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

Un pratico elenco per proteggere i dispositivi endpoint in rete.

I nuovi regolamenti richiedono alle aziende di aumentare la loro attenzione sulla sicurezza IT per garantire la protezione dei dati sensibili dei clienti e dei dati aziendali. Inoltre, le direttive, come il Regolamento generale UE sulla protezione dei dati (General Data Protection Reform, GDPR), richiedono alle aziende di valutare, monitorare e segnalare le violazioni della sicurezza entro pochi giorni.

La costante modifica dei regolamenti può rendere difficoltoso per le aziende trovare tempo e risorse necessari per tenersi al passo. Tuttavia, se non è possibile offrire più di un semplice firewall come protezione contro gli attacchi, esse potrebbero violare tali regolamenti e incorrere in sanzioni milionarie. Non vi è dubbio che ogni azienda subirà una violazione, sarà quindi fondamentale identificarla e adottare al più presto le misure correttive necessarie con i prodotti, i processi e gli strumenti idonei.

Questa checklist di controllo è una risorsa pratica per coloro che desiderano migliorare la propria sicurezza IT e proteggere la reputazione del marchio, evitare le gravose conseguenze di una violazione e rispettare i nuovi e rigorosi regolamenti. Iniziando dalla base, proseguite nella checklist fino ai massimi livelli di sicurezza, e potrete essere certi che la sicurezza degli endpoint sarà in linea con questi nuovi e rigorosi regolamenti.

Questa pratica checklist fornirà supporto anche al reparto IT a proteggere gli endpoint della stampante.

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