White paper tecnico

Considerazioni relative alla sicurezza della stampante

Aspetti di sicurezza importanti da tener presenti nella valutazione delle soluzioni di stampa

Sommario

L'assenza di sicurezza nei dispositivi di stampa e scansione rappresenta l'attuale status quo

Tra i compiti principali da sempre affidati al reparto IT c'è la protezione delle informazioni riservate, inclusi identità dei dipendenti e dati dei clienti, su una molteplicità di dispositivi. Tale servizio deve essere fornito a utenti diversi caratterizzati da differenti approcci al lavoro all'interno dell'organizzazione, il che rende le minacce inattese alla sicurezza informatica una sfida costante nel tempo.

Sebbene le misure relative alla sicurezza su computer individuali e sulla rete aziendale vengano applicate in maniera rigorosa da parte di molti reparti IT, le minacce relative ai dispositivi di stampa e scansione vengono spesso sottovalutate, lasciando vulnerabili tali apparecchiature. Le minacce alla sicurezza sono reali e la sofisticatezza raggiunta dai dispositivi di stampa e scansione offre agli hacker sempre maggiori opportunità di compromettere i dispositivi o l'intera rete aziendale.

Le cinque aree principali nella sicurezza delle stampanti

Obiettivo principale del presente documento non è solo fornire un quadro generale, ma anche illustrare una serie di specifici aspetti relativi alla sicurezza di stampa da considerare durante l'acquisto, la distribuzione o l'utilizzo di stampanti e soluzioni di stampa. Le stampanti HP in grado di supportare le "3 principali" funzionalità di sicurezza (HP Sure Start, la tecnologia Whitelisting e il Rilevamento intrusioni durante l'operatività), lanciate sul mercato durante l'autunno 2015, soddisfano tutti i requisiti elencanti in ogni sezione (se abbinati a JetAdvantage Security Manger e ArcSight).[1] I dispositivi FutureSmart che non supportano HP Sure Start soddisfano tutti i requisiti ad eccezione di quelli elencati nella sezione numero 1 (Meccanismo Secure Boot). Consultate la tabella dispositivi di seguito per i dettagli relativi al supporto delle funzionalità di sicurezza.

È necessario concentrarsi su cinque aree fondamentali della sicurezza della stampante:

1. Meccanismo Secure Boot
2. Integrità del codice firmware
3. Rilevamento intrusioni durante l'operatività
4. Garanzia continua sulle impostazioni relative alle policy di sicurezza
5. Analisi e rilevamento minacce in tempo reale

Meccanismo Secure Boot

I punti elencati di seguito sono aspetti di un meccanismo Secure Boot che HP consiglia per la massima sicurezza:

- All'avvio, il dispositivo deve convalidare l'integrità del BIOS.
- Il dispositivo deve essere dotato di capacità di "auto-riparazione" di un BIOS infetto, sostituendolo con una copia sicura dell'hardware protetto del BIOS.
- Il dispositivo deve inviare notifiche all'amministratore mediante meccanismi di notifica dell'evento standard, tra cui i sistemi SIEM, in relazione a qualsiasi criticità riscontrata.
- Il dispositivo deve ripristinarsi a uno stato valido conosciuto dopo aver rilevato un BIOS infetto e sostituirlo con una copia sicura.

Integrità del codice firmware

I punti elencati di seguito sono aspetti relativi all'Integrità del codice firmware che dovrebbero essere inclusi come parte delle richieste di preventivo:

- Il dispositivo deve convalidare l'integrità del codice firmware al momento del caricamento e consentire esclusivamente l'esecuzione del firmware sicuro conosciuto.
- Il dispositivo deve inviare notifiche all'amministratore mediante meccanismi di notifica dell'evento standard, tra cui i sistemi SIEM, in relazione a qualsiasi criticità riscontrata.

Rilevamento intrusioni durante l'operatività

I punti elencati di seguito sono aspetti relativi al Rilevamento delle intrusioni durante l'operatività che HP consiglia per la massima sicurezza:

- Il dispositivo deve eseguire un monitoraggio costante in merito agli attacchi malware presenti in memoria.
- Il dispositivo deve inviare notifiche all'amministratore mediante meccanismi di notifica dell'evento standard, tra cui i sistemi SIEM, in relazione a qualsiasi criticità riscontrata.
- Il dispositivo deve interrompere la normale operatività nel momento in cui viene rilevata un'anomalia, riavviandosi in condizioni sicure conosciute.
- L'algoritmo di rilevamento intrusioni deve essere inserito in modo casuale in postazioni differenti nell'immagine codice al fine di prevenirne il rilevamento stesso.

L'algoritmo di rilevamento intrusioni deve essere eseguito di frequente al fine di rilevare attacchi malware prima che tali attacchi compromettano l'integrità del dispositivo.

Garanzia continua sulle impostazioni relative alle policy di sicurezza

La Garanzia continua sulle impostazioni relative alle policy di sicurezza viene largamente eseguita mediante l'uso dello strumento per la conformità della sicurezza. I punti elencati di seguito sono aspetti di uno strumento per la conformità della sicurezza che HP consiglia per la massima sicurezza:

- Lo strumento per la conformità della sicurezza deve rendere conformi le stampanti e le multifunzione risultate non conformi, in base alla policy di sicurezza.
- Lo strumento per la conformità della sicurezza deve eseguire l'inserimento dei dispositivi nuovi o ripristinati e renderli immediatamente conformi alle policy vigenti.
- Lo strumento per la conformità della sicurezza deve includere l'editor Intuitive Security Policy in grado di guidare l'amministratore nella scelta di criteri appropriati, evidenziando possibili dipendenze contrastanti.
- Lo strumento per la conformità della sicurezza deve gestire e installare certificati attraverso un processo automatico in tutto il parco di stampanti e multifunzione.

Analisi e rilevamento minacce in tempo reale

L'Analisi e rilevamento minacce in tempo reale è eseguito principalmente mediante l'uso del sistema di Security Information Event Management (SIEM). I punti elencati di seguito sono aspetti di un sistema SIEM che HP consiglia per la massima sicurezza:

- Il SIEM deve recuperare eventi critici relativi alla sicurezza dalle stampanti.
- Il SIEM deve consentire al Security Analyst di personalizzare report ed avvisi dai messaggi che indicano la presenza di minacce in tempo reale.
- Il SIEM deve integrarsi con altre risorse IT della rete (server, router ecc.) sottoposte al monitoraggio per il rilevamento delle minacce in tempo reale.
- Il SIEM deve trasformare i Big Data in azioni di security intelligence implementabili, avvalendosi di una correlazione in tempo reale combinata con potenti analisi di sicurezza.
- Il SIEM deve rilevare comportamenti inusuali da parte degli utenti e prevenire qualsiasi minaccia che comprometta i dati sensibili.

Dispositivi supportati da FutureSmart e disponibilità delle funzionalità

Nella griglia seguente vengono illustrate le nuove funzionalità di sicurezza integrate che saranno supportate all'interno del parco HP Enterprise FutureSmart, in fase di lancio a partire dal tardo autunno 2015. Tutti i nuovi dispositivi FutureSmart che verranno introdotti sul mercato dall'autunno 2015 in poi supporteranno le 3 nuove funzionalità di sicurezza integrate (HP Sure Start, tecnologia Whitelisting e Rilevamento intrusioni). A causa di limitazioni dell'hardware del dispositivo, alcune funzionalità non saranno supportate su piattaforme più datate.

Categoria RFP		**Meccanismo Secure Boot**	**Integrità del codice firmware**	**Rilevamento intrusioni durante l'operatività**	**Garanzia continua sulle impostazioni relative alle policy di sicurezza**	**Analisi e rilevamento minacce in tempo reale**
Piattaforma dispositivi (include tutti i pacchetti e le opzioni gestite)	Disponibilità della nuova funzionalità di sicurezza incorporata	HP Sure Start	Tecnologia Whitelisting	Rilevamento intrusioni durante l'operatività	HP JetAdvantage Security Manager	Integrazioni HP ArcSight
Multifunzione HP LaserJet Enterprise MFP M527	Autunno 2015	✓	✓	✓	✓	✓
Multifunzione HP Color LaserJet Enterprise M577	Autunno 2015	✓	✓	✓	✓	✓
HP LaserJet Enterprise M506	Autunno 2015	✓	✓	✓	✓	✓
HP Color LaserJet Enterprise M552 e M553	Autunno 2015	✓	✓	✓	✓	✓
HP LaserJet Enterprise M604, M605 e M606	Autunno 2015	✓	✓	✓	✓	✓
Multifunzione HP LaserJet Enterprise 700 MFP M775 a colori	Primavera 2016	⊘	✓	✓	✓	✓
Multifunzione HP LaserJet Enterprise 500 MFP M575 a colori	Primavera 2016	⊘	✓	✓	✓	✓
Multifunzione HP LaserJet Enterprise 500 MFP M525	Primavera 2016	⊘	✓	✓	✓	✓
Multifunzione HP LaserJet Enterprise MFP M725	Primavera 2016	⊘	✓	✓	✓	✓
Multifunzione Flow HP LaserJet Enterprise MFP M830	Primavera 2016	⊘	✓	✓	✓	✓
HP LaserJet Enterprise M806	Primavera 2016	⊘	✓	✓	✓	✓
HP Color LaserJet Enterprise M855	Primavera 2016	⊘	✓	✓	✓	✓
Multifunzione Flow HP Color LaserJet Enterprise MFP M880	Primavera 2016	⊘	✓	✓	✓	✓

Categoria RFP		**Meccanismo Secure Boot**	**Integrità del codice firmware**	**Rilevamento intrusioni durante l'operatività**	**Garanzia continua sulle impostazioni relative alle policy di sicurezza**	**Analisi e rilevamento minacce in tempo reale**
Piattaforma dispositivi (include tutti i pacchetti e le opzioni gestite)	Disponibilità della nuova funzionalità di sicurezza incorporata	HP Sure Start	Tecnologia Whitelisting	Rilevamento intrusioni durante l'operatività	HP JetAdvantage Security Manager	Integrazioni HP ArcSight
Multifunzione HP OfficeJet Enterprise Color MFP X585	Primavera 2016	⊘	✓	✓	✓	✓
HP OfficeJet Enterprise Color X555	Primavera 2016	⊘	✓	✓	✓	✓
HP Color LaserJet Enterprise M651	Primavera 2016	⊘	✓	✓	✓	✓
Multifunzione HP Color LaserJet Enterprise MFP M680	Primavera 2016	⊘	✓	✓	✓	✓
Multifunzione HP LaserJet Enterprise MFP M630	Primavera 2016	⊘	✓	✓	✓	✓
HP LaserJet Enterprise 700 M712	Primavera 2016	⊘	✓	✓	✓	✓
HP Color LaserJet Enterprise M750	Primavera 2016	⊘	✓	✓	✓	✓
HP LaserJet Enterprise 600 M601, M602 e M603	Primavera 2016	⊘	✓	✓	✓	✓
HP LaserJet Enterprise M551 a colori	Primavera 2016	⊘	✓	✓	✓	✓
Multifunzione HP LaserJet Enterprise M4555 MFP	Non supportato	⊘	⊘	⊘	✓	✓
Multifunzione HP Color LaserJet CM4540 MFP	Non supportato	⊘	⊘	⊘	✓	✓
HP LaserJet Enterprise CP5525	Non supportato	⊘	⊘	⊘	✓	✓
HP Digital Sender Flow 8500 fn1	Non supportato	⊘	⊘	⊘	✓	✓
HP ScanJet Enterprise 7000n	Non supportato	⊘	⊘	⊘	✓	⊘

[1] Potrebbe essere necessario un aggiornamento dei service pack FutureSmart per attivare le funzionalità di sicurezza.

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

Condividi con i colleghi

4AA6-3571ITE, dicembre 2015