Broschüre

Helfen Sie Ihren Kunden, die Sicherheit ihrer Druckumgebung zu verbessern

Viele Organisationen haben eine Sicherheitsstrategie für ihre Netzwerke und Endgeräte implementiert, einschließlich strenger Maßnahmen für die PC-Sicherheit. Allerdings bleiben Drucker und Bildbearbeitungsgeräte bei der Gesamtstrategie für die Sicherheit häufig unberücksichtigt. Doch wenn Drucker und MFPs nur unzureichend geschützt werden, können auch diese Geräte Sicherheitsrisiken ausgesetzt sein. Unternehmen sollten die Sicherheitsanforderungen ihrer Bildbearbeitungs- und Druckumgebung in ihre Gesamtstrategie für die IT-Sicherheit aufnehmen.

HP LaserJet Drucker und MFPs weisen rund 200 verschiedene Sicherheitsfunktionen auf, die Ihre Kunden aktivieren können, um deren Geräte und Daten zu schützen. Dank moderner Technologien lässt sich ein ausgewogenes Verhältnis zwischen Nutzbarkeit und Sicherheit erzielen. Da jedes Unternehmen einzigartig ist, sind HP Drucker und MFPs werksseitig so ausgestattet, dass sie die Anforderungen unterschiedlichster Benutzer erfüllen können. Allerdings kann die Vielzahl der Einstellungen Unternehmen auch vor Herausforderungen stellen.

Dieser Leitfaden unterstützt Sie dabei, sich mit einigen der grundlegenden Geräteeinstellungen vertraut zu machen, die alle Unternehmen unabhängig von Größe oder Branche implementieren sollten, um die Bildbearbeitungsgeräte und Drucker in ihren Netzwerken zu schützen. Mit Erläuterungen zu den einzelnen Einstellungen und Risiken, die bestehen, wenn diese nicht aktiviert werden, können Sie Ihren Kunden den Einstieg bei der Entwicklung einer Sicherheitsstrategie für ihre Bildbearbeitungs- und Druckumgebung erleichtern.

Empfohlene Geräteeinstellungen für HP Druckerflotten

Ihre Kunden benötigen möglicherweise Hilfe bei der Ermittlung der Sicherheitseinstellungen, die sie zum Schutz ihrer Daten in Betracht ziehen sollten. Wir haben die möglichen Geräteeinstellungen auf 200 Konfigurationseinstellungen eingegrenzt. Dies sind die grundlegenden Sicherheitseinstellungen, die alle Unternehmen unabhängig von ihrer Größe und Branche in Betracht ziehen sollten. HP empfiehlt, mindestens diese Sicherheitseinstellungen fe stzulegen, um den häufigsten Sicherheitsproblemen zu begegnen.

Es sollte unbedingt beachtet werden, dass jede Kundenumgebung einzigartig ist. Jeder Kunde muss für sich das richtige Verhältnis z wischen Sicherheit und Endbenutzerproduktivität finden. Bei der Konfiguration eines MFPs für ein Netzwerk müssen möglicherweise Anpassungen vorgenommen werden – Ihre Kunden müssen abwägen, welche Konfiguration sich für ihre Netzwerkumgebung eignet.

Potenzielle Folgen bei ungeschützten Geräten:

- Verlust von Mitarbeiterproduktivität, weil die Geräteeinstellungen geändert wurden und die Benutzer nicht mehr drucken, kopieren, scannen oder faxen können
- Nicht autorisierter Zugriff auf sensible Daten
- Potenzielle Offenlegung von Geräteeinstellungen, einschließlich der Anmeldeinformationen
- Mehr Anrufe beim Support, die die IT-Abteilung wertvolle Zeit kosten

Vorab sollten Sie den Kunden Folgendes empfehlen:

- Sie sollten ein Upgrade der Geräte auf die neueste Firmware-Version durchführen, um sicherzustellen, dass die Geräte über die neuesten Funktionen verfügen.
- Sie sollten sicherstellen, dass sich die Drucker oder MFPs hinter ihrer Firewall befinden, damit sie geschützt sind. Einige HP Lösungen erfordern, dass die Geräte mit dem Internet verbunden sind, damit die Funktionen ordnungsgemäß genutzt werden können.

Zu vermeidendes Risiko	Sicherheitseinstellungen	Maßnahme	Zweck der Einstellung
Jeder kann die Geräteeinstellungen oder die Funktionen der Tasten auf dem Bedienfeld ändern (z. B. um Produktfunktionen zu deaktivieren).	Administratorpasswort für HP Embedded Web Server (EWS)	Passwort einrichten	Steuert den Zugriff auf die Konfigurationsparameter des HP EWS.
Jeder kann die Einstellungen des Bedienfelds ändern.	Printer Job Language-Passwort (PJL)	Passwort einrichten	PJL-Befehle ermöglichen eine Zwei-Wege-Kommunikation mit dem Drucker und können genutzt werden, um die Bedienfeldeinstellungen zu ändern.
Jeder kann die Einstellungen am Drucker ändern, wenn der SNMPv1/v2-Schreibzugriff aktiviert ist.	SNMPv1/v2 Simple Network Management Protocol	Lesezugriff einstellen	Diese Einstellungen bieten Unterstützung für ältere Verwaltungstools, die für die Geräteerkennung und für den Abruf des Gerätestatus auf SNMPv1/v2 angewiesen sind.
Jeder kann ein Gerät im Netzwerk erkennen und dessen Einstellungen ändern, wenn SNMPv3 nicht aktiviert wird.	SNMPv3	Aktivieren, Konto auf dem Gerät erstellen	SNMPv3 verwendet ein benutzerbasiertes Sicherheitsmodell, dass Authentifizierung und Datenschutz durch Verschlüsselung bietet. Sicherere Methode als SNMPv1/v2.
Jeder kann die Firmware aktualisieren, auf eine weniger sichere Version zurücksetzen und so die Funktionalität vorhandener Lösungen beeinträchtigen.	FTP-Firmware-Update	Deaktivieren	Eine Methode zum Aktualisieren der Firmware auf einem Gerät per Fernzugriff.
Jeder kann die Firmware per Fernzugriff aktualisieren, auf eine weniger sichere Version zurücksetzen und so vorhandene Lösungen beeinträchtigen.	Remote Firmware Upgrade (RFU)	Deaktivieren Hinweis: Aktivieren Sie die Option, wenn Sie Firmware per Fernzugriff aktualisieren möchten, und deaktivieren Sie sie anschließend wieder.	Eine weitere Methode zum Aktualisieren der Firmware auf einem Gerät per Fernzugriff.
Jemand könnte den Netzwerkdatenverkehr ausspähen und Daten einsehen, wenn diese nicht verschlüsselt werden.	HTTPS-Redirect erfordern	Aktivieren	Verschlüsselt Daten bei der Übertragung vom Gerät zum Computer, wenn zum integrierten Webserver des Geräts navigiert wird.
Nicht autorisierte Personen können auf Geräte zugreifen und Änderungen an den Gerätekonfigurationen vornehmen, wenn Protokolle aktiviert bleiben.	Nicht benötigte Protokolle deaktivieren • Telnet • File Transfer Protocol (FTP) • Novell (IPX/SPX) • Appletalk	Deaktivieren	Diese Protokolle ermöglichen das Senden oder Empfangen von Informationen von einem Netzwerkgerät. Üblicherweise werden nicht benötigte Protokolle für Legacy-Anwendungen beibehalten.
Benutzer könnten so auf Dateien zugreifen und diese verändern, als wären sie lokal auf ihrer eigenen Festplatte gespeichert.	Dateizugriff verhindern • Network File Systems • Printer Management Language • Printer Job Language • Postscript	Deaktivieren, alle Kontrollkästchen aktivieren	Ermöglicht es allen Benutzern im Netzwerk, per Fernzugriff auf Dateien zuzugreifen, die sich auf der Festplatte eines Druckers befinden.

Sicherheitsrichtlinien lassen sich problemlos für ganze Druckerflotten mit HP Geräten anwenden

Annähernd 90 %

der Unternehmen geben an, dass sie mindestens einen Fall von Datenverlust aufgrund von ungeschützten Druckern erlebt haben.[1]

65 %

der Verstöße gegen die Datensicherheit passieren versehentlich, durch die Unachtsamkeit von Mitarbeitern oder durch Fehler in den IT- oder Geschäftsabläufen.[2]

7,6 Mio. $ insgesamt

Die Kosten einer einzigen Sicherheitslücke belaufen sich im Durchschnitt auf 136 US-Dollar pro entwendetem Datensatz und insgesamt auf 7,6 Mio. US-Dollar.[2]

Warum Sicherheitsrichtlinien wichtig sind

Ihre Kunden erstellen ständig wertvolle vertrauliche Daten, die für ihr Geschäft unverzichtbar sind. Sie nutzen vermutlich bereits diverse Sicherheitsverfahren – beispielsweise Authentifizierung, Verschlüsselung und Überwachung – um diese Daten in Netzwerken und auf PCs und Servern zu schützen. Aber ist ihre Druck- und Bildbearbeitungsumgebung genau so sicher wie ihre übrige Infrastruktur?

Sicherheitslücken können zur Folge haben, dass vertrauliche Daten offengelegt werden:

- Bildbearbeitungsgeräte und Drucker speichern Dateien auf internen Laufwerken oder Festplatten, sodass auch unbefugte Benutzer auf vertrauliche Informationen auf diesen Medien zugreifen können.
- Mit Multifunktionsgeräten können Druckaufträge einfach erfasst und an unterschiedlichste Ziele weitergeleitet werden. Auf diese Weise können möglicherweise vertrauliche Daten offengelegt werden.

Sicherheitseinstellungen sind möglicherweise nicht aktuell oder erfüllen nicht die Sicherheitsvorschriften:

- In einigen Ländern drohen Unternehmen Geldstrafen, wenn ihre Sicherheitseinstellungen gegen die Sicherheitsvorschriften verstoßen.

Mithilfe der grundlegenden Sicherheitseinstellungen auf Seite 2 können Sie Ihren Kunden den Einstieg bei der Entwicklung einer Sicherheitsstrategie für ihre Bildbearbeitungs- und Druckumgebung erleichtern.

Leitfragen

Um die Anforderungen Ihrer Kunden zu bewerten, sollten Sie zunächst Fragen zu ihren Arbeitsumgebungen klären, wie beispielsweise:

- Welche IT-Sicherheitsrichtlinien sind bei Ihnen zurzeit implementiert?
- Gelten Ihre Sicherheitsrichtlinien auch für Bildbearbeitungsgeräte und Drucker?
- Sind Sie sich darüber im Klaren, dass Ihre Netzwerkdrucker eine Schwachstelle sein können?
- Wissen Sie, wie Sie diese Sicherheitseinstellungen auf Ihren Geräten festlegen können?
- Wissen Sie, dass HP eine Lösung anbietet, die es Ihnen ermöglicht, eine Sicherheitsrichtlinie zu erstellen und diese für alle Geräte Ihrer Flotte anzuwenden?

HP JetAdvantage Security Manager

HP JetAdvantage Security Manager ist ein leistungsstarkes Tool zum Erstellen und Bearbeiten flottenweiter Sicherheitsrichtlinien für HP Drucker und Bildbearbeitungsgeräte.[3] Mit dem HP Security Manager lässt sich höchste Sicherheit erzielen, ohne dass die Administratoren Sicherheitsexperten sein müssen.

Mit dem Embedded Web Server (EWS) können einzelne Druckgeräte geschützt werden. Das Tool ist jedoch unpraktisch, wenn eine ganze Flotte geschützt werden muss. Die Verwaltung von Sicherheitseinstellungen für eine ganze Flotte muss nicht verwirrend oder zeitraubend sein. Den häufigsten Sicherheitsproblemen lässt sich begegnen, indem mindestens die von HP empfohlenen und auf Seite 2 aufgeführten Sicherheitseinstellungen festgelegt werden. Es handelt sich dabei um eine Auswahl der Einstellungen, die zu der Basisrichtlinie des HP Security Manager gehören.

Sobald Ihre Kunden beginnen, ihr Druckernetzwerk aktiv zu schützen, können eigene Sicherheitsrichtlinien eingerichtet und später weitere Einstellungen ergänzt werden. Durch die Verwendung von HP JetAdvantage Security Manager und Instant-On-fähigen Geräten können Ihre Kunden wichtige Sicherheitseinstellungen aktivieren, sobald ein neuer Drucker mit dem Netzwerk verbunden wird.

HP Security Manager
Schützen Sie Ihre HP Druckerflotte mit der Lösung, die Buyers Laboratory (BLI) als „wegweisend" bezeichnet.[4]

So schützt der HP JetAdvantage Security Manager Ihre Flotte

Der HP Security Manager bietet Unterstützung bei der Verfahrensoptimierung zur Anwendung benutzerdefinierter Sicherheitsrichtlinien für eine Flotte an HP Druckern und Bildbearbeitungsgeräten sowie bei der Überwachung und Sicherstellung der Konformität. Der HP Security Manager identifiziert Geräte, die nicht konform sind, und stellt richtlinienbasierte Sicherheitseinstellungen automatisch wieder her. Mit HP Instant-on Security lassen sich neue HP Geräte problemlos schützen, sobald diese dem Netzwerk hinzugefügt werden. So wird der Verwaltungsprozess für die IT-Administratoren vereinfacht und Ihre Kunden können Zeit und Geld sparen.

Im Gegensatz zu den herkömmlichen Tools für die Netzwerkgeräteverwaltung, die zum allgemeinen Gebrauch für die Überwachung und Verwaltung von Ausgabegeräten im Netzwerk geeignet sind, ist HP JetAdvantage Security Manager die umfassendste Druck- und Sicherheitslösung auf dem Markt und bietet einen effektiven richtlinienbasierten Ansatz für den Schutz von HP Druck- und Bildbearbeitungsgeräten.[5]

Machen Sie noch heute den ersten Schritt, indem Sie unter software.hp.com/kiosk eine kostenlose 60-Tage-Testversion beziehen.

Benutzername: HPSM_TRIAL60_KIOSK
Passwort: hpsm60020112

Weitere Informationen

Weitere Informationen dazu, wie Sie HP Security Manager zu einem integralen Bestandteil der übergeordneten IT-Sicherheitsstrategie Ihres Unternehmens machen oder eine kostenlose Testversion beziehen, finden Sie unter hp.com/go/securitymanager.

[1] „Managed Print Services Landscape, 2014", Quocirca, Juni 2014.
[2] Ponemon 2014 Global Report zu durch Cyberkriminalität verursachte Kosten, Oktober 2014.
[3] HP JetAdvantage Security Manager ist separat erhältlich. Weitere Informationen hierzu und zu einer kostenlosen Demoversion finden Sie unter hp.com/go/securitymanager.
[4] Quelle: Lösungsbericht zu HP JetAdvantage Security Manager 2.1 von Buyers Laboratory LLC, Februar 2015. Weitere Informationen finden Sie unter hp.com/go/securitymanager oder buyerslab.com.
[5] Angaben basieren auf internen HP Daten (Vergleich zur Gerätesicherheit, Januar 2015) und einem Lösungsbericht zu HP JetAdvantage Security Manager 2.1 von Buyers Laboratory LLC, Februar 2015.

Für Updates registrieren unter
hp.com/go/getupdated

4AA5-8727DEE, Juli 2015