Technisches Whitepaper

Hinweise zur Druckersicherheit

Wichtige Sicherheitsaspekte im Hinblick auf die Bewertung von Drucklösungen

Inhalt

Unsichere Druck- und Bildbearbeitungsgeräte sind die Regel

Die IT sieht sich ständig mit der Herausforderung konfrontiert, die Sicherheit vertraulicher Informationen, darunter die persönlichen Daten von Mitarbeitern sowie Kundendaten, auf den verschiedenen im Unternehmen genutzten Geräten gewährleisten zu müssen. Dabei ist zu berücksichtigen, dass sich aus der Anforderung, einer Vielzahl von im ganzen Unternehmen verteilten Mitarbeitern und deren unterschiedlichen Arbeitsweisen gerecht zu werden, eine kontinuierliche Bedrohung für die IT-Sicherheit ergibt.

Auch wenn viele IT-Abteilungen mittlerweile strenge Sicherheitsmaßnahmen durchgesetzt haben, um einzelne Computer und das Unternehmensnetzwerk zu schützen, fallen die Druck- und Bildbearbeitungsgeräte oft durch das Raster und stellen so ein Sicherheitsrisiko dar. Die Gefahren für die Sicherheit sind allerdings real und mit dem steigenden Funktionsumfang von Druckern und Bildbearbeitungsgeräten bieten sich Hackern immer mehr Möglichkeiten, um entweder das Gerät selbst oder das gesamte Netzwerk anzugreifen.

Fünf wichtige Bereiche der Druckersicherheit

Mit diesem Dokument möchten wir Ihnen nicht nur einen Überblick vermitteln, sondern auch konkret einzelne Aspekte der Druckersicherheit ansprechen, die Sie beim Kauf, bei der Implementierung oder bei der Verwendung von Druckern und Drucklösungen berücksichtigen sollten. HP Drucker mit Unterstützung für die im Herbst 2015 vorgestellten „Big 3“ der Sicherheitsfunktionen (HP Sure Start, Whitelisting und Erkennung von Runtime-Angriffsversuchen) erfüllen alle Kriterien in den jeweiligen Bereichen (wenn in Kombination mit JetAdvantage Security Manager und ArcSight verwendet).[1] Geräte mit FutureSmart, die HP Sure Start nicht unterstützen, erfüllen alle Kriterien, mit Ausnahme der in Abschnitt 1 genannten (Sicherer Systemstart). Detaillierte Angaben zur Unterstützung der Sicherheitsfunktionen finden Sie in der nachstehenden Gerätetabelle.

Sie sollten sich auf fünf zentrale Bereiche der Druckersicherheit konzentrieren:

1. Sicherer Systemstart
2. Integrität des Firmware-Codes
3. Erkennung von Runtime-Angriffsversuchen
4. Kontinuierliche Durchsetzung von Sicherheitsrichtlinien
5. Erkennen und Analysieren von Bedrohungen in Echtzeit

Sicherer Systemstart

Die folgenden Punkte sind wichtige Aspekte für einen sicheren Systemstart, die HP empfiehlt, um ein Höchstmaß an Sicherheit zu erreichen:

- Beim Systemstart muss ein Gerät die Integrität des BIOS überprüfen.
- Das Gerät muss in der Lage sein, ein infiziertes BIOS selbst zu reparieren, indem es dieses durch eine hardwaregeschützte Golden Copy des BIOS ersetzt.
- Bei Problemen muss das Gerät den Administrator mittels eines Standardmechanismus für Vorfälle, beispielsweise eines SIEM-Systems, benachrichtigen können.
- Das Gerät muss in der Lage sein, nach Identifizierung einer BIOS-Infektion dieses durch eine Golden Copy zu ersetzen und einen bekannten, sicheren Systemstatus wiederherzustellen.

Integrität des Firmware-Codes

Die folgenden Punkte sind wichtige Aspekte für die Integrität des Firmware-Codes und sollten daher in der Ausschreibung erwähnt werden:

- Das Gerät muss die Integrität des Firmware-Codes beim Laden überprüfen können und darf nur die Ausführung einer erwiesenermaßen sicheren Firmware zulassen.
- Bei Problemen muss das Gerät den Administrator mittels eines Standardmechanismus für Vorfälle, beispielsweise eines SIEM-Systems, benachrichtigen können.

Erkennung von Runtime-Angriffsversuchen

Die folgenden Punkte sind wichtige Aspekte für die Erkennung von Runtime-Angriffsversuchen, die HP empfiehlt, um ein Höchstmaß an Sicherheit zu erreichen:

- Das Gerät muss über eine fortlaufende Überwachungsfunktion verfügen, die Angriffe durch das Einschleusen von Malware in den Speicher erkennt.
- Bei Problemen muss das Gerät den Administrator mittels eines Standardmechanismus für Vorfälle, beispielsweise eines SIEM-Systems, benachrichtigen können.
- Bei Erkennung einer Abweichung muss das Gerät den Betrieb unterbrechen und einen Neustart durchführen, um den korrekten Betriebszustand wiederherzustellen.
- Der Algorithmus zur Erkennung von Angriffsversuchen muss per Zufallsprinzip über den gesamten Code verteilt sein, um ihn so vor einer Erkennung durch die Schadsoftware zu schützen.

Der Algorithmus zur Erkennung von Angriffsversuchen muss in so regelmäßigen Abständen ausgeführt werden, dass er das Einschleusen von Malware erkennt, bevor diese die Integrität des Geräts beeinträchtigen kann.

Kontinuierliche Durchsetzung von Sicherheitsrichtlinien

Die kontinuierliche Durchsetzung von Sicherheitsrichtlinien erfolgt primär mittels eines Compliance-Tools für die Sicherheit. Die folgenden Punkte sind wichtige Aspekte eines Compliance-Tools für die Sicherheit, das HP empfiehlt, um ein Höchstmaß an Sicherheit zu erreichen:

- Das Compliance-Tool für die Sicherheit muss anhand der Sicherheitsrichtlinien die Compliance von Druckern bzw. MFPs wiederherstellen, falls deren Sicherheit beeinträchtigt ist.
- Das Compliance-Tool für die Sicherheit muss dafür sorgen, dass neue oder zurückgesetzte Geräte sich im Netzwerk melden, um sofort deren Compliance gewährleisten zu können.
- Das Compliance-Tool für die Sicherheit muss über einen intuitiven Editor für Sicherheitsrichtlinien verfügen und Konflikte bei Abhängigkeiten anzeigen, damit der Administrator die geeigneten Richtlinieneinstellungen vornehmen kann.
- Das Compliance-Tool für die Sicherheit muss über Funktionen zur automatischen Verwaltung und Installation von Zertifikaten in der gesamten Druckerflotte verfügen.

Erkennen und Analysieren von Bedrohungen in Echtzeit

Das Erkennen und Analysieren von Bedrohungen in Echtzeit erfolgt hauptsächlich über das Security Information Event Management (SIEM) System. Die folgenden Punkte sind wichtige Aspekte für ein SIEM-System, die HP empfiehlt, um ein Höchstmaß an Sicherheit zu erreichen:

- Das SIEM muss wichtige, sicherheitsrelevante Vorfälle vom Drucker abfragen.
- Das SIEM muss dem Sicherheitsanalysten die Anpassung von Berichten und Alarmen bei Meldungen gestatten, die auf in Echtzeit auftretende Bedrohungen aufmerksam machen.
- Das SIEM muss sich in andere vernetzte IT-Assets (Server, Router usw.) integrieren lassen, die zwecks der Erkennung von Bedrohungen in Echtzeit kontinuierlich überwacht werden.
- Das SIEM muss Big Data in verwertbare Sicherheitsintelligenz umwandeln, indem es Echtzeit-Korrelation in Kombination mit leistungsstarken Sicherheitsanalysen verwendet.
- Das SIEM muss ungewöhnliches Benutzerverhalten erkennen und so eine Bedrohung für vertrauliche Daten verhindern können.

Unterstützte Geräte mit FutureSmart und Verfügbarkeit von Funktionen

Die nachstehende Matrix zeigt, welche neuen integrierten Sicherheitsfunktionen von welchen HP Enterprise FutureSmart Geräten ab Ende Herbst 2015 unterstützt werden. Alle nach Herbst 2015 ausgelieferten FutureSmart Geräte unterstützen die 3 neuen integrierten Sicherheitsfunktionen. (HP Sure Start, Whitelisting und Erkennung von Angriffsversuchen). Aufgrund der eingeschränkten Hardwaretauglichkeit werden manche Funktionen von bestimmten älteren Plattformen nicht mehr unterstützt.

Kategorie der Ausschreibung		**Sicherer Systemstart**	**Integrität des Firmware-Codes**	**Erkennung von Runtime-Angriffsversuchen**	**Kontinuierliche Durchsetzung von Sicherheitsrichtlinien**	**Erkennen und Analysieren von Bedrohungen in Echtzeit**
Geräteplattform (darunter alle Paketangebote und verwalteten Optionen)	Verfügbarkeit der neuen integrierten Sicherheitsfunktion	HP Sure Start	Whitelisting	Erkennung von Runtime-Angriffsversuchen	HP JetAdvantage Security Manager	HP ArcSight-Integration
HP LaserJet Enterprise MFP M527	Herbst 2015	✓	✓	✓	✓	✓
HP Color LaserJet Enterprise M577	Herbst 2015	✓	✓	✓	✓	✓
HP LaserJet Enterprise M506	Herbst 2015	✓	✓	✓	✓	✓
HP Color LaserJet Enterprise M552 und M553	Herbst 2015	✓	✓	✓	✓	✓
HP LaserJet Enterprise M604, M605 und M606	Herbst 2015	✓	✓	✓	✓	✓
HP LaserJet Enterprise 700 Color MFP M775	Frühling 2016	⊘	✓	✓	✓	✓
HP LaserJet Enterprise 500 Color MFP M575	Frühling 2016	⊘	✓	✓	✓	✓
HP LaserJet Enterprise 500 MFP M525	Frühling 2016	⊘	✓	✓	✓	✓
HP LaserJet Enterprise MFP M725	Frühling 2016	⊘	✓	✓	✓	✓
HP LaserJet Enterprise Flow MFP M830	Frühling 2016	⊘	✓	✓	✓	✓
HP LaserJet Enterprise M806	Frühling 2016	⊘	✓	✓	✓	✓
HP Color LaserJet Enterprise M855	Frühling 2016	⊘	✓	✓	✓	✓
HP Color LaserJet Enterprise Flow MFP M880	Frühling 2016	⊘	✓	✓	✓	✓
HP OfficeJet Enterprise Color MFP X585	Frühling 2016	⊘	✓	✓	✓	✓
HP OfficeJet Enterprise Color X555	Frühling 2016	⊘	✓	✓	✓	✓

Kategorie der Ausschreibung		Sicherer Systemstart	Integrität des Firmware-Codes	Erkennung von Runtime-Angriffsver-suchen	Kontinuierliche Durchsetzung von Sicher-heitsrichtlinien	Erkennen und Analysieren von Bedrohungen in Echtzeit
Geräteplattform (darunter alle Paketangebote und verwalteten Optionen)	Verfügbarkeit der neuen integrierten Sicherheits-funktion	HP Sure Start	Whitelisting	Erkennung von Runtime-Angriffsver-suchen	HP JetAdvantage Security Manager	HP ArcSight-Integration
HP Color LaserJet Enterprise M651	Frühling 2016	⊘	✓	✓	✓	✓
HP Color LaserJet Enterprise MFP M680	Frühling 2016	⊘	✓	✓	✓	✓
HP LaserJet Enterprise MFP M630	Frühling 2016	⊘	✓	✓	✓	✓
HP LaserJet Enterprise 700 M712	Frühling 2016	⊘	✓	✓	✓	✓
HP Color LaserJet Enterprise M750	Frühling 2016	⊘	✓	✓	✓	✓
HP LaserJet Enterprise 600 M601, M602 und M603	Frühling 2016	⊘	✓	✓	✓	✓
HP LaserJet Enterprise Color M551	Frühling 2016	⊘	✓	✓	✓	✓
HP LaserJet Enterprise M4555 MFP	Nicht unterstützt	⊘	⊘	⊘	✓	✓
HP Color LaserJet CM4540 MFP	Nicht unterstützt	⊘	⊘	⊘	✓	✓
HP LaserJet Enterprise CP5525	Nicht unterstützt	⊘	⊘	⊘	✓	✓
HP Digital Sender Flow 8500 fn1	Nicht unterstützt	⊘	⊘	⊘	✓	✓
HP ScanJet Enterprise 7000n	Nicht unterstützt	⊘	⊘	⊘	✓	⊘

[1] Möglicherweise ist ein FutureSmart Service-Pack-Update erforderlich, um die Sicherheitsfunktionen zu aktivieren.

Melden Sie sich noch heute an.
hp.com/go/getupdated

An Kollegen weiterleiten

4AA6-3571DEE, Dezember 2015