Suggerimenti fondamentali per assicurare che i dispositivi endpoint soddisfino i requisiti di conformità.

Il regolamento generale sulla protezione dei dati dell'Unione Europea richiede alle aziende di implementare misure tecniche e organizzative per proteggere le informazioni personali degli utenti e per rendere noto ai soggetti e alle autorità eventualmente interessate, in tempi strettissimi, il verificarsi di un'eventuale violazione della sicurezza.

Questo rappresenta una sfida per le aziende che dovranno organizzarsi per tempo dotandosi delle risorse necessarie per conformarsi al regolamento.

Tuttavia, nel caso in cui le aziende non fossero in condizione di adottare più di un semplice firewall come protezione contro gli attacchi, significherebbe per loro esporsi a una violazione di tali regolamenti e ad incorrere in sanzioni milionarie. Al fine di tutelarsi da quanto evidenziato, sarà quindi fondamentale strutturare procedure e strumenti atti a identificare le violazioni e a rendere concrete tutte le misure correttive più idonee.

Questa checklist rappresenta una risorsa pratica per coloro che desiderano migliorare la propria sicurezza IT ed evitare le gravose conseguenze di una violazione. Iniziando dalla base, proseguite nella checklist verificando lo stato dei vostri sistemi fino ai massimi livelli di sicurezza: potrete così essere certi che i vostri endpoint saranno protetti e allineati con i requisiti previsti dal incombente GDPR.

Un pratico elenco per proteggere i dispositivi endpoint in rete.

Livello di sicurezza base

- Acquistare solo dispositivi con protezione contro i malware integrata e hard disk crittografati
- Aggiornare il firmware, in particolare le versioni con patch di protezione critiche, come nel caso di aggiornamenti delle applicazioni su cellulare
- Configurare le interfacce del dispositivo e bloccare i protocolli come FTP e telnet che non sono richiesti dalle applicazioni
- Analizzare i nuovi dispositivi e chiudere porte o protocolli non attualmente in uso che potrebbero consentire l'accesso agli intrusi
- Applicare password amministrative univoche a ciascun dispositivo
- Bloccare il pannello anteriore per disattivare l'accesso alle funzioni di amministratore
- Crittografare i dati in transito da e verso il dispositivo
- Impostare le procedure di cancellazione dell'hard disk per i vecchi dati, in particolare sulle stampanti che vengono cedute

Una volta completato, passare al livello di sicurezza successivo.

Livello di sicurezza medio

- Integrare i dati di registro dei sistemi delle stampanti nello strumento SIEM per garantire un monitoraggio completo della rete. Secondo i nuovi regolamenti in materia di conformità, la visibilità è fondamentale per soddisfare i requisiti di segnalazione.
- Adottare l'autenticazione dell'utente alla stampante per tenere traccia di chi esegue copie, scansioni e fax dal dispositivo. Questi dati sono utili per lo svolgimento di indagini dopo una violazione.
- Adottare la stampa pull per evitare che nelle stampanti vengano lasciati documenti contenenti informazioni importanti. Ciò contribuisce anche all'ottimizzazione dei vostri standard ambientali riducendo le stampe inutili.

Una volta completato, passare al livello di sicurezza finale.

Livello di sicurezza avanzato

- Impostare il monitoraggio delle attività di stampa e la rendicontazione per utente.
- Prendere in considerazione di impostare e applicare in modo automatico regole su chi e per quale motivo, abbia il permesso di accedere o utilizzare stampanti specifiche, con l'autorizzazione basata sui ruoli
- Adottare certificati digitali univoci per ogni stampante come per altri dispositivi connessi a Internet in rete
- Implementare una soluzione di stampa mobile gestita per la crittografia dei dati, l'accesso ai dispositivi in rete, l'autenticazione e il monitoraggio dell'utente

4AA7-1093ITE