Livre blanc technique

Considérations de sécurité d'impression intégrées

Aspects importants de la sécurité à prendre en compte lors de l'évaluation des imprimantes

Table des matières

La sécurité des appareils d'impression et d'imagerie est souvent négligée

Les responsables informatiques se voient constamment confier la tâche de protéger des informations confidentielles, y compris l'identité des employés et les données des clients, sur plusieurs dispositifs. Face à la nécessité de répondre aux besoins de nombreuses personnes ayant différents modes de travail dans l'ensemble de l'organisation, les menaces pour la sécurité non anticipées constituent un défi permanent.

Bien que de nombreux départements informatiques appliquent rigoureusement des mesures de sécurité aux ordinateurs individuels et au réseau d'entreprise, les périphériques d'imagerie et d'impression sont souvent négligés et vulnérables. Les menaces pour la sécurité sont réelles, cependant. À mesure que les appareils d'impression et d'imagerie deviennent de plus en plus élaborés et interconnectés avec davantage d'appareils mobiles et de terminaison, les imprimantes deviennent des vecteurs d'attaque potentiels pour les pirates qui cherchent à compromettre l'appareil ou l'intégralité du réseau.

Cinq domaines clés de la sécurité de l'impression

Le but du présent document est de fournir non seulement une structure, mais aussi des aspects très spécifiques de la sécurité de l'impression que vous devriez prendre en compte lors de l'achat, du déploiement ou de l'utilisation des solutions d'impression. Les imprimantes HP FutureSmart qui prennent en charge les quatre principales fonctions de sécurité (HP Sure Start, liste blanche, détection des intrusions à l'exécution et HP Connection Inspector) remplissent tous les critères dans chacune des sections (lorsqu'elles sont associées à HP JetAdvantage Security Manager et à des outils de gestion des événements et informations de sécurité tels que ArcSight, Splunk, SIEMonster ou McAfee).[1] Les appareils FutureSmart qui ne prennent pas en charge HP Sure Start satisfont à tous les critères sauf ceux listés dans le processus de démarrage sécurisé. Voir le tableau des dispositifs en pages 4 et 5 pour les informations relatives à la compatibilité des dispositifs de sécurité.

Vous devez vous concentrer sur six domaines essentiels de la sécurité des imprimantes :

1. Processus de démarrage sécurisé
2. Intégrité du code du micrologiciel
3. Détection d'intrusion pendant l'exécution
4. Détection d'anomalies de comportement du réseau
5. Assurance permanente des paramètres de la politique de sécurité
6. Analyse et détection des menaces en temps réel

Processus de démarrage sécurisé

Les éléments suivants sont des aspects du processus de démarrage sécurisé que HP recommande pour une sécurité optimale :

- Au démarrage, le dispositif doit valider l'intégrité du BIOS.
- Le dispositif doit « auto-réparer » un BIOS infecté en le remplaçant par une copie garantie authentique du BIOS protégée par le matériel.
- Le dispositif doit informer l'administrateur de tous les problèmes via les mécanismes d'évènements standard, y compris les systèmes de gestion des événements et informations de sécurité (SIEM).
- Le dispositif doit revenir à un état fonctionnel connu après la détection d'un BIOS infecté et son remplacement par une copie garantie authentique.

Intégrité du code du micrologiciel

Les éléments suivants sont des aspects de l'intégrité du code du micrologiciel que HP recommande pour une sécurité optimale :

- Le dispositif doit valider l'intégrité du code du micrologiciel pendant le temps de chargement et permettra uniquement au micrologiciel correct de s'exécuter.
- Le dispositif doit informer l'administrateur de tous les problèmes via les mécanismes d'évènements standard, y compris les systèmes de gestion des événements et informations de sécurité (SIEM).

Détection d'intrusion pendant l'exécution

Les éléments suivants sont des aspects de la détection des intrusions à l'exécution que HP recommande pour une sécurité optimale :

- Le dispositif doit fournir un contrôle permanent pour les attaques par injection de logiciels malveillants en mémoire.
- Le dispositif doit informer l'administrateur de tous les problèmes via les mécanismes d'évènements standard, y compris les systèmes de gestion des événements et informations de sécurité (SIEM).
- Le dispositif doit interrompre le fonctionnement normal lorsqu'une anomalie est détectée et redémarrer à un état correct antérieur.
- L'algorithme de détection des intrusions doit être inséré au hasard en différents endroits dans l'image du code pour prévenir sa propre détection.
- L'algorithme de détection des intrusions doit s'exécuter suffisamment fréquemment pour détecter l'injection de logiciels malveillants avant qu'un logiciel malveillant ne puisse compromettre l'intégrité du dispositif.

Détection d'anomalies de comportement du réseau

Les éléments suivants sont des aspects de la détection d'anomalies de comportement du réseau que HP recommande pour une sécurité optimale :

- Le dispositif doit assurer une surveillance permanente des anomalies de comportement du réseau.
- Le dispositif doit informer l'administrateur de tous les problèmes via les mécanismes d'évènements standard, y compris les systèmes de gestion des événements et informations de sécurité (SIEM).
- Le dispositif doit interrompre le fonctionnement normal lorsqu'une anomalie est détectée et redémarrer à un état correct antérieur.

Assurance permanente des paramètres de la politique de sécurité

La garantie permanente des paramètres de politique de sécurité est assurée en grande partie par l'utilisation d'un outil de mise en conformité de la sécurité. Les éléments suivants sont des aspects de l'outil de mise en conformité de la sécurité que HP recommande pour une sécurité optimale.

- L'outil de mise en conformité de la sécurité doit mettre en conformité les imprimantes/multifonctions qui ne le sont pas, en se basant sur la politique de sécurité.
- L'outil de mise en conformité de la sécurité doit faire en sorte que les dispositifs nouveaux ou réinitialisés sur le réseau s'annoncent et soient immédiatement mis en conformité.
- L'outil de mise en conformité de la sécurité doit inclure un éditeur de la politique de sécurité qui guide l'administrateur lors de la sélection des paramètres appropriés en signalant les dépendances conflictuelles.
- L'outil de mise en conformité de la sécurité doit gérer et installer des certificats avec un processus automatisé via un parc d'imprimantes/multifonctions.

Analyse et détection des menaces en temps réel

L'analyse et détection des menaces en temps réel s'effectue principalement avec un système de gestion des événements et informations de sécurité (SIEM). Les éléments suivants sont des aspects du système SIEM que HP recommande pour une sécurité optimale :

- Le SIEM doit récupérer les événements critiques de sécurité des imprimantes.
- Le SIEM doit autoriser les analyses de sécurité à personnaliser les rapports et les alertes à partir de messages indiquant les alertes en temps réel.
- Le SIEM doit s'intégrer à d'autres actifs informatiques (serveurs, routeurs, etc.) qui sont contrôlés pour la détection des menaces en temps réel.
- Le SIEM doit transformer les données volumineuses en renseignements de sécurité permettant d'engager une action sur la base d'une corrélation en temps réel associée à une puissante analyse de la sécurité.
- Le SIEM doit repérer le comportement anormal des utilisateurs et prévenir les menaces envers les données sensibles.

Dispositifs FutureSmart compatibles et disponibilité de la fonctionnalité

La matrice suivante montre comment les fonctionnalités de sécurité intégrées sont prises en charge à l'échelle du parc HP Enterprise FutureSmart. La totalité des dispositifs FutureSmart lancés après l'automne 2015 prennent en charge les quatre fonctions de sécurité intégrées. (HP Sure Start, liste blanche, détection des intrusions pendant l'exécution et HP Connection Inspector). La pérennisation de l'investissement apportée par le micrologiciel HP FutureSmart vous permet d'ajouter certaines de ces fonctionnalités à des modèles d'imprimantes HP Enterprise spécifiques. En raison des limitations matérielles du dispositif, certaines fonctionnalités ne seront pas supportées sur certaines plates-formes plus anciennes.

Catégorie de l'appel d'offres	Assurance permanente des paramètres de la politique de sécurité HP Security Manager	Analyse et détection des menaces en temps réel Intégration avec les outils SIEM	Intégrité du code du micrologiciel Liste blanche	Détection d'intrusion pendant l'exécution Détection d'intrusion pendant l'exécution	Détection d'anomalies de comportement du réseau HP Connection Inspector	Processus de démarrage sécurisé Protection du BIOS HP Sure Start
Multifonctions						
HP LaserJet Enterprise 500 M525	✓	✓	✓	✓	✓	⊘
HP LaserJet Enterprise M527	✓	✓	✓	✓	✓	✓
HP LaserJet Enterprise 500 couleur M575	✓	✓	✓	✓	✓	⊘
HP Color LaserJet Enterprise M577	✓	✓	✓	✓	✓	✓
HP LaserJet Enterprise M630	✓	✓	✓	✓	✓	⊘
HP LaserJet Enterprise M631, M632 et M633	✓	✓	✓	✓	✓	✓
HP Color LaserJet Enterprise M652, M653	✓	✓	✓	✓	✓	✓
HP Color LaserJet Enterprise M680	✓	✓	✓	✓	✓	⊘
HP Color LaserJet Enterprise Flow M681-M682	✓	✓	✓	✓	✓	✓
HP LaserJet Managed E62550-E62560-E62570	✓	✓	✓	✓	✓	✓
HP Color LaserJet Managed E67550-E67560	✓	✓	✓	✓	✓	✓
HP LaserJet Enterprise M725	✓	✓	✓	✓	✓	⊘
HP LaserJet Enterprise 700 couleur M775	✓	✓	✓	✓	✓	⊘
HP LaserJet Enterprise Flow M830z	✓	✓	✓	✓	✓	⊘
HP Color LaserJet Enterprise Flow M880z	✓	✓	✓	✓	✓	⊘
HP PageWide Enterprise Color M586	✓	✓	✓	✓	✓	✓
HP PageWide Enterprise Color 780, 785	✓	✓	✓	✓	✓	✓
HP PageWide Managed Color P77440dn	✓	✓	✓	✓	✓	✓
HP PageWide Managed P77940-P77950-P77960	✓	✓	✓	✓	✓	✓
HP PageWide Managed E77650-E77660	✓	✓	✓	✓	✓	✓
HP LaserJet Managed E72520-E72540	✓	✓	✓	✓	✓	✓
HP Color LaserJet Managed E77820-E77830	✓	✓	✓	✓	✓	✓
HP LaserJet Managed E82540-E82560	✓	✓	✓	✓	✓	✓
HP Color LaserJet Managed E87640-E87660	✓	✓	✓	✓	✓	✓

Catégorie de l'appel d'offres	Assurance permanente des paramètres de la politique de sécurité HP Security Manager	Analyse et détection des menaces en temps réel Intégration avec les outils SIEM	Intégrité du code du micro-logiciel Liste blanche	Détection d'intrusion pendant l'exécution Détection d'intrusion pendant l'exécution	Détection d'anomalies de comportement du réseau HP Connection Inspector	Processus de démarrage sécurisé Protection du BIOS HP Sure Start
Appareils monofonctions						
HP LaserJet Enterprise M506	✓	✓	✓	✓	✓	✓
HP LaserJet Enterprise 500 Color M551	✓	✓	✓	✓	✓	⊘
HP Color LaserJet Enterprise 500 M552dn	✓	✓	✓	✓	✓	✓
HP Color LaserJet Enterprise M553	✓	✓	✓	✓	✓	✓
HP LaserJet Enterprise 600 M601, M602, M603	✓	✓	✓	✓	✓	⊘
HP LaserJet Enterprise M604, M605, M606	✓	✓	✓	✓	✓	✓
HP LaserJet Enterprise M607, M608, M609	✓	✓	✓	✓	✓	✓
HP Color LaserJet Enterprise M651	✓	✓	✓	✓	✓	⊘
HP LaserJet Managed E60055-E60065-E60075	✓	✓	✓	✓	✓	✓
HP Color LaserJet Managed E65050-E65060	✓	✓	✓	✓	✓	✓
HP LaserJet Enterprise 700 M712	✓	✓	✓	✓	✓	⊘
HP Color LaserJet Enterprise M750	✓	✓	✓	✓	✓	⊘
HP LaserJet Enterprise M806	✓	✓	✓	✓	✓	⊘
HP Color LaserJet Enterprise M855	✓	✓	✓	✓	✓	⊘
HP OfficeJet Enterprise Color X555	✓	✓	✓	✓	✓	⊘
HP PageWide Enterprise Color 556	✓	✓	✓	✓	✓	✓
HP PageWide Enterprise Color 765dn	✓	✓	✓	✓	✓	✓
HP PageWide Managed Color P75250dn	✓	✓	✓	✓	✓	✓
HP PageWide Managed Color E75160dn	✓	✓	✓	✓	✓	✓
HP Officejet Enterprise Color X585	✓	✓	✓	✓	✓	⊘
Scanners						
HP Digital Sender Flow 8500 fn2	✓	✓	✓	✓	✓	✓
HP ScanJet Enterprise Flow N9120 fn2	✓	✓	✓	✓	✓	✓

En savoir plus
hp.com/printersthatprotect

[1] La mise à jour par installation d'un Service Pack HP FutureSmart pourra être nécessaire pour activer ces fonctionnalités de sécurité.

Abonnez-vous pour les mises à jour
hp.com/go/getupdated

Partager avec des collègues

4AA6-3571FRE, mars 2018, rév. 1