni. Eventuali violazioni delle disposizioni possono causare sanzioni fino a 20 milioni di euro o il 4% dei ricavi annuali a livello mondiale, a seconda di quale valore sia maggiore. Per le altre violazioni, le autorità possono imporre sanzioni fino a 10 milioni di euro o il 2% dei ricavi annuali a livello mondiale, a seconda di quale valore sia maggiore.
- Il 74% degli intervistati afferma che il rispetto del GDPR avrà un impatto significativo e negativo sulle loro organizzazioni, con il rischio di potenziali sanzioni di importo elevato e una maggiore portata territoriale dei regolamenti.

Tali preoccupazioni sono comprensibili se si considerano gli estesi requisiti del GDPR, con misure a livello sia organizzativo sia tecnico. Dal punto di vista organizzativo, le politiche previste dal GDPR includono il mantenimento di registri delle attività di elaborazione dati, la segnalazione di eventuali violazioni ai dati delle quali l'organizzazione sia venuta a conoscenza, la risposta alle richieste di informazioni e di cancellazione dei propri dati da parte dei clienti e, in determinate circostanze, la nomina di un agente responsabile per la protezione dei dati.

Le misure necessarie a livello tecnico includono funzionalità per l'accesso remoto sicuro ai dati e il trasferimento sicuro dei dati. I dati devono essere tenuti al sicuro, a prescindere dal fatto che siano condivisi all'interno dell'organizzazione o con altre organizzazioni. Le organizzazioni con più banche dati, sia in locale sia sul cloud, devono applicare tali misure in modo completo. Inoltre, per dimostrare la conformità con il GDPR, le organizzazioni devono attuare misure complete di governance per ridurre al minimo il rischio di violazioni, salvaguardare la protezione dei dati personali, nonché garantire e dimostrare che i requisiti tecnici e organizzativi descritti nel GDPR siano stati rispettati.

L'Ufficio del commissario delle informazioni (Information Commissioner's Office, ICO) del Regno Unito offre orientamenti particolarmente rilevanti ai fini della conformità al GDPR: le organizzazioni dovrebbero "garantire che la protezione della privacy e dei dati sia una priorità fondamentale nelle fasi iniziali di qualsiasi progetto e successivamente durante tutto il suo ciclo di vita". Gli esempi citati dall'ICO includono progetti quali:

- Realizzare nuovi sistemi informatici per l'archiviazione o l'accesso ai dati personali
- Sviluppare normative, politiche o strategie con implicazioni sulla privacy
- Avviare iniziative di condivisione dei dati
- Utilizzare i dati per nuovi scopi[2]

Nel seguire questi principi, l'ICO raccomanda di adottare un approccio "privacy-by-design" che promuove la conformità alla privacy e alla protezione dei dati fin dall'inizio, definendolo "uno strumento essenziale per ridurre al minimo i rischi per la privacy e per creare fiducia".[3] Utilizzando sistemi IT dove la privacy è integrata nel design e nell'architettura, le organizzazioni possono adottare misure proattive per implementare in modo predefinito una privacy end-to-end, anziché

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

[3] https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

"Le organizzazioni dovrebbero garantire che la protezione della privacy e dei dati sia una priorità fondamentale nelle fasi iniziali di qualsiasi progetto e successivamente durante tutto il suo ciclo di vita."

L'Ufficio del commissario delle informazioni (Information Commissioner's Office, ICO) del Regno Unito

ricorrere a tecnologie di protezione aggiuntive applicate in modo frammentario a sistemi privi di misure di sicurezza integrate. Le soluzioni di workspace digitali di Citrix supportano l'approccio "privacy-by-design" raccomandato dall'ICO grazie alla sicurezza unificata e contestuale integrata nel loro nucleo.

In che modo la sicurezza di Citrix aiuta le organizzazioni a essere pronte per il GDPR

Le soluzioni di Citrix possono aiutare le organizzazioni a essere pronte per il GDPR fornendo una base fondamentale per la riservatezza, l'integrità e la disponibilità in tutti i tipi di ambienti IT in locale, su cloud ibridi e su cloud pubblici. L'approccio di Citrix in ambito di sicurezza e conformità si basa su quattro principi:

- Laddove è possibile, centralizzate le applicazioni e i dati nel datacenter o sul cloud, in modo tale che i dati aziendali sensibili non vengano memorizzati sui dispositivi.
- Quando i dati sensibili devono essere distribuiti, resi mobile o utilizzati offline, assicuratevi che siano protetti in un'area sicura.
- Controllate con precisione l'accesso alle risorse utilizzando policy contestuali basate su utente, dispositivo, ubicazione, applicazione e sensibilità dei dati.
- Fornite funzionalità di visibilità e gestione in grado di contemplare l'intera infrastruttura IT per fornire una sicurezza specifica per i dati e per le applicazioni.

Questi principi vengono adottati nelle tecnologie integrate di Citrix per l'accesso contestuale, la sicurezza della rete, delle applicazioni e dei dati, nonché gli strumenti analitici e di approfondimento per supportare la conformità al GDPR nelle seguenti cinque aree:

Accesso ai dati personali

Il GDPR richiede che le organizzazioni controllino e limitino l'accesso ai dati personali. Grazie a Citrix le organizzazioni possono controllare e proteggere l'accesso alle applicazioni e ai dati attraverso l'autenticazione a più fattori. Le policy di accesso basate su gruppi e su utenti sono integrate da controlli contestuali che adattano i privilegi di accesso in modo dinamico in base al dispositivo, alla posizione e alla rete rilevati per l'utente, applicazione per applicazione.

Crittografia dei dati in transito

Il GDPR richiede la crittografia dei dati personali in transito. Per evitare che i dati vengano compromessi durante il trasferimento sulla rete, le soluzioni offerte da Citrix si avvalgono di misure di crittografia per le comunicazioni tra gli endpoint e i dati centralizzati. Di conseguenza, le organizzazioni possono consentire l'accesso remoto sicuro alle applicazioni e ai desktop virtuali ai dipendenti così come agli appaltatori, ai fornitori, ai partner e ad altri soggetti terzi, il tutto disciplinato da controlli degli accessi contestuali e senza mettere i dati a rischio.

Isolamento e protezione dei dati

Per rafforzare ulteriormente la protezione dei dati e ridurre il rischio di violazioni, come richiesto dal GDPR, Citrix fornisce misure complete per la sicurezza delle applicazioni e dei dati, inclusa la centralizzazione, la containerizzazione, l'ispezione e la segmentazione. Le soluzioni Citrix sono costruite su un'architettura centralizzata che mantiene i dati nel datacenter, dove sia i dipendenti sia terze parti autorizzate possono accedervi in remoto senza essere esposti a rischi sull'endpoint di un utente. La centralizzazione migliora anche la protezione dei dati consentendo una gestione più semplice, più efficiente e ottimizzata dei backup, delle patch e delle configurazioni del sistema. Questo aiuta le organizzazioni a rimanere aggiornate con l'ultima protezione contro il ransomware e le altre minacce, oltre ad agevolare il recupero dei dati in caso di incidenti. Per i dispositivi mobile come gli smartphone e i tablet, la containerizzazione mantiene i dati aziendali e dei clienti separati dai dati personali dell'utente che il dispositivo può contenere. L'ispezione della rete aiuta le organizzazioni a dissuadere dagli attacchi contro i servizi aziendali critici e a prevenire le perdite dei dati. All'interno del datacenter, il reparto IT può applicare la segmentazione della rete per isolare i dati personali di ogni cliente da quelli degli altri clienti, dalle applicazioni di back-office e dal resto dell'infrastruttura IT.

Crittografia dei dati a riposo

In un panorama dove il GDPR cerca di proteggere i clienti dalla divulgazione involontaria dei loro dati, sia da persone interne sia da terze parti, le soluzioni offerte da Citrix aiutano le organizzazioni a proteggere e cifrare i dati ovunque vengano memorizzati. Il reparto IT può impedire che i dati

siano memorizzati sugli endpoint mantenendoli criptati nel datacenter per ridurre la perdita di dati a causa di endpoint smarriti, rubati o distrutti. Sui dispositivi mobile, inclusi gli smartphone e i tablet bring-your-own (BYO), la containerizzazione consente di separare le applicazioni personali e aziendali e i relativi dati memorizzati in locale. I dati dei clienti sui dispositivi mobile vengono cifrati e controllati dal reparto IT per impedirne la perdita nel caso in cui uno smartphone o un tablet vada perso o rubato. Gli strumenti di livello aziendale per la condivisione dei file e la collaborazione sui contenuti consentono agli utenti di lavorare in modo produttivo con i dati dei clienti senza ricorrere a servizi meno sicuri di livello consumer. Le funzionalità di sicurezza integrate, come le firme digitali, le filigrane elettroniche e la gestione dei diritti delle informazioni (IRM) consentono al reparto IT di mantenere una protezione ampia e multilivello, a prescindere da dove e come i dati dei clienti siano utilizzati.

Registri delle attività di elaborazione

Il GDPR invita le organizzazioni a mantenere registri completi sul trattamento dei dati personali. Le soluzioni Citrix offrono la visibilità e la verificabilità dell'accesso dell'utente per monitorare esattamente come e da chi è stato effettuato l'accesso ai dati personali. Mettendo al sicuro e registrando il movimento dei dati da un'estremità all'altra fra il datacenter e l'endpoint, le organizzazioni possono soddisfare al meglio le linee guida del GDPR.

Mantenere la conformità al GDPR grazie alle soluzioni Citrix

Per oltre un quarto di secolo, le organizzazioni di tutti i settori, inclusi quelli maggiormente regolamentati, si sono affidate a Citrix per proteggere le informazioni aziendali sensibili senza compromettere la produttività della forza lavoro. Citrix offre un'infrastruttura sicura per la distribuzione delle applicazioni e dei dati, fornendo al reparto IT strumenti molto potenti per controllare l'accesso alle applicazioni e ai dati su qualsiasi dispositivo, rete e cloud.

Citrix offre una soluzione integrata e sicura di workspace digitale che comprende le migliori tecnologie del settore per la distribuzione di applicazioni e desktop, il networking, la mobility e la condivisione dei file, per una distribuzione sicura di applicazioni e dati. Questa soluzione offre alle organizzazioni la flessibilità di scegliere tra una distribuzione sul cloud, con un service provider o completamente in locale.

Citrix può aiutare a supportare le linee guida del GDPR grazie alle seguenti tecnologie sicure.

Citrix XenApp e XenDesktop: distribuzione sicura di applicazioni e desktop virtuali.
Le applicazioni, i desktop e i dati a loro associati sono gestiti centralmente e messi in sicurezza nel datacenter. Il reparto IT può applicare dinamicamente una protezione contestuale all'applicazione o al desktop associato in base a criteri di controllo granulari, per consentire un accesso remoto sicuro da qualsiasi dispositivo. Le organizzazioni che devono rispettare requisiti di sovranità dei dati possono utilizzare la centralizzazione dei dati per consentire l'accesso remoto da altre aree geografiche senza consentire ai dati di lasciare il proprio territorio.

Citrix NetScaler: accesso remoto sicuro e protezione delle applicazioni web.
Il reparto IT ottiene il controllo, la visibilità e la crittografia end-to-end per il traffico di rete e le applicazioni in modo da garantire la distribuzione sicura di applicazioni e dati. Il reparto IT può applicare un controllo granulare degli accessi tramite policy di accesso contestuali in base all'utente, al dispositivo, alla posizione e alla rete. Le applicazioni e i siti web sono protetti da attacchi noti e sconosciuti. Inoltre, il firewall per le applicazioni web, la protezione dagli attacchi DDoS e il filtraggio degli URL aiutano a raggiungere la conformità.

Citrix XenMobile: gestione della mobility aziendale.
I dati e le applicazioni aziendali possono essere containerizzati su dispositivi mobile, compresi smartphone e tablet BYO, e cancellati in remoto dal reparto IT per proteggere i dati dei clienti nel caso in cui il dispositivo vada perso o rubato. Qualsiasi tipo di contenuto di proprietà dell'utente eventualmente presente sul dispositivo viene tenuto separato dai contenuti aziendali e non viene alterato in nessun modo dalla funzione di cancellazione da remoto. Inoltre, grazie alla funzionalità micro-VPN di Citrix, i dati in transito vengono criptati.

Citrix ShareFile: leader nella sincronizzazione e condivisione dei file.
L'accesso a dati personali in locale e sul cloud può essere controllato e garantito attraverso l'autenticazione multifattoriale, le policy di password, la sicurezza mobile e le funzionalità di sicurezza della rete. Tutti i dati all'interno di ShareFile sono cifrati a riposo e possono essere ulteriormente protetti tramite IRM e DLP. Il reparto IT può impostare policy di condivisione dei dati per limitare e controllare ulteriormente l'accesso ai dati personali.

Se un dispositivo mobile o un computer portatile vengono smarriti oppure rubati, i dati di ShareFile in esso contenuti possono essere cancellati in remoto dal reparto IT. Le funzionalità di controllo e verifica dell'accesso ai dati semplificano la conformità al GDPR nelle varie postazioni delle risorse.

Conclusioni

Anche se il GDPR può rappresentare una sfida significativa per gran parte delle organizzazioni, molti dei requisiti tecnici richiesti sono in linea con le best practice di sicurezza e conformità già supportate dalle soluzioni Citrix, nonché con i principi di sicurezza su cui esse si fondano. Citrix può aiutare le organizzazioni di ogni settore (incluso il settore governativo, finanziario e sanitario che sono altamente regolamentati) a soddisfare i requisiti interni e regolamentari nell'ambito della sicurezza e della protezione dei dati. Ora che le organizzazioni di tutto il mondo si preparano al GDPR, le soluzioni per il workspace digitale sicuro di Citrix consentono di adottare un approccio semplice per ottenere la conformità senza ostacolare la produttività.

Per maggiori informazioni sulla sicurezza e la conformità con le soluzioni di workspace digitale sicuro di Citrix, visitate citrix.it/secure.

Reparto vendite per le aziende
Dal Nord America | +1 800 424 8749
Dal resto del mondo | +1 408 790 8000

Sedi
Sede centrale | 851 Cypress Creek Road Fort Lauderdale, Florida 33309 Stati Uniti
Silicon Valley | 4988 Great America Parkway Santa Clara, California 95054 Stati Uniti