Brochure

Migliora la sicurezza di stampa dei tuoi clienti

Molte aziende hanno implementato un piano strategico per la sicurezza delle loro reti ed endpoint, che include anche una rigorosa protezione dei PC. Nonostante ciò, la maggior parte di tali piani d'azione non copre i dispositivi di stampa e imaging. Se stampanti e dispositivi multifunzione non sono protetti in modo adeguato possono mettere a repentaglio la sicurezza dell'intera rete. È quindi raccomandabile integrare le esigenze di sicurezza di imaging e stampa nelle proprie strategie di più ampio respiro per la sicurezza IT.

Le stampanti e dispositivi multifunzione HP LaserJet offrono circa 200 funzioni esclusive di sicurezza, che possono essere abilitate dai vostri clienti per mettere in sicurezza dispositivi e dati. La tecnologia di oggi consente di trovare un equilibrio tra sicurezza e fruibilità. E dato che ogni azienda è unica, le stampanti e dispositivi multifunzione HP escono dalla fabbrica già predisposte per adattarsi a un ampio numero di utenti. Le impostazioni disponibili sono talmente varie che, al primo sguardo, può sembrare non facile scegliere le più appropriate alle esigenze di ognuno.

Questa guida è stata pensata per aiutare a conoscere alcune funzioni base che tutte le aziende, indipendentemente dalle dimensioni o dal settore, dovrebbero implementare per salvaguardare i propri dispositivi di stampa e imaging di rete. Grazie alla spiegazione dell'utilizzo di ciascuna funzione e dei rischi connessi a impostazioni non sicure, potrete aiutare i clienti ad avviare una strategia di sicurezza che comprenda anche stampanti e dispositivi di imaging.

Impostazioni raccomandate per i dispositivi di stampa HP

I clienti potrebbero aver bisogno di aiuto per capire quali impostazioni di sicurezza utilizzare per proteggere i loro dati. Per questo abbiamo selezionato le impostazioni principali tra le oltre 200 disponibili. Si tratta di configurazioni di sicurezza di base, che qualsiasi azienda, indipendentemente da dimensione o settore, dovrebbe implementare. HP raccomanda queste impostazioni di sicurezza minime per affrontare i problemi più comuni.

Naturalmente ogni azienda è diversa e unica. Ogni cliente deve quindi identificare il miglior equilibrio tra sicurezza e produttività dell'utente finale. La configurazione di una multifunzione di rete potrebbe richiedere modifiche a queste impostazioni: sarà compito del cliente selezionare la configurazione più adatta alla sua rete.

Possibili effetti di dispositivi non sicuri

- Minore produttività dei dipendenti causata dalla modifica delle impostazioni del dispositivo: non sono più in grado di stampare, fotocopiare, effettuare scansioni o inviare fax
- Accesso non autorizzato a dati sensibili
- Potenziale vulnerabilità delle stampanti, incluse le credenziali
- Incremento delle richieste di assistenza, che rubano tempo prezioso al lavoro del personale IT

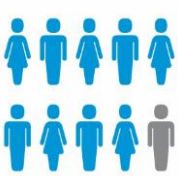
Prima di iniziare, raccomandate al cliente di:

- Effettuare l'upgrade del dispositivo alla versione di firmware più recente, per assicurarsi che il dispositivo sia dotato di tutte le funzionalità più aggiornate.
- Assicurarsi che la stampante o multifunzione sia protetta da un firewall. Alcune soluzioni HP richiedono una connessione Internet per funzionare al meglio.

Per evitare che...	Impostazione di sicurezza	Azione	Scopo dell'impostazione
Qualcuno possa modificare le impostazioni o i pulsanti di comando del dispositivo dal pannello di controllo (per es. per disabilitare alcune funzioni)	Password amministratore per Embedded Web Server (EWS) HP	Impostare una password	Regola l'accesso ai parametri di configurazione dell'EWS HP.
Qualcuno possa modificare le impostazioni del pannello di controllo	Password Printer Job Language (PJL)	Impostare una password	La funzione PJL offre un canale di comunicazione bidirezionale con la stampante e può essere utilizzata per modificare le impostazioni del pannello di controllo.
Qualcuno possa modificare le impostazioni sulla stampante, se la funzione "write" (scrittura) SNMPv1/v2 è abilitata	Protocollo SNMPv1 / v2 (Simple Network Management Protocol)	Impostare su “Read Only” (solo lettura)	Queste impostazioni forniscono supporto a strumenti di gestione più datati, basati su SNMPv1/v2 per il rilevamento e stato del dispositivo.
Qualcuno possa rilevare un dispositivo in rete e modificarne le impostazioni, se il protocollo SNMPv3 è lasciato aperto	SNMPv3	Abilitare e creare un account sul dispositivo	Il protocollo SNMPv3 utilizza un modello di sicurezza basato sull'utente, che include autenticazione e protezione dei dati tramite crittografia È un metodo più sicuro di SNMPv1/v2.
Qualcuno possa aggiornare il firmware, tornando a una versione meno sicura e influenzando la funzionalità delle soluzioni correnti, se lasciato accessibile	Aggiornare il firmware FTP	Disattivare	Un metodo per aggiornare il firmware sui dispositivi da remoto.
Qualcuno possa aggiornare il firmware da remoto, tornando a una versione meno sicura e influenzando la funzionalità delle soluzioni correnti, se lasciato accessibile	Aggiornamento firmware da remoto (Remote firmware upgrade – RFU)	Disabilitare NB: attivare per aggiornare il firmware da remoto, quindi disattivare una volta terminato l'aggiornamento.	Un altro metodo per aggiornare il firmware sui dispositivi da remoto.
Qualcuno possa inserirsi nel traffico di rete e visualizzare i dati, se non sono crittografati	Richiedere reindirizzamento HTTPS	Abilitare	Crittografare i dati trasmessi dal dispositivo al computer tramite un web server integrato.
Qualcuno possa accedere al dispositivo e modificarne le configurazioni, se i protocolli sono lasciati attivi	Disattivare i protocolli inutilizzati • Telnet • File Transfer Protocol (FTP) • Novell (IPX/SPX) • Appletalk	Disattivare	Questi protocolli consentono l'invio e la ricezione di informazioni da un dispositivo in rete. Tipicamente, i protocolli inutilizzati vengono lasciati per applicazioni legacy.
Gli utenti possano accedere e manipolare file come se fossero archiviati localmente sul loro disco rigido	Evitare l'accesso ai file • Network File Systems • Printer Management Language • Printer Job Language • Postscript	Disabilitare; verificare tutte le caselle	Consente a tutti gli utenti di rete di accedere da remoto ai file archiviati sul disco rigido della stampante.

Applica le policy di sicurezza a un intero parco stampanti HP in tutta semplicità

Circa il 90%



delle imprese dichiara di aver subito almeno una volta la perdita dei dati a causa di un sistema di stampa non protetto[1]

Il 65%

delle violazioni è dovuto a negligenze accidentali dei collaboratori o a errori nelle procedure IT o aziendali[2]

USD 7,6M totali

Il costo di una singola violazione dei dati è in media di USD 136 per dato compromesso e complessivamente di 7,6 milioni di dollari[2]

L'importanza delle policy di sicurezza

I tuoi clienti creano continuamente dati riservati e di valore, fondamentali per l'esecuzione delle loro attività. E probabilmente stanno utilizzando diversi metodi di sicurezza, tra cui autenticazione, crittografia e monitoraggio, per proteggere i dati nelle reti, nei PC e nei server. Ma il loro ambiente di imaging e stampa è protetto tanto quanto la loro infrastruttura?

Le falle alla sicurezza possono rendere i dati sensibili pericolosamente esposti:

- I dispositivi di imaging e stampa memorizzano i file su unità o dischi rigidi interni, dai quali chiunque può accedere a informazioni riservate.
- Le multifunzione acquisiscono e distribuiscono i lavori verso numerose destinazioni, potenzialmente esponendo i dati sensibili.

Le impostazioni di sicurezza possono essere obsolete o non conformi ai regolamenti.

- In alcuni paesi, l'azienda può subire sanzioni in caso di non conformità delle configurazioni di sicurezza.

Grazie alle impostazioni di sicurezza base descritte a pagina 2, potete aiutare i clienti ad avviare una strategia di protezione dei loro dispositivi di stampa e imaging.

Domande guida

Per identificare le esigenze del cliente, cominciate ponendogli domande relative al suo ambiente di lavoro, come:

- Quali criteri di protezione IT implementa attualmente?
- Le policy di sicurezza aziendali includono anche i dispositivi di stampa e imaging?
- È cosciente del fatto che le stampanti di rete sono un elemento vulnerabile?
- È in grado di configurare le impostazioni di sicurezza sui suoi dispositivi?
- Sapeva che HP offre una soluzione per progettare una policy di sicurezza e implementarla su tutti i dispositivi del parco?

HP JetAdvantage Security Manager

HP JetAdvantage Security Manager è uno strumento potente per creare e configurare le policy di sicurezza su tutti i dispositivi del parco stampa e imaging HP[3]. HP Security Manager offre una protezione ottimale ed è gestibile anche da chi non sia un esperto di sicurezza.

I dispositivi di stampa possono essere configurati per la sicurezza uno alla volta tramite l'Embedded Web Server (EWS), una soluzione non molto pratica quando si deve mettere in sicurezza un intero parco. Ma gestire la protezione del parco non deve necessariamente essere un esercizio gravoso o disagevole. Le impostazioni fornite a pagina 2 sono i parametri base raccomandati da HP per affrontare le questioni di sicurezza più comuni. Sono un sottogruppo di configurazioni collegate alle policy minime incluse in HP Security Manager.

Una volta avviato il processo di messa in sicurezza della rete, il cliente potrà poi creare la propria policy, basandosi sui parametri minimi e aggiungendone altri nel tempo. Utilizzando HP JetAdvantage Security Manager e dispositivi con tecnologia Instant-On, il cliente potrà abilitare impostazioni chiave di sicurezza non appena una nuova stampante è collegata in rete.

HP Security Manager
Metti in sicurezza il tuo parco stampanti HP con la soluzione definita pionieristica da Buyers Laboratory (BLI)[4]

HP JetAdvantage Security Manager mette in sicurezza il tuo parco

HP Security Manager consente di ottimizzare il processo di applicazione delle policy di sicurezza definite dal cliente su tutto il parco stampa e imaging HP, anche monitorando e garantendo la compliance. HP Security Manager identifica facilmente i dispositivi non conformi, riapplicando automaticamente le configurazioni di sicurezza previste dalla policy. HP Instant-on Security semplifica inoltre la protezione dei nuovi dispositivi HP non appena vengono aggiunti alla rete. Per gli amministratori IT diventa più facile gestire le procedure relative ai certificati, e la tua azienda risparmia tempo e denaro.

A differenza dei servizi tradizionali di gestione dei dispositivi in rete, che sono strumenti di utilizzo generico per il monitoraggio e la gestione dei dispositivi in uscita sulla rete, HP JetAdvantage Security Manager è la soluzione di sicurezza per la stampa più completa del mercato, in grado di offrire un approccio basato su policy per mettere efficacemente in sicurezza i dispositivi di stampa e imaging HP[5].

Per iniziare subito con una prova gratuita di 60 giorni, visita: software.hp.com/kiosk.

Username: HPSM_TRIAL60_KIOSK
Password: hpsm60020112

Per saperne di più

Per maggiori dettagli su come rendere HP Security Manager una parte integrante della tua strategia globale IT di sicurezza aziendale o su come ottenere una prova gratuita, visita hp.com/go/securitymanager.

[1] "Managed Print Services Landscape, 2014," Quocirca, giugno 2014.
[2] Ponemon 2014 Global Report on the Cost of Cyber Crime, ottobre 2014.
[3] HP JetAdvantage Security Manager deve essere acquistato separatamente. Per saperne di più o per una prova gratuita, visita hp.com/go/securitymanager.
[4] Fonte: Solutions Report on HP JetAdvantage Security Manager 2.1 di Buyers Laboratory LLC, febbraio 2015. Per maggiori dettagli, consulta hp.com/go/securitymanager o buyerslab.com.
[5] Basato su dati sicuri interni HP (Device Security Comparison, gennaio 2015) e Solutions Report on HP JetAdvantage Security Manager 2.1 di Buyers Laboratory LLC, febbraio 2015.

Iscriviti per ricevere gli aggiornamenti
hp.com/go/getupdated

4AA5-8727ITE, luglio 2015