ivanti

Cinque strategie di sicurezza in vista del GDPR

Sommario

Introduzione

2017 è stato l'anno delle violazioni di dati. Se si aggiungono poi le maggiori esigenze in termini di protezione dei dati personali, si comprende perché vengono introdotte normative più rigorose volte a proteggere i dati dei cittadini, come il nuovo regolamento generale sulla protezione dei dati, o GDPR. Queste tuttavia comportano un maggior carico di responsabilità per i reparti IT aziendali, che devono trovare nuovi modi di potenziare la sicurezza senza ostacolare la produttività dei lavoratori. Questa guida offre importanti consigli pratici per aiutare i responsabili IT a districarsi tra i requisiti di conformità GDPR e la protezione dei dati personali.

L'impatto del GDPR

Con organizzazioni quali Equifax e Uber che sono cadute vittima di attacchi informatici e non hanno comunicato tempestivamente l'esposizione di dati personali, l'Unione Europea invita a implementare riforme importanti con la nuova normativa GDPR. Per molte organizzazioni questo significa adottare modalità completamente nuove di acquisire, gestire, proteggere e monitorare le informazioni sui clienti e i dipendenti. Inoltre, non è più possibile celare eventuali violazioni di dati personali. Questa normativa mira a standardizzare e rendere più severe le leggi in materia di dati personali per tutte le organizzazioni che trattano con dipendenti o clienti europei. La mancata conformità al regolamento GDPR prevede sanzioni, penali e risarcimenti dei danni subiti[i]. Le sole sanzioni amministrative per la mancata conformità ad alcuni dei requisiti GDPR possono ammontare a 20 milioni di euro o al 4% del fatturato mondiale annuo dell'azienda.

Entro quando occorre essere in linea con il nuovo regolamento? La scadenza è il 25 maggio 2018. Il potenziale di un tale impatto economico preoccupa molti nel mondo delle finanze EU. Per le assicurazioni per le imprese, la conformità GDPR rappresenta una notevole fonte di rischio nel calcolo del premio assicurativo annuo, e gli studi legali cercheranno di trarre vantaggio dalle organizzazioni inadempienti che espongono i dati dei clienti a potenziali rischi. La posta in gioco è alta e il tempo stringe.

Il regolamento GDPR introduce:

- Procedure di conformità dettagliate per rimediare alle minacce, con 72 ore di tempo per segnalare al garante competente eventuali violazioni di dati
- Sanzioni elevate in caso di violazione del regolamento GDPR
- Requisiti volti a garantire ai cittadini europei maggior controllo sui propri dati personali
- La necessità per le aziende di designare un Data Protection Officer (DPO) la cui responsabilità si incentra sulla protezione dei dati dei consumatori

In preparazione al GDPR: cinque strategie di sicurezza chiave

Il regolamento GDPR è chiaro sulla necessità di requisiti di sicurezza per la protezione dei dati dei cittadini europei, ma non specifica con altrettanta chiarezza ciò che si deve effettivamente fare per proteggere i dati personali in proprio possesso. Il percorso verso la conformità sarà diverso per aziende diverse, ma per la maggior parte di esse è possibile ridurre al minimo le minacce ai dati personali e il rischio di pesanti sanzioni affrontando cinque sfide chiave in merito alla sicurezza:

1. Protezione dei dati personali dalle minacce rivolte ai dispositivi mobili
2. Gestione dei diritti di amministratore per i sistemi e le applicazioni
3. Riduzione dell'impatto economico di ransomware e altri malware

4. Riduzione dei rischi associati all'onboarding e all'offboarding dei dipendenti
5. monitoraggio e reporting dell'accesso ai dati personali

Fortunatamente, per ognuna di queste sfide esistono strategie di sicurezza efficaci e di rapida implementazione da adottare in preparazione al GDPR e per proteggere i dati personali.

Strategia n.1: Ridurre l'esposizione a violazioni da parte dei lavoratori mobili.

Entro il 2020 si stima che il 72% dei lavoratori degli Stati Uniti utilizzaerà un dispositivo mobile per svolgere il proprio lavoro[ii]. Ma ogni dispositivo mobile e punto di accesso aumenta notevolmente il rischio di infiltrazione nell'infrastruttura aziendale. Per anni sono state sviluppate tecnologie di sicurezza statiche basate sul perimetro della rete aziendale, che purtroppo a nulla servono quando un dipendente solerte controlla dei dati dal suo smartphone collegato alla Wi-Fi di un bar o di un hotel.

Ridurre il rischio e contribuire a garantire la conformità GDPR non è un compito facile. Per proteggere le organizzazioni da questi nuovi tipi di rischi e garantire il rispetto dei requisiti GDPR, è necessario adottare nuovi criteri e controlli di sicurezza basati sul contesto. I controlli basati sul contesto adattano in modo dinamico l'ambiente di lavoro di ogni lavoratore al livello di sicurezza necessario di volta in volta, in base al livello di rischio:

- Si collegano con un dispositivo noto?
- Si collegano tramite una rete affidabile?
- Utilizzano periferiche o unità USB autorizzate dall'azienda?
- Tentano di accedere a informazioni sensibili durante l'orario di lavoro o a un'ora insolita?

Strategia n. 2: Riassumere il controllo degli accessi "privilegiati".

I diritti di amministratore forniscono agli utenti un livello di accesso che, se non utilizzato correttamente, può richiedere costosi interventi di supporto e compromettere l'esperienza degli utenti. In molti casi, la sicurezza viene anche compromessa da fattori quali l'errato trattamento dei dati, l'installazione di hardware o software non approvato, la perdita di dati o un attacco da minacce software. Ogni utente "privilegiato" rappresenta un potenziale obiettivo per attacchi informatici e aumenta la vulnerabilità: le sue autorizzazioni di accesso possono infatti essere sfruttate dai criminali informatici per accedere alle reti, ai sistemi e alle applicazioni aziendali.

Ma esistono molte situazioni in cui gli utenti hanno bisogno di diritti di amministratore locali per lavorare in modo efficiente. Molte applicazioni, incluse quelle più nuove, consentono di apportare modifiche alle impostazioni hardware o alle schede di rete, e richiedono quindi diritti di amministratore per poter essere eseguite. Tali modifiche comprendono ad esempio l'aggiornamento di applicazioni Web o di moduli Adobe/Flash/Java, oppure l'installazione di componenti Active-X o di driver di stampa.

Per rapidità e maggiore efficienza IT, alcune organizzazioni concedono autorizzazioni elevate praticamente a tutti nell'azienda, perché non dispongono delle risorse e capacità necessarie per gestire le autorizzazioni di accesso in modo più mirato. Nella maggior parte delle aziende, i criteri di accesso per "utenti con meno privilegi" sono spesso affiancati da standard piuttosto liberali. Inoltre, se gli utenti non possono accedere alle applicazioni di cui hanno bisogno, potrebbero ricorrere a soluzioni non autorizzate, introducendo elementi di rischio nell'ambiente di lavoro e compromettendo le iniziative di conformità.

Le organizzazioni devono essere in grado di assegnare e revocare i diritti di amministratore in base alle effettive esigenze, per proteggere l'azienda senza ostacolare la produttività degli utenti. Grazie ai controlli dinamici, i diritti di accesso possono essere ridotti immediatamente all'uscita da un'applicazione o al completamento di un determinato lavoro. Ogni volta che vengono ridotti i diritti di accesso, viene anche ridotto il rischio di violazione dei dati. L'implementazione di controlli dinamici ha un impatto notevole sulla gestione dei diritti di amministratore su grande scala e sul conseguimento della conformità ai requisiti GDPR.

Strategia n. 3: Contenere gli attacchi da ransomware e malware.

Per ridurre a zero l'impatto di ransomware e altri malware sull'azienda esiste una soluzione molto semplice: basterebbe... non lasciarli entrare! Questi attacchi si infiltrano in genere tramite messaggi e-mail di phishing e software vulnerabili a causa della mancata applicazione di patch. Oppure tramite unità esterne utilizzate per trasferire codice dannoso e accedere ai dati personali. Quando un utente fa clic su un collegamento pericoloso in un messaggio e-mail, visita un sito Web compromesso o collega un'unità USB non protetta, il dispositivo o computer su cui lavora può venire infettato. Il malware tenta quindi di diffondersi nell'ambiente e di carpire credenziali con cui accedere a siti web di terze parti, come siti di banking e retail. Con l'applicazione rigorosa delle patch ai sistemi operativi e alle applicazioni di terze parti, la gestione di whitelist con cui impedire l'esecuzione di codice non autorizzato e il blocco di siti Web e accesso ai file, le organizzazioni possono notevolmente ridurre l'esposizione agli attacchi.

Molte organizzazioni dispongono già di qualche forma di whitelisting, ma il più delle volte non si tratta di metodi completamente indolori. Le operazioni di discovery possono essere molto impegnative. Una volta implementata, la whitelist deve essere costantemente gestita e aggiornata. Gli utenti devono poter lavorare in modo efficace ed efficiente. Ogni giorno vengono introdotte nell'ambiente aziendale nuove app e versioni, che contribuiscono all'innalzamento dei costi nella gestione se si utilizzanoi metodi di whitelisting tradizionali. Alcune soluzioni, poi, possono rallentare sensibilmente il sistema, in quanto ogni applicazione a cui si accede deve essere valutata per verificare che corrisponda all'applicazione valida nota e che non si tratti di un file modificato o rinominato in modo da simulare uno dei file autorizzati.

Vale quindi la pena considerare soluzioni di whitelisting in grado di ridurre il carico di lavoro e massimizzare il valore apportato. Inoltre, l'aggiunta di controlli granulari a livello di hash, che utilizzano firme per l'apertura di file o l'esecuzione di applicazioni, può fare molto per evitare che gli utenti diano il via a un attacco facendo involontariamente clic su un collegamento o un allegato. È anche possibile implementare controlli per bloccare in modo dinamico l'accesso a specifici siti Web o file, per evitare che gli utenti salvino file sospetti sul proprio disco rigido e per bloccare i dispositivi esterni in modo che possano essere aperti o salvati solo i file protetti o crittografati. Infine, è importante assicurarsi che gli endpoint non siano compromessi da applicazioni affidabili modificate e in esecuzione nella memoria. Grazie ai controlli proattivi, le aziende possono proteggere i dati personali e dimostrare il rispetto dei requisiti di sicurezza GDPR.

Strategia n. 4: Implementare processi di onboarding e offboarding sicuri.

Molte organizzazioni si affidano ancora a processi manuali per l'onboarding e l'offboarding dei dipendenti, con conseguenti inesattezze e ritardi che possono protrarsi anche per diversi giorni o addirittura settimane. Secondo un recente studio condotto da Ponemon Institute, oltre il 24% delle persone che lasciano un'azienda ha ancora accesso ai dati aziendali anche a distanza di diverse settimane.[iii] Con specifici processi IT è possibile gestire automaticamente le autorizzazioni di accesso alle applicazioni e ai servizi a seconda del ruolo del dipendente. La stessa tecnologia permette anche di annullare automaticamente tali autorizzazioni di accesso non appena un dipendente lascia l'azienda, o di modificarle in seguito a un cambiamento di ruolo. L'automazione di tali processi aumenta la sicurezza e facilita notevolmente le attività IT in preparazione a un audit. Questi processi possono essere integrati direttamente nelle app già utilizzate dalle Risorse Umane, nei sistemi di gestione dei progetti o negli archivi di gestione delle identità, in modo che possano essere attivati automaticamente quando in tali sistemi si registrano delle modifiche allo stato dell'identità di un dipendente. Con un approccio più olistico di questo tipo, le organizzazioni possono migliorare sensibilmente sia la produttività degli utenti, sia la sicurezza a supporto dei requisiti del regolamento GDPR.

Strategia n. 5: Maggiore visibilità e capacità di reporting sui dati personali

Per dimostrare lo stato di conformità alle normative GDPR, è importante disporre di un elevato livello di visibilità nei dati che scorrono nell'ambiente IT. Deve essere possibile tenere traccia di chi accede ai dati, e

dimostrare che sono stati implementati i controlli adeguati per la protezione dei dati personali. Per individuare e porre rimedio alle minacce prima che facciano notizia, gli amministratori IT devono essere in grado di consolidare l'enorme quantità di informazioni da monitorare e trovare il modo di usufruirne in modo efficiente, estraendo in tempo reale le informazioni più critiche.

È inoltre necessario generare report con dettagli sull'ambiente di lavoro, comprese modifiche, utilizzo, dispositivi, app e configurazioni. Grazie al monitoraggio e ai report basati sui log, le aziende possono dimostrare l'effettiva conformità ai requisiti GDPR, nonché preparare rapidamente e trasmettere tutte le informazioni necessarie in caso di violazione di dati. Un elevato livello di visibilità su enormi moli di dati consente non solo di dimostrare in modo più efficiente l'effettivo stato di conformità, ma anche di condividere dati preziosi con chi ne ha bisogno, per accelerare le attività di business e cogliere nuove opportunità.

Ivanti può assistervi nell'attuare una solida strategia GDPR

Aiutiamo le organizzazioni più fidate al mondo a gestire e proteggere il loro ambiente IT con soluzioni tecnologiche che colmano il divario tra sicurezza, gestione dei servizi e operazioni IT, per automatizzare e proteggere l'ambiente di lavoro digitale.

Valutazione

In preparazione al GDPR, occorre innanzitutto valutare l'attuale livello di rischio di mancata compliance. Aspetti fondamentali per tale valutazione sono la trasparenza e la capacità di accedere ai dati di provisioning per utenti, client e server. Ivanti può aiutarvi a valutare rapidamente il livello di rischio grazie a pannelli personalizzati e strumenti di reporting. Potete visualizzare le minacce alla sicurezza dei dati personali in tempo reale e raccogliere informazioni sui flussi di lavoro richiesti per conseguire uno stato di conformità.

Automazione

Quindi occorre garantire il rispetto dei criteri applicabili per assicurare la corretta gestione dei dati personali e della privacy. Considerate, ad esempio, che oltre il 50% degli ex-dipendenti risulta ancora in grado di accedere alle applicazioni aziendali, e il 20% delle violazioni di dati sono imputabili alla mancata rimozione dei diritti di accesso[iv]. Le organizzazioni devono quindi essere in grado di prendere tempestivamente le misure necessarie a proteggere i dati personali.

Ivanti può aiutarvi a trasformare i criteri ed i processi manuali e soggetti ad errori in flussi di lavoro automatizzati basati sui ruoli degli utenti all'interno dell'azienda. Con le nostre soluzioni potete facilmente eseguire il provisioning e de-provisioning dei dipendenti nell'intero ambiente IT.

Protezione

Le soluzioni Ivanti rilevano e forniscono informazioni sui punti deboli nell'ambiente IT, e applicano le misure necessarie per proteggere i dati sensibili dagli attacchi. Grazie alle soluzioni Ivanti potete:

- Individuare le risorse hardware e software presenti nel vostro ambiente (DISCOVERY ed INVENTORY). Perché è impossibile proteggere o proteggersi dall'ignoto.
- Recuperare e monitorare dati, report e analisi.
- Applicare le PATCH alle applicazioni soggette a patch, e controllare l'accesso a quelle che non lo sono.
- Implementare controlli applicativi per proteggere i dati personali ed evitare di cadere vittima di attacchi ransomware.
- Controllare l'utilizzo di dispositivi removibili e applicare la cifratura dei dati su dispositivi removibili e unità disco rigide.
- Limitare i DIRITTI di AMMINISTRATORE senza limitare la produttività degli utenti e senza sovraccaricare il team IT.
- Assegnare agli utenti il livello di accesso appropriato in base alla loro identità, senza ostacolare la loro produttività e mantenendo i sistemi aziendali sempre protetti.

Capacità di risposta e ottemperanza

Infine, Ivanti può aiutarvi a dimostrare che i criteri necessari sono effettivamente applicati e rispettati, consolidando i dati nell'intero ecosistema IT per

fornire report contestuali in tempo reale e velocizzare le richieste di audit. Grazie ai connettori per oltre 50 delle maggiori soluzioni IT di terze parti già integrati nei prodotti Ivanti, iniziare col piede giusto è più facile che mai. Potete anche automatizzare i flussi di lavoro per individuare i dati richiesti in pochi minuti (e non ore) e ottenere informazioni immediatamente fruibili sui sistemi e gli endpoint per rispettare i requisiti GDPR.

Contattate Ivanti

La scadenza si fa sempre più vicina e i rischi alla sicurezza sono in agguato. L'implementazione di una strategia di conformità GDPR richiede del tempo. Iniziate subito a impostare le tecnologie, i processi e i criteri adeguati. Per saperne di più su come Ivanti può personalizzare una soluzione per le vostre esigenze, contattateci all'indirizzo sales@ivanti.com.

www.ivanti.it/GDPR

+39 02 8734 3421

contact@ivanti.it

i http://eur-lex.europa.eu/eli/reg/2016/679oj Articles 83 & 84
ii http://www.channelfutures.com/mobile-computing/idc-mobile-workers-us-exceed-105-million-2020
iii http://media.techtarget.com/Syndication/NATIONALS/data_Loss_Risks_During_Downsizing_Feb_23_2009.pdf
iv https://www.onelogin.com/press-center/press-releases/new-research-from-onelogin-finds-over-50-of-ex-employees-still-have-access-to-corporate-applications