Mehrstufige Sicherheit für Drucker:

Wie Dell Organisationen hilft, ihre Drucker zu sichern

Zusammenfassung

Organisationen suchen nach Möglichkeiten, die Sicherheit ihrer IT-Umgebungen zu maximieren. Ein wichtiger Aspekt der IT-Sicherheit ist der Schutz von Netzwerkdruckern. Diese wichtigen Geräte sind sowohl physischen als auch netzwerkbasierten Bedrohungen durch interne und externe Quellen ausgesetzt. Zum Schutz vor diesen Gefahren sind Dell Drucker und Multifunktionsdruckgeräte mit einer Reihe von Sicherheitsfunktionen ausgestattet.

Dieses Dokument bietet eine umfassende Übersicht über die Druckersicherheitsfunktionen, die Dell anbietet. Mit diesen Funktionen können Organisationen die Gefahr eines unbefugten Zugriffs auf Dokumente minimieren, sich vor Hackern und anderen netzwerkbasierten Sicherheitsrisiken schützen und Benutzeraktivitäten überprüfen. Zusammen bieten diese Funktionen einen umfassenden, mehrstufigen Schutz und geben IT-Administratoren die Möglichkeit, ihre Drucker rundum zu sichern.

Mehrstufige Sicherheit für Drucker

Wie Dell Organisationen hilft, ihre Drucker zu sichern

Drucker werden bei der Bewertung von IT-Sicherheit und Risikomanagement leicht übersehen. Multifunktionsdrucker (multifunction printers, MFPs), die neben dem Drucken erweiterte Funktionen wie Fax und Scan-Weiterleitung an E-Mail bieten, werden oft als einfache Ausgabegeräte gesehen. Netzwerkdrucker und MFPs sind jedoch Sicherheitsbedrohungen durch interne und externe Quellen ausgesetzt. Diese Gefahren können als physisch oder netzwerkbasiert kategorisiert werden.

IT-Organisationen sind damit vertraut, Server vor netzwerkbasierten Bedrohungen schützen zu müssen. Drucker, die in vernetzten Umgebungen eingesetzt werden, sollten auf die gleiche Weise behandelt werden. Moderne Drucker sind mit leistungsstarken Prozessoren ausgestattet, auf denen integrierte Web-Server (embedded Web Servers, EWSs) ausgeführt werden. Diese Server sind die Voraussetzung für wichtige Services, können jedoch auch als Einlasspunkte für Angriffe auf das Netzwerk missbraucht werden. Zu den potenziellen Bedrohungen in einer Netzwerkumgebung gehören:

- Unberechtigter Zugriff auf den Drucker oder MFP
- Denial-of-Service-Angriffe: Manipulation der Administratoreinstellungen des Geräts oder sogar Änderung des Netzwerkstandorts des Druckers
- Verwendung des Druckers oder MFPs zum Starten eines externen Hackangriffs durch einen nicht genutzten oder offenen Port

Physische Sicherheitsrisiken sind nicht minder wichtig. An Arbeitsplätzen, wo sich viele Benutzer einen gemeinsamen Drucker teilen, besteht immer die Gefahr von physischen Sicherheitsverletzungen. Ein Benutzer mit uneingeschränktem Zugriff auf den Drucker kann sich ein vertrauliches Dokument aneignen, das von jemand anderem gedruckt wurde. Anfällige Dokumente wären beispielsweise Ausdrucke oder Kopien, die versehentlich in den Ausgabefächern des Druckers liegen bleiben, oder eingegangene Faxe, die unbeaufsichtigt auf einem Multifunktionsdrucker verbleiben.

Netzwerksicherheit	Gerätesicherheit	
	Daten	Physisch
Vertraulichkeit **Integrität** **Nachweisbarkeit** • HTTPS (SSL/TLS) • IPSec • Secure IPP • SNMPv3	**Authentifizieren** **Autorisieren** **Identifizieren Daten löschen** • Zugriff auf Kennwort/PIN • Datenträgerlöschung (M5220.22) • AES-Verschlüsselung • Initiierte/geplante Datenlöschung	**Zugriff** • Möglichkeit zum Absperren von Gerät, Formatierer und Fächern
Überwachung und Verwaltung		
Konfiguration und Verwaltung Nutzungsprotokolle und Prüfpfade Überwachung der Serviceverfügbarkeit • Möglichkeit zum Deaktivieren nicht genutzter Ports/Protokolle • Einrichtung von PIN-Nummer/Kennwort beim Einschalten		

Abbildung 1. Dell Laserdrucker verfügen über mehrstufigen Schutz, um die Sicherheit von Datenbeständen zu gewährleisten

Unbefugter Zugriff auf diese Dokumente kann zu Datenlecks oder zur Offenlegung von vertraulichen Informationen wie Finanzdaten oder geistigem Eigentum einer Organisation führen. Dadurch kann das Risiko eines Identitätsdiebstahls erhöht werden und es können sogar gesetzliche Vorschriften verletzt werden, wenn Dokumente wie Krankenakten ins Spiel kommen. In der digitalen Welt von heute haben die Minimierung von Sicherheitsrisiken und der Schutz vertraulicher Informationen höchste Priorität, und der Schutz von Netzwerkdruckern darf beim Thema Datensicherheit nicht außer Acht gelassen werden.

Maßnahmen zur Sicherung von Druckern

Als ein Technologieunternehmen, das mit den Sicherheitsanforderungen vertraut ist, die Unternehmen von Desktop-PCs bis hin zu Rechenzentren zu beachten haben, misst Dell der Dokumentensicherheit die verdiente Priorität zu. Zudem geben wir IT-Administratoren die Möglichkeit, Sicherheitsmaßnahmen an die Anforderungen ihrer jeweiligen Organisation anzupassen. Dell Laserdrucker bieten nicht nur hervorragende Druckleistung zu einem niedrigen Seitenpreis, sondern werden zudem mit Standardsicherheitstechnologien geliefert. Diese stellen mehrstufigen Druckerschutz bereit und helfen so, die Datenbestände der Organisation zu schützen.

Der mehrstufige Schutz von Dell deckt unterschiedliche Aspekte ab, die vom physischen Gerät über den Druckinhalt bis hin zum Netzwerk reichen (Abbildung 1). Im Folgenden werden einige der wichtigsten Sicherheitsfunktionen beschrieben, die von vielen Dell Druckern unterstützt werden. Eine vollständige Liste der Funktionen, die von den unterschiedlichen Dell Laserdruckermodellen unterstützt werden, finden Sie auf Seite 6 dieses Dokuments.

Sicherheitsfunktionen für Druckaufträge

Diese Dell Drucker- und MFP-Funktionen helfen, das Risiko von unbefugten Zugriffen auf gedruckte Dokumente zu minimieren.

Gesichertes Drucken

Die Dell Funktion für gesichertes Drucken hilft Risiken zu minimieren, da der Druckauftrag sicher an einem kennwortgeschützten Ort gespeichert wird. Benutzer können den Zeitpunkt der Ausgabe steuern, indem sie beim Absenden des Druckauftrags an den Drucker ein vierstelliges Kennwort eingeben. Der Druckauftrag wird dann entweder im RAM oder auf dem Festplattenlaufwerk gespeichert. Er wird erst ausgegeben, wenn der Absender im Bedienfeld des Druckers das vierstellige Kennwort eingibt.

Gespeicherte Druckaufträge

Benutzer können Druckaufträge im Drucker speichern und den Druckauftrag mit einem vierstelligen Kennwort sicher ausgeben. Diese Funktion ist praktisch zum Speichern von häufig gedruckten Dokumenten wie Formularen. Statt mehrere Male zum Drucker gehen zu müssen, um Ausdrucke abzuholen, können Benutzer mehrere Druckaufträge sicher zur gleichen Zeit ausgeben.

Der Zugriff auf die Optionen für gesichertes Drucken und gespeicherte Druckaufträge erfolgt über das Druckertreiberfenster. Klicken Sie dort auf die Schaltfläche "Properties" (Eigenschaften) und wählen Sie im Pulldown-Menü "Job Type" (Auftragsart) die Option "Secure Printing" (Gesichertes Drucken) aus (Abbildung 2). Der Druckauftrag wird durch Auswahl des Benutzernamens und Eingabe des Kennworts im Bedienfeld des Druckers ausgegeben.

Wiederaufnahme nach Papierstau

Administratoren können die Funktion zur Wiederaufnahme nach einem Papierstau deaktivieren. So wird verhindert, dass Druckaufträge automatisch erneut gedruckt werden, nachdem ein Papierstau behoben wurde. Wenn es zu einem Papierstau kommt, wird dieser oft nicht vom Absender des Druckauftrags behoben. Dies stellt ein potenzielles Sicherheitsrisiko dar, da die erneut gedruckten Exemplare Unbefugten in die Hände fallen können. Wenn die Wiederaufnahme nach einem Papierstau deaktiviert ist, werden Seiten erst erneut gedruckt, wenn der Absender den Auftrag erneut sendet.

Physische Sperrung

Dell Drucker und MFPs bieten Möglichkeiten zum Abschließen des Geräts und seiner Fächer. Bei vielen Druckern sind optionale Druckfächer mit integrierten Schlössern geschützt.

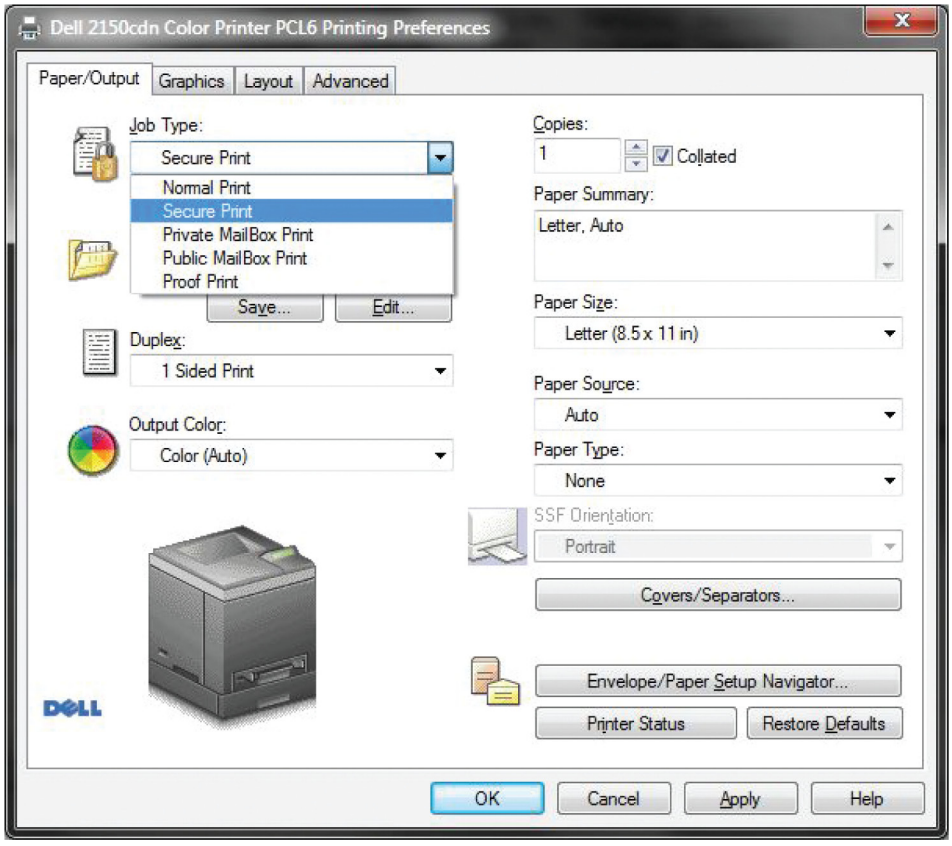

Abbildung 2. Benutzer können im Druckertreiberfenster auf der Registerkarte "Paper/Output" (Papier/Ausgabe) unter "Properties" (Eigenschaften) auf die Funktion zum gesicherten Drucken zugreifen.

Datenträgerlöschung

Alle Druckaufträge werden automatisch auf der Festplatte des Druckgeräts gespeichert. Mit der Datenträgerlöschungsfunktion können Administratoren die Festplatte bereinigen. Dies hilft das Risiko zu eliminieren, dass unbefugte Personen auf die Festplatte zugreifen und Daten aus dem Drucker entnehmen. Zudem können mit dieser Funktion Daten auf dem Gerät zur Sicherheit gelöscht werden, wenn dieses entsorgt oder weiterverkauft wird.

Netzwerksicherheitsfunktionen

Diese Funktionen dienen dem Schutz vor Hackern und anderen netzwerkbasierten Sicherheitsrisiken.

Schutz für das Dell Webtool

Dell Netzwerkdrucker und MFPs bieten die Möglichkeit zur Remote-Steuerung durch autorisierte Personen über einen integrierten Web-Server (embedded Web Server, EWS), das Dell Webtool. Zum Schutz vor unbefugtem Zugriff können Administratoren das Dell Webtool mit einem Kennwort absichern. Alle Drucker werden mit einem Standardkennwort von Null (kein Kennwort) ausgeliefert. Administratoren können das Standardkennwort während des Setups ändern und damit verhindern, dass sich Hacker Zugriff auf den EWS verschaffen und die Druckereinstellungen ändern.

IP-Filter (Zugriffssteuerungsliste)

Auf das Dell Webtool kann durch Eingeben der IP-Adresse eines Geräts in einem Internetbrowser zugegriffen werden. Administratoren können einen IP-Filter einsetzen, der als Zugriffssteuerungsliste bezeichnet wird. Damit kann verhindert werden, dass ein unbefugter Host auf den Drucker zugreift. Der IP-Filter besteht aus einer Liste der IP-Adressen von PCs und Notebooks, die zum Zugriff auf den Drucker berechtigt sind. Wenn die IP-Adresse eines Computers nicht in der Zugriffssteuerungsliste enthalten ist,

kann dieser Computer den Drucker nicht benutzen oder über das Dell Webtool konfigurieren.

Administratoren können den IP-Filter über das Dell Webtool einrichten. Der Prozess ist durch einen integrierten Schutzmechanismus gesichert: Wenn die IP-Adressen in der IP-Filterliste nicht korrekt eingegeben werden, geht der Zugriff auf den Drucker verloren und das Gerät muss auf die Werkseinstellungen zurückgesetzt werden, um wieder einsatzfähig zu sein.

Sicherer Zugriff über HTTPS

Dell Drucker unterstützen zudem das Protokoll HTTP über SSL (HTTPS) für einen sicheren Zugriff auf das Dell Webtool mit einem Eintrag wie https://169.XX.XX.XX. HTTPS-Verbindungen werden oft für Zahlungsvorgänge über das Internet und für vertrauliche Transaktionen in den Informationssystemen von Unternehmen eingesetzt. Durch die Verwendung von HTTPS kann sichergestellt werden, dass Kennwörter und jegliche Kommunikation von Administratoren mit dem Gerät verschlüsselt werden.

Schutz durch IPSec

IP Security (IPSec) ist eine Suite von Protokollen, mit der IP-Kommunikation gesichert werden kann, indem jedes IP-Paket authentifiziert und verschlüsselt wird. Diese Suite unterstützt sowohl Netzwerkbetrieb über IPv4 als auch über IPv6. Bei Druckern und MFPs wird IPSec dazu verwendet, Druckauftragsdaten zu schützen, die zwischen einem Host und dem Drucker gesendet werden. Die Druckdaten werden sicher vom Host zum Drucker transportiert, indem die Datenpakete in der Transportschicht des Netzwerks verschlüsselt werden. Da die Daten verschlüsselt sind, bleiben etwaige Sniffer-Angriffe während des Transports wirkungslos. IPSec kann mithilfe des Dell Webtools über den Druckerserver aktiviert werden.

Sichere Verwaltung im Netzwerk (SNMPv3 und HTTPS)

IT-Administratoren können ihre Druckerbestände mithilfe von Druckerverwaltungstools wie Dell™ OpenManage™ Printer Manager verwalten und überwachen. Diese Verwaltungstools für Netzwerkdrucker verwenden oft branchenübliche Netzwerkprotokolle wie SNMP (Simple Network Management Protocol) und HTTP (Hypertext Transfer Protocol). Dell Drucker verfügen über die erforderlichen Sicherheitsprotokolle, einschließlich HTTPS und SNMPv3, um die Verwaltung des Geräts über eine sichere Netzwerkverbindung zu ermöglichen.

SNMPv3 verwendet einen Authentifizierungsmechanismus und ein Datenschutzkennwort, um eine Verwaltungssitzung mit dem Gerät über das Netzwerk zu sichern. Das Datenschutzkennwort wird zum Verschlüsseln der Daten verwendet, die über das Netzwerk zwischen dem Gerät und dem Host, der die sichere Sitzung eingeleitet hat, übertragen werden.

Deaktivieren nicht genutzter Ports und Protokolle

Nicht genutzte Ports und Protokolle offen zu lassen, lädt Hacker dazu ein, sich unbefugt Zugriff zu verschaffen. Daher ist es ratsam, nicht genutzte Ports und Protokolle zu sperren. So sollten beispielsweise in einem Netzwerk, das ausschließlich TCP/IP verwendet, Protokolle wie Ethertalk, Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) usw. deaktiviert werden.

Auch nicht genutzte Ports wie ftp oder Telnet sollten geschlossen werden. Dell Drucker bieten Administratoren die Möglichkeit, nicht genutzte Ports und Protokolle mit dem Dell Webtool zu deaktivieren. Beim Schließen nicht genutzter Ports sollten Administratoren darauf achten, Port 9100 offen zu halten, da die meisten Druckdaten durch diesen Port gehen.

Zugriffssteuerung und Authentifizierung

Benutzerauthentifizierungs- und Zugriffssteuerungsfunktionen helfen, den Benutzerzugriff zu sichern und Benutzeraktivitäten zu überprüfen.

Bedienfeldverriegelung

Der Zugriff auf die Konfigurationseinstellungen für Drucker oder MFPs kann über die Menütaste im Bedienfeld an der Vorderseite des Geräts erfolgen. Diese bequeme Zugänglichkeit kann dazu führen, dass Nicht-Administratoren auf Konfigurationseinstellungen zugreifen und unerwünschte Änderungen vornehmen. Administratoren können jedoch das Bedienfeld mit einem vierstelligen Kennwort sperren, um das Risiko eines unbefugten Zugriffs auf die Konfigurationseinstellungen zu minimieren. Über das Dell Webtool kann das Bedienfeld auch remote gesperrt werden.

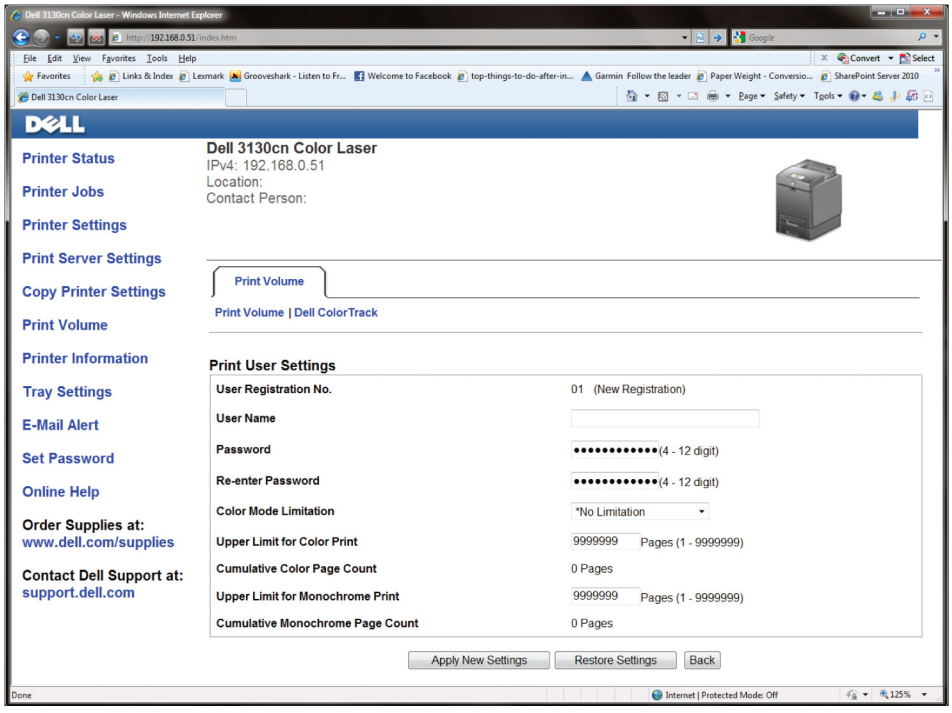

Abbildung 3. Administratoren können über den integrierten Webbrowser des Druckers auf ColorTrack zugreifen und Einstellungen vornehmen

Mehrstufige Sicherheit für Drucker

Wie Dell Organisationen hilft, ihre Drucker zu sichern

Farbdruckkontrolle

Festzulegen, wer Zugriff auf Farbdruck haben sollte und in welchem Umfang, ist ein wichtiger Gesichtspunkt bei der effektiven Verwaltung von Druckkosten. Mit der Dell ColorTrack Technologie können Administratoren unterschiedlichen Personen oder Gruppen angemessene Zugriffsebenen zuweisen (Abbildung 3). So benötigen Grafikdesigner vielleicht uneingeschränkten Zugriff auf Farbdruckfunktionen, um produktiv arbeiten zu können, während die Buchhaltungsabteilung auch mit Schwarz-Weiß-Drucken auskommt. Für andere Gruppen wie etwa den Vertrieb könnten eingeschränkte Farbdruckmöglichkeiten sinnvoll sein.

Administratoren können das Dell Webtool des gewünschten Druckers öffnen, indem sie die IP-Adresse des Druckers in einen Webbrowser eingeben. Die Dell ColorTrack Einstellungen können durch Klicken auf "Print Volume" (Druckvolumen) und dann auf den Link "Dell ColorTrack" aufgerufen werden.

Nutzungsüberprüfung

Für Dell Drucker und MFPs sind Berichte mit Druckhistorie und Druckauftragszähler verfügbar. Mit diesen Berichten können IT-Administratoren alle Druckaktivitäten auf ihren Geräten verfolgen. Diese Funktion hilft bei der Vermeidung unerlaubter Verwendung, da übermäßige Nutzung und Anomalien erkannt werden. Zudem kann so besser sichergestellt werden, dass Drucker so platziert sind, dass die Druckerbestände optimal genutzt werden. Wenn ein Drucker nur wenig genutzt wird, kann dieser an einen besseren Standort in der Arbeitsumgebung versetzt werden.

MFP-Benutzerauthentifizierung

Multifunktionsgeräte in Umgebungen mit vielen vertraulichen Daten können ein Sicherheitsrisiko darstellen. Unbefugte könnten vertrauliche Dokumente fotokopieren oder scannen und per E-Mail versenden und damit die Sicherheit verletzen. Der Dell Farblaserdrucker MFP 2145cn unterstützt die Benutzerauthentifizierung über Kerberos, SMB oder eine lokale Benutzerzugriffsliste, sodass er gut für hochvertrauliche Umgebungen geeignet ist.

		Farb-Einzelfunktionsdrucker						Farb-Multifunktionsdrucker		
Bereiche	**Sicherheitsattribute**	**Dell 1250c**	**Dell 1350cnw**	**Dell 2150cn/ 2150cdn**	**Dell 3130cn**	**Dell 7130cdn**	**Dell 5130cdn**	**Dell 1355cn/ 1355cnw**	**Dell 2155cn/ 2155cdn**	**Dell 3115cn**
Sichere Ausgabe (Druckauftrag)	Vertrauliche Druckaufträge	Nein	Nein	Ja[1]	Ja[1]	Ja[1]	Ja[1]	Nein	Ja[1]	Ja[1]
	Vertrauliche gespeicherte Druckaufträge	Nein	Nein	Nein	Nein	Ja[1]	Ja[1]	Nein	Nein	Nein
	Verschlüsselung von Druckaufträgen	Nein	Nein	Nein	Nein	Ja[6]	Nein	Nein	Nein	Nein
	Wiederaufnahme nach Papierstau (Ein/Aus)	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Nein	Nein
Druckdaten-sicherheit	Festplatten-verschlüsselung	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Nein
	Sichere Festplattenlöschung	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein	Nein
Netzwerk-sicherheit (mit Kabel)	HTTPS/SSL/TLS	Nein	Nein	Ja	Ja	Ja	Ja	Nein	Ja	Ja[3]
	IP-Filter (Zugriffssteuerungsliste)	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Ja	Ja
	SNMPv3	Nein	Nein	Ja	Ja	Ja	Ja	Nein	Ja	Nein
	IPSec	Nein	Nein	Ja	Ja	Ja	Ja	Nein	Ja	Nein
	802.1x-Sicherheit für verkabelte Netzwerke	Nein	Nein	Ja	Nein	Ja	Ja	Nein	Ja	Nein
	Portverwaltung (Ports deaktivieren)	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Sicherer Benutzerzugriff	Sicherer Dell Webtool (EWS)-Zugriff	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja[3]
	Bedienfeldverriegelung	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
	Zugriffssteuerung für Farbdruck	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja
	Kopiersteuerung (für MFPs)	–	–	–	–	–	–	Nein	Ja	Ja
	Netzwerk-authentifizierung (Kerberos/SMB)	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Nein
Faxgeräte	Vertraulicher Faxempfang	–	–	–	–	–	–	Nein	Ja	Ja
	Spam-Fax-Sperre	–	–	–	–	–	–	Ja	Ja	Ja
	Isolierung von LAN und Faxschaltkreis	–	–	–	–	–	–	Ja	Ja	Ja
Physische Sicherheit	Anschlussmöglichkeit für Kensington Sicherheitsschloss am Drucker	Ja	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja
	Kensington Anschluss am Fach	Nein	Nein	Ja	Ja	Nein	Ja	–	Ja	Ja

Tabelle 1. Aktuelle Dell Produktunterstützung, Farblaserdrucker

Faxsicherheitsfunktionen

Auch die Faxfunktionen von modernen Multifunktionsgeräten müssen vor physischen und netzwerkbasierten Angriffen geschützt werden.

LAN-Analogfax-Brücke

Bei MFP-Geräten besteht ein Risiko, wenn zwischen dem Faxschaltkreis und dem LAN Firmware- oder Hardware-Bridging stattfindet. Wenn eine Brücke vorliegt, kann ein Hacker sich über das Analogfax Zugriff auf das Netzwerk verschaffen. Bei der Entwicklung der Schaltschemas von Dell MFPs wird auf die Trennung von Analogfax und LAN geachtet, um die Sicherheit der Faxfunktion zu gewährleisten.

Sicherer Faxempfang

Wenn gedruckte Faxe unbeaufsichtigt im Ausgabefach eines Multifunktionsdruckers verbleiben, besteht das Risiko, dass vertrauliche Informationen in die Hände von Unbefugten gelangen. Mit der sicheren Faxfunktion können Administratoren das unbeaufsichtigte Drucken von Faxaufträgen unterbinden. Der Administrator konfiguriert den MFP so, dass eingegangene Faxaufträge erst ausgegeben werden, wenn der Benutzer einen vierstelligen PIN-Code im Bedienfeld des MFPs eingibt. Im sicheren Faxmodus werden eingehende Faxe im Arbeitsspeicher des Druckers gespeichert. Wenn der Speicher voll ist, werden keine weiteren Faxe angenommen, bis die Aufträge ausgegeben wurden.

[1] Funktionsunterstützung mit optionalem 512 MB/1 GB DIMM-Arbeitsspeicher

[2] Funktionsunterstützung mit optionalem Festplattenlaufwerk

[3] Funktionsunterstützung mit optionaler Multi-Protocol Card (MPC) oder optionalem Adapter für Netzwerkprotokolle

[4] Funktionsunterstützung mit optionaler Gigabit-Karte

[5] Funktionsunterstützung mit optionaler Druckverschlüsselungskarte

[6] Funktionsunterstützung durch IPP/SSL

[7] Funktionsunterstützung mit optionalem integriertem 256 MB RAM

[8] HTTPS unterstützt

Mehrstufige Sicherheit für Drucker

Wie Dell Organisationen hilft, ihre Drucker zu sichern

		Einzelfunktions-Schwarz-Weiß-Drucker											Multifunktions Schwarz-Weiß-Drucke				
Bereiche	**Sicherheitsattribute**	**Dell 1130**	**Dell 1130n**	**Dell 1135n**	**Dell 2230d**	**Dell 2350 d/dn**	**Dell 3330dn**	**Dell 5330dn**	**Dell 7330dn**	**Dell 5230n/dn**	**Dell 5350dn**	**Dell 5530dn**	**Dell 2335dn**	**Dell 2355dn**	**Dell 3333dn**	**Dell 3335dn**	**Dell 5535dn**
Sichere Ausgabe (Druckauftrag)	Vertrauliche Druckaufträge	–	–	–	Nein	Nein	Ja	Ja	Ja[1]	Ja	Ja	Ja	Ja[7]	Ja	Ja	Ja	Ja
	Vertrauliche gespeicherte Druckaufträge	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja[1]	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
	Verschlüsselung von Druckaufträgen	Nein	Nein	Nein	Nein	Nein	Ja[5]	Nein	Ja[6]	Ja[5]	Ja[5]	Ja[5]	Nein	Nein	Ja[5]	Ja[5]	Ja[5]
	Wiederaufnahme nach Papierstau (Ein/Aus)	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Ja[1]	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
Druckdaten-sicherheit	Festplatten-verschlüsselung	–	–	–	Nein	Nein	–	Ja	Nein	Ja[2]	Ja[2]	Ja[2]	Nein	Nein	Ja[2]	Ja[2]	Ja[2]
	Sichere Festplattenlöschung	–	–	–	Nein	Nein	–	Ja	Ja	Ja[2]	Ja[2]	Ja[2]	Nein	Nein	Ja[2]	Ja[2]	Ja[2]
Netzwerk-sicherheit (mit Kabel)	HTTPS/SSL/TLS	–	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja[8]	Ja	Ja	Ja	Ja
	IP-Filter (Zugriffssteuerungsliste)	–	Ja	Ja	–	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
	SNMPv3	–	Ja	Ja	–	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
	IPSec	–	Ja	Ja	–	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
	Portverwaltung (Deaktivieren nicht genutzter Ports)	–	Nein	Nein	–	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja
	802.1x-Sicherheit für verkabelte Netzwerke	–	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Ja	Ja
Sicherer Benutzer-zugriff	Sicherer Dell Webtool (EWS)-Zugriff	–	Nein	Nein	–	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
	Bedienfeldverriegelung	Nein	Nein	Nein	–	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
	Kopiersteuerung (für MFPs)	–	–	Nein	–	–	–	–	–	–	–	–	Ja	Ja	Ja	Ja	Ja
	Netzwerk-authentifizierung (Kerberos/SMB)	–	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja
Faxgeräte	Vertraulicher Faxempfang	–	–	Ja	–	–	–	–	–	–	–	–	Ja	Ja	–	Ja	Ja
	Spam-Fax-Sperre	–	–	Ja[9]	–	–	–	–	–	–	–	–	Ja	Ja	–	Ja	Ja
	Isolierung von LAN und Faxschaltkreis	–	–	Ja	–	–	–	–	–	–	–	–	Ja	Ja	–	Ja	Ja
Physische Sicherheit	Anschlussmöglichkeit für Kensington Sicherheitsschloss am Drucker	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Nein	Ja	Ja	Ja
	Kensington Anschluss am Fach	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein

Tabelle 2. Aktuelle Dell Produktunterstützung, Schwarz-Weiß-Drucker

Spam-Fax-Beschränkung

Administratoren möchten unter Umständen die Nummern festlegen, von denen MFPs Faxe empfangen können, oder Faxe von bestimmten Nummern sperren. Mithilfe der Spam-Fax-Funktion im Bedienfeld des MFPs können Administratoren entsprechende Einstellungen konfigurieren.

Sicherheitsfunktionsmatrix

Die Tabellen 1 und 2 zeigen die Sicherheitsfunktionen an, die von bestimmten Dell Laserdruckermodellen unterstützt werden. In beiden Tabellen bedeutet "Ja", dass eine Funktion unterstützt wird, "Nein", dass diese nicht unterstützt wird und "–", dass diese Funktion für diese Produktklasse nicht relevant ist.

[1] Funktionsunterstützung mit optionalem 512 MB/1 GB DIMM-Arbeitsspeicher

[2] Funktionsunterstützung mit optionalem Festplattenlaufwerk

[3] Funktionsunterstützung mit optionaler Multi-Protocol Card (MPC) oder optionalem Adapter für Netzwerkprotokolle

[4] Funktionsunterstützung mit optionaler Gigabit-Karte

[5] Funktionsunterstützung mit optionaler Druckverschlüsselungskarte

[6] Funktionsunterstützung durch IPP/SSL

[7] Funktionsunterstützung mit optionalem integriertem 256 MB RAM

[8] HTTPS unterstützt

Weitere Informationen

Weitere Informationen zu Dell Druckern und Druckersicherheit finden Sie unter **dell.com/printers**.

Wenn Sie die Sicherheitsfunktionen Ihres Dell Druckers erweitern möchten oder Fragen zu Sicherheit und Dell Druckern haben, wenden Sie sich an das Dell Vertriebsteam und bitten Sie um ein Gespräch mit einem Druckmanagement-Berater. Umfassende Informationen zur Verwendung von Dell Druckern und Sicherheitsfunktionen finden Sie im Handbuch zu Ihrem Dell Drucker.

Dieses White Paper dient ausschließlich zu Informationszwecken und enthält möglicherweise Druckfehler und technische Ungenauigkeiten. Alle Angaben wurden sorgfältig zusammengestellt, dennoch kann keinerlei ausdrückliche oder stillschweigende Haftung übernommen werden.

*Andere unter Umständen in diesem Dokument genannte Marken und Handelsnamen verweisen auf die Inhaber dieser Marken und Namen oder auf deren Produkte. Dell erhebt keinerlei Anspruch auf Eigentumsrechte an den Marken und Handelsnamen Dritter.

Die Angaben in diesem Dokument können ohne Vorankündigung geändert werden.

In den USA zum Patent angemeldet

Weitere Informationen finden Sie unter dell.com/printers.