

Modernste Lexmark Sicherheitsfunktionen für Drucker und Multifunktionsgeräte



Unternehmensdaten sind Ihr wertvollstes Gut.
Lexmark hilft Ihnen dabei, dieses Gut zu bewahren!

Sicherheitsfunktionen von Lexmark

Sie haben vor, ein neues Gerät in Ihr Netzwerk zu integrieren? Doch wissen Sie, ob das Gerät auch wirklich sicher ist? Ob es unberechtigte Zugriffe verhindert? Ob es die Sicherheit Ihres Netzwerks gefährdet? Vielleicht – vielleicht auch nicht? Es gibt viele Dinge, die zu bedenken sind, bevor ein neuer Drucker oder ein neues Multifunktionsgerät ins Unternehmen geholt wird. Wie bei allen anderen Komponenten Ihres Netzwerks handelt es sich auch bei Druckern und Multifunktionsgeräten um komplexe Geräte, die bei nicht ausreichender Sicherung ein potenzielles Risiko darstellen können.

Lexmark stellt Netzwerkgeräte her, die höchsten Sicherheitsanforderungen genügen. Unsere Drucker und Multifunktionsgeräte schützen Ihre Daten und Dokumente innerhalb des gesamten Arbeitsprozesses vom Datenversand im Netzwerk bis hin zur gedruckten Seite im Ausgabeschacht. In dieser Broschüre erfahren Sie, was wir tun, damit Sie sicher arbeiten können.



Sichere Remote-Verwaltung Leistungsfähige Funktionen zur effektiven und sicheren Geräteverwaltung

Zur effizienten und effektiven Verwaltung einer großen Anzahl von Netzwerkdruckern ist die Remote-Verwaltung das Nonplusultra – vorausgesetzt, sie ist sicher. Dazu gehört, dass das Gerät die Konfiguration nur durch berechtigte Anwender zulässt.

Außerdem muss der Prozess der Geräteverwaltung sicher sein, sodass der Datenaustausch über das Netzwerk nicht ausspioniert oder missbraucht werden kann. Lexmark-Geräte bieten zahlreiche Funktionen für eine einfache und sichere Remote-Verwaltung. Diese Funktionen können bequem über die Website konfiguriert werden, mit der das Gerät verknüpft ist.

Sicherheitsprotokoll: Mithilfe des Sicherheitsprotokolls können sicherheitsrelevante Ereignisse nachvollzogen werden. Dies beinhaltet u. a. die Verfolgung von Ereignistypen, Exportfunktionen sowie eine umfassende Ereignisprotokollierung. Die Aktivierung des Sicherheitsprotokolls bietet folgende Vorteile: geringeres Risiko durch Ereignisverfolgung, proaktive Verfolgung und Erkennung potenzieller Risiken sowie Integration in vorhandene Angriffserkennungssysteme für eine proaktive Echtzeitverfolgung. Innerhalb des Geräts werden mehr als 100 Variablen und Ereignisse protokolliert.

Digital signierte Firmware-Aktualisierungen: Heruntergeladene Firmware-Aktualisierungen werden von Druckern und Multifunktionsgeräten automatisch auf die entsprechenden digitalen Lexmark-Signaturen überprüft. Dabei wird Firmware, die nicht ordnungsgemäß von Lexmark verpackt und signiert wurde, abgelehnt. Somit kann auf den Geräten nur genehmigte Firmware ausgeführt werden, was sie für schädliche Programme wie Viren oder Würmer unangreifbar macht.

Zertifikatsverwaltung: Drucker und Multifunktionsgeräte verwenden Zertifikate zur HTTPS-, SSL-, IPSec- und 802.1x-Authentifizierung.

Die Zertifikatsverwaltung ermöglicht die Integration der Geräte in eine Umgebung mit Public-Key-Infrastruktur (PKI), indem sie die sichere Kommunikation zwischen Geräten mit 802.1x und IPSec sowie die Zertifikatsgenehmigung zur Validierung der Domain Controller-Zertifikate, von EWS bzw. LDAP SSL sowie anderen Diensten sicherstellt, die SSL verwenden.

HTTPS: HTTPS dient der sicheren Verwaltung von Netzwerkdruckern und Multifunktionsgeräten. Es ermöglicht die Verschlüsselung des Datenverkehrs und damit eine sichere Remote-Verwaltung über die mit dem Gerät verknüpfte Webseite.

SNMPv3: SNMP ist ein standardmäßiges Netzwerkprotokoll. Version 3 dieses Protokolls enthält umfangreiche Sicherheitsmechanismen. Die Drucker und Multifunktionsgeräte von Lexmark unterstützen SNMPv3 mitsamt der Authentifizierungs- und Verschlüsselungskomponente, was eine sichere Remote-Verwaltung der Geräte ermöglicht. SNMP Version 1 und 2 werden ebenfalls unterstützt und können unabhängig konfiguriert und/oder deaktiviert werden.

IPv6: Das Internet Protocol Version 6 wird für Drucker und Multifunktionsgeräte unterstützt, damit diese mit IPv6-Netzwerken verbunden werden können.

Sicheres Zurücksetzen von Passwörtern: Mithilfe der Funktion zum sicheren Zurücksetzen von Passwörtern können die im Sicherheitsmenü des Geräts vorgenommenen Einstellungen für die Zugriffssteuerung zurückgesetzt werden. Dies kann zum Beispiel erforderlich sein, wenn ein Administratorpasswort vergessen oder die Netzwerkverbindung des Geräts unterbrochen wurde. Das Zurücksetzen erfolgt mithilfe einer Firmware-Einstellung auf der mit dem Gerät verknüpften Website sowie durch Umschalten einer Steckbrücke im Systemboard des Geräts.

Passwortsicherung: Die Passwortsicherung ermöglicht unabhängig vom zugewiesenen Schutzmechanismus oder dessen Verfügbarkeit den Zugriff auf das Sicherheitsmenü des Geräts. Damit kann der Administrator z. B. auch bei Nichtverfügbarkeit eines LDAP-Servers oder -Netzwerks auf das Sicherheitsmenü des Geräts zugreifen, um die für den Gerätezugriff notwendigen Einstellungen vorzunehmen.

Sicherheitsfunktionen von Lexmark

Sichere Netzwerkschnittstellen Schutz Ihrer Geräte vor Hackern und Viren



Beim sogenannten Device-Hardening eines Netzwerkgeräts werden die Netzwerkschnittstellen des Geräts geschützt. Dies beinhaltet die Abschaltung nicht erforderlicher oder nicht verwendeter Komponenten und Funktionen, um deren Missbrauch zu verhindern, die Sicherung der verbleibenden Schnittstellen sowie den Schutz der auf diesem Gerät verwendeten Daten. Drucker und Multifunktionsgeräte von Lexmark verfügen über verschiedene Mechanismen, die das Device-Hardening vereinfachen.

Filtern von TCP-Verbindungen: Drucker und Multifunktionsgeräte können so konfiguriert werden, dass nur TCP-/IP-Verbindungen von festgelegten TCP-/IP-Adressen zulässig sind. Dadurch werden TCP-Verbindungen von anderen Adressen abgelehnt und das Gerät vor unberechtigten Druckerzugriffen und Konfigurationsänderungen geschützt. Zum Konfigurieren dieser Filterfunktion werden in einem Listenfeld die zulässigen Server eingetragen.

Port-Filterung: Die Netzwerkanschlüsse, über die Drucker und Multifunktionsgeräte Netzwerkdaten senden und empfangen, sind konfigurierbar und bieten so ein hohes Maß an Kontrolle über die Netzwerkaktivität des Geräts.

Durch das Herausfiltern von Datenverkehr für bestimmte Netzwerkports können Protokolle wie Telnet, FTP, SNMP, HTTP und viele weitere explizit gesperrt werden.

802.1x: Bei der 802.1x-Authentifizierung müssen sich Drucker und Multifunktionsgeräte in kabelgebundenen und drahtlosen Netzwerken zunächst authentifizieren, bevor sie auf das Netzwerk zugreifen können. Gemäß dem Sicherheitsstandard WPA-Enterprise kann die 802.1x-Authentifizierung mit der WPA-Funktion (WLAN-geschützter Zugriff) eines optionalen drahtlosen Druckservers verwendet werden.

IPSec: Mithilfe des Sicherheitsprotokolls IPSec wird der gesamte Netzwerkverkehr zu bzw. von Netzwerkgeräten durch Verschlüsselungs- und Authentifizierungsmechanismen gesichert, sodass die Daten sicher an Drucker und Multifunktionsgeräte gesendet werden können. IPSec ermöglicht den verschlüsselten Versand von gescannten Daten im Netzwerk. Dadurch werden Druckaufträge geschützt, die für ein bestimmtes Ziel, wie z. B. einen Server, auf dem Lexmark Document Distributor ausgeführt wird, ein E-Mail-Programm oder einen Netzwerkspeicher, gescannt werden.

Secure SNTP: Lexmark-Geräte unterstützen das Simple Network Time Protocol (SNTP) – ein Protokoll, das für die Zeitsynchronisation zwischen verschiedenen Geräten im Netzwerk verwendet wird. Innerhalb unserer SNTP-Konfiguration unterstützen Lexmark-Geräte ein Authentifizierungs- und Berechtigungsfeld; dies ist eine grundlegende Anforderung für die SNTP-Implementierung.

Trennung von Fax und Netzwerk: Verschiedene Multifunktionsgeräte von Lexmark erlauben den Anschluss von Netzwerkadaptern und Faxmodems. In sicherheitskritischen Netzwerkeumgebungen kann die Kombination beider Funktionen in einem Gerät problematisch sein. Bei den Multifunktionsgeräten von Lexmark werden diese Mechanismen bei Hard- und Firmware jedoch voneinander getrennt, sodass zwischen Modem und Netzwerkadapter keine direkte Interaktion stattfinden kann. Darüber hinaus akzeptiert das Modem Bilddaten nur für Faxübertragungen. Alle anderen Daten, z. B. im Zusammenhang mit Remote-Zugriff oder mit Netzwerk- bzw. Firmwareaktualisierungen, werden als ungültig abgelehnt und sorgen für eine Trennung der Datenverbindung.



Sicherheitsfunktionen von Lexmark

Sichern von Daten auf der Festplatte

Verschlüsselung, Löschung und physischer Schutz Ihrer gespeicherten Daten

Einige Drucker und Multifunktionsgeräte von Lexmark sind mit internen Festplatten ausgestattet, auf denen Abbildungen von Dokumenten für die Auftragsverarbeitung gespeichert werden können. Lexmark bietet wirksame Sicherheitsmechanismen, mit denen die Sicherheit der auf der Festplatte gespeicherten bzw. der gesendeten Daten erhöht wird und böswillige Anwender daran gehindert werden können, sich physischen Zugriff auf die Festplatte zu verschaffen.



Festplattenverschlüsselung: Inhalte von Festplatten in Druckern und Multifunktionsgeräten können verschlüsselt werden. Dabei wird intern im Drucker bzw. Multifunktionsgerät ein bis zu 256 Bits langer AES-Schlüssel (Advanced Encryption Standard) generiert, mit dem sämtliche Daten auf der Festplatte verschlüsselt werden. Der Schlüssel wird nicht zusammenhängend auf dem Gerät gespeichert, sodass nur der Originaldrucker oder das Original-MFP auf den Inhalt der Festplatte zugreifen kann. Im Falle eines Festplattendiebstahls können die darauf enthaltenen Daten selbst dann nicht gelesen werden, wenn die Festplatte in einen identischen Drucker oder MFP eingesetzt werden.

Hard Disk Wiping zum sicheren Löschen von Festplattendaten: Die auf der Festplatte gespeicherten Daten können so bereinigt werden, dass keine Restdaten mehr gelesen werden können. Hard Disk Wiping kann manuell, automatisch oder geplant erfolgen. Entsprechend den Vorgaben des US-amerikanischen National Institute of Standard Technology (NIST) und des US-Verteidigungsministeriums können dabei mehrere Sektoren der Festplatte bereinigt werden.

Physischer Schutz: Drucker und Multifunktionsgeräte von Lexmark können mit Schlössern wie z. B. von Kensington gegen Diebstahl oder unbefugtes Öffnen gesichert werden. Damit wird gleichzeitig das Metallgehäuse gesichert, in dem sich Festplatten und optionale Komponenten befinden.

Löschen des nichtflüchtigen Speichers: Beim Löschen des nichtflüchtigen Speichers werden alle Inhalte gelöscht, die in den verschiedenen Formen von Flash-Speichern auf dem Gerät gespeichert sind. Dabei werden sämtliche Einstellungen, Lösungen, Aufträge und Faxe gelöscht. Diese Funktion kann verwendet werden, wenn das Lexmark Gerät ausgetauscht, recycelt oder anderweitig aus der sicheren Umgebung eines Kunden entfernt werden soll.

Sicherer Zugriff Alltägliche Abläufe einfacher und sicherer gestaltet

Bei der Analyse der Netzwerksicherheit werden Netzwerkscan- und Druckdaten leider meistens außer Acht gelassen. Dabei enthalten Dokumente häufig sensible Informationen wie z. B. Finanzdaten, personenbezogene Kunden- oder Mitarbeiterdaten sowie Kontodaten.



Drucker und bildergezeugende Geräte befinden sich in der Regel an stark frequentierten Orten mit wenigen oder keinen physischen Sicherheitsvorkehrungen. So können vertrauliche Informationen – versehentlich oder absichtlich – schnell in falsche Hände gelangen.

Lexmark Geräte umfassen Standardfunktionen, die diese Gefahr erheblich reduzieren.

Geschützte USB-Ports: Laserdrucker und Multifunktionsgeräte von Lexmark unterstützen USB-Geräte, was in sicherheitskritischen Umgebungen u. U. zu Problemen führen kann. Die USB-Host-Ports von Lexmark sind jedoch mit verschiedenen Mechanismen ausgestattet, die böswillige Angriffe verhindern. Dazu zählen z. B. die Zugriffsbeschränkung durch Authentifizierung, Dateitypen-Parameter, Planung der Geräteinteraktion, Sperre für Boot-Unterstützung und die Möglichkeit zur vollständigen Deaktivierung des USB-Host-Anschlusses.

LDAP-Adressbuchsuche: Beim Senden von E-Mails oder Faxnachrichten können E-Mail-Adresse und Faxnummer des Empfängers gesucht werden. Die Lexmark-Multifunktionsgeräte nutzen für die Suchfunktion LDAP und leiten Anfragen an den Verzeichnisserver Ihres Unternehmens.

Sicheres LDAP: Bei Lexmark Geräten kann der gesamte eingehende und abgehende LDAP-Datenverkehr mit TLS/SSL gesichert werden. Beim Austausch von LDAP-Daten wie Anmeldeinformationen, Namen, E-Mail-Adressen und Faxnummern über TLS/SSL-Verbindungen werden die Daten verschlüsselt, um deren Vertraulichkeit zu gewährleisten.

Authentifizierung und Berechtigung: Der Zugriff auf Gerätefunktionen kann beschränkt werden, sodass sich die Benutzer authentifizieren müssen, um bestimmte Funktionen wie Kopieren, Faxen, Scannen für E-Mail-Versand oder Netzwerkordner, Workflow-Skripte und/oder integrierte Anwendungen nutzen zu können. Darüber hinaus können Lexmark-Geräte so konfiguriert werden, dass sich Benutzer für interne Konten, Passwörter und/oder PINs sowie für den Zugriff auf Unternehmensverzeichnisse über NTLM, Kerberos 5, LDAP und/oder LDAP+GSSAPI authentifizieren müssen.



Sicherheitsfunktionen von Lexmark



Diese Authentifizierungsmethoden sind sicher – vorausgesetzt, sie erfolgen über einen SSL-Kanal und sind mit Active Directory bzw. anderen Verzeichnisserver-Plattformen kompatibel. Zusätzlich lässt sich der Zugriff auf Gerätefunktionen auf bestimmte Benutzer oder Gruppen innerhalb des Unternehmensverzeichnisses einschränken.



Automatisches Einfügen der Absender-

Adresse in E-Mails: Wenn sich ein Benutzer authentifiziert, um ein Dokument für den E-Mail-Versand zu scannen, wird automatisch seine E-Mail-Adresse abgerufen und in das Absenderfeld eingetragen. Dadurch kann der Empfänger erkennen, dass die E-Mail von einer Person und nicht anonym oder vom MFP erstellt wurde.

Sicherheitsvorlagen: Sicherheitsvorlagen werden zur Zugriffsbeschränkung verwendet. Sie bestehen aus einem oder mehreren Bausteinen. Sicherheitsvorlagen werden vom Administrator des Geräts definiert und im Dropdown-Menü zur Zugriffssteuerung angezeigt. Diese Vorlagen gelten für bestimmte Menüs und Arbeitsabläufe am Lexmark-Gerät. Sicherheitsvorlagen können eine weitreichende Wirkung haben und die Steuerung wichtiger Sicherheitseinstellungen auf dem Lexmark Gerät ermöglichen.

Zugriffssteuerungen: Mithilfe von Zugriffssteuerungen können Sie aus einer Dropdown-Liste Sicherheitsvorlagen auswählen, mit denen sich der lokale oder der Remote-Zugriff auf bestimmte Menüs, Funktionen und Arbeitsabläufe kontrollieren lässt. Außerdem ist es möglich, Funktionen vollständig zu deaktivieren.

Insgesamt sind mehr als 50 Zugriffssteuerungen verfügbar, die eine größere Flexibilität für Ihre individuelle Umgebung bieten, so z. B. für Gerätefunktionen (Kopieren, Drucken, Faxen, Scannen für E-Mail-Versand, FTP, angehaltene Aufträge, Adressbuch und weitere), Sicherheitsmenüs, Firmware-Aktualisierungen, integrierte Anwendungen, Gerätemenü-einstellungen (Berichte, Papier, Einstellungen, Netzwerk/Ports usw.), Sperren des Bedienpanels, Einstellungen für Fernverwaltung uvm.

Anmeldebeschränkungen: Um die unbefugte Nutzung eines Geräts zu verhindern, können Sie die Anzahl der aufeinanderfolgenden Fehlversuche bei der Anmeldung beschränken. Nach Erreichen dieser Anzahl wird das Gerät für den vom Administrator festgelegten Zeitraum gesperrt. Diese Einstellungen lassen sich bei der Einrichtung von Anmeldebeschränkungen für das Lexmark Gerät konfigurieren. Ergänzend lassen sich bei der Konfiguration der Anmelde-einstellungen der Startbildschirm sowie die Zeitlimits für die Fernanmeldung anpassen. Wenn das Sicherheitsprotokoll aktiviert ist, verfolgt das Gerät die auf die Anmeldebeschränkungen bezogenen Sicherheitsereignisse.

Sperren des Bedienpanels: Das Sperren des Bedienpanels sorgt für die Sperrung eines Geräts, sodass Benutzereingaben und Konfigurationsänderungen auf dem Panel nicht mehr möglich sind. Das Gerät kann dann keine Aufträge mehr kopieren bzw. scannen, und eingehende Aufträge bleiben nicht offen im Ausgabefach liegen. Wenn das Gerät über eine Festplatte verfügt, werden die eingehenden Druck- und Faxe auf der Festplatte gespeichert und nicht gedruckt. Durch Eingabe der Anmeldeinformationen eines berechtigten Benutzers kann das Gerät entsperrt werden. Anschließend werden die angehaltenen Aufträge gedruckt, und der Drucker geht wieder in den normalen Betriebsmodus über.

Vertrauliches Drucken: Druckaufträge werden so lange im Arbeitsspeicher oder auf der Festplatte gespeichert, bis der vorgesehene Empfänger die PIN eingibt und die Druckfreigabe für den Auftrag erteilt. Je nach Einstellung können angehaltene Aufträge nach einer bestimmten Zeit verfallen (Zeitraum von einer Stunde bis zu einer Woche einstellbar). Darüber hinaus kann ein Höchstwert für fehlerhafte PIN-Eingaben eingerichtet werden, nach dessen Erreichen der jeweilige Auftrag gelöscht wird.

PrintCryption-Karte: Die Anwendungslösung Lexmark PrintCryption™ schützt mithilfe von Ver- und Entschlüsselungsmechanismen sensible Daten beim Drucken auf Ihren Netzwerkgeräten und erhöht damit die Sicherheit Ihrer Unternehmensumgebung. Diese Stufe der Drucksicherheit eignet sich für Unternehmen, die vertrauliche, personenbezogene, finanzielle, medizinische, technische oder Geschäftsdaten verarbeiten.

Halten eingehender Faxe: Lexmark-Geräte können so konfiguriert werden, dass Faxe, die zu bestimmten Zeiten eingehen, nicht gedruckt, sondern gehalten werden. Eingehende Faxe werden dann so lange sicher auf der Festplatte abgelegt, bis am Lexmark Gerät die entsprechenden Anmeldeinformationen (z. B. PIN, Passwort und Netzwerk-Benutzerkennung und Passwort) eingegeben wurden.

Sicherheitsfunktionen von Lexmark

Common Criteria

IEEE 2600: Viele Multifunktionsgeräte von Lexmark erfüllen nicht nur die Common Criteria, sondern darüber hinaus auch die besonders strikten Vorgaben für Betriebsumgebungen der IEEE-Arbeitsgruppe 2600. Aufgabe dieser Arbeitsgruppe ist es, auf Grundlage der Erfahrungen von Dutzenden Spezialisten bei den großen Herstellern von Druckern und Ausgabegeräten, bei Prüflaboren, staatlichen Behörden oder anderen Organisationen Sicherheitsstandards für Drucker und Ausgabegeräte zu formulieren. Im Jahre 2008 wurden von der National Information Assurance Partnership (NIAP) die Standards IEEE 2600 verabschiedet, die als Ausgangspunkt für eine Produktevaluierung dienen und auch als Schutzprofil bezeichnet werden.

Wissenswertes über Lexmark USB-Host-Ports:

Das können diese Ports leisten: Anzeigen von Bildern vom USB-Stick, Anzeigen von Flash-Dateien nach Namen (bei Auswahl einer Flash-Datei erfolgt, sofern laut Sicherheitseinstellungen zulässig, eine Aktualisierung der Drucker-Firmware), Auswählen der zu druckenden Aufträge sowie Scannen von Daten direkt auf einen USB-Stick, wenn diese in einem unterstützten Scan-Format vorliegen.

Das können diese Ports NICHT leisten: Anschließen oder Verwenden von USB-Geräten mit Ausnahme von Massenspeichern, Kartenlesern und HID-Geräten (Human Interface Devices); Senden bzw. Verarbeiten von PCL-, PostScript- und anderen Druckerdaten; Übertragen von Daten jeder Art; Erfassen von Daten jeder Art über den Drucker; Ausführen von Code; Starten des Druckers von einem per USB angeschlossenen Gerät.



Deaktivieren von USB-Laufwerken: Der USB-Port eines Lexmark Geräts kann über den mit dem Gerät verbundenen Webserver problemlos deaktiviert werden. Dies ist besonders wichtig für Unternehmen, deren Sicherheitsrichtlinien bzw. -vorgaben solche Funktionen verbieten.

Größere Sicherheit: Um Sicherheitsrisiken für das Produkt bzw. die Umgebung des Kunden auszuschließen, ist der USB-Anschluss an der Vorderseite des Geräts so beschaffen, dass nur bestimmte Aktionen möglich sind. Darüber hinaus kann der Zugriff auf die USB-Host-Anschlüsse durch den Geräteadministrator mithilfe der Authentifizierungs- und Autorisierungskontrolle beschränkt und individuell auf die Sicherheitsrichtlinien des Unternehmensnetzwerks abgestimmt werden.

Fragen und Antworten zum Thema Faxesicherheit

Kann auf die Daten meines MFP über eine externe Telefonverbindung zugegriffen werden?

Nein, bei Lexmark Geräten ist dies nicht möglich. Einige Geräte unterstützen den Remote-Zugriff über Protokolle wie z. B. Telnet, Lexmark Geräte jedoch nicht. Die Multifunktionsgeräte von Lexmark lassen keine Konfiguration per Telefon zu. Des Weiteren gibt es keinen Diagnosemodus, über den externe Mechanismen das Verhalten des Modems steuern oder es neu konfigurieren könnten. Das Einzige, was über ein analoges Telefonmodem möglich ist, ist das Versenden und Empfangen von Faxdaten.

Sind Fax- und Netzwerkkarte vollständig miteinander verknüpft?

Die internen Funktionen des Netzwerkadapters werden separat vom Modem implementiert und befinden sich jeweils in unterschiedlichen Komponentengruppen.

Die Faxkarte und eine untergeordnete Karte werden per Kabel miteinander verbunden; der Netzwerkadapter hingegen befindet sich direkt auf der Hauptplatine des MFP. Die Faxverbindung und die Interaktion mit dem Netzwerkadapter werden von der Lexmark Firmware gesteuert. Diese ist so konfiguriert, dass keine direkte Interaktion zwischen Fax- und Netzwerkkomponenten möglich ist.

Ist es möglich, die Firmware meines MFP per Telefon zu aktualisieren?

Ihr Lexmark Faxmodem bzw. die Lexmark Firmware akzeptiert keinen ausführbaren Code, sondern nur Bilddaten. Wenn die eingehenden Daten kein Bild darstellen, werden sie als ungültig abgelehnt. Es ist nicht möglich, geänderte Firmware (oder andere Arten von Code) als Faxe auftrag zu verpacken und in funktionsfähigem Zustand an das MFP weiterzuleiten.



Sicherheitsfunktionen von Lexmark

Modelle Sicherheitsfunktionen	Einfache Drucker											Multifunktionale Lösungen																					
	E280	E380	E46x	T65x	W880	C340	C343	C344	C546	C734	C736	C792	C925	C950	X20x	X284	X383	X384	X463	X464	X466	X543	X544	X546	X548	X65x	X73x	X792	X86x	X922x	X95x		
Monochromdrucker	•	•	•	•	•										•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•			
Farbdrucker						•	•	•	•	•	•	•	•	•								•	•	•	•	•	•	•	•	•			
Papierformat A4	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•			
Papierformat A3					•								•	•													•	•	•				
Sichere Fernverwaltung																																	
Sicherheitsprotokoll			•	•	•					•	•	•	•	•				•	•	•				•	•	•	•	•	•	•			
Digital signierte Firmware-Aktualisierungen	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		
Zertifikatsverwaltung			•	•	•		• ¹			•	•	•	•	•			•	•	•	•		• ¹		•	•	•	•	•	•	•			
HTTPS			•	•	•					•	•	•	•	•																			
SNMPv3			•	•	•					•	•	•	•	•																			
IPv6	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		
Sicheres Zurücksetzen von Passwörtern			•	•	•					•	•	•	•	•																			
Passwortsicherung			•	•	•					•	•	•	•	•																			
Sichere Netzwerkschnittstellen																																	
Filterung von TCP-Verbindungen	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		
Port-Filterung			•	•	•		•	•	•	•	•	•	•	•					•	•	•												
802.1x			•	•	•		• ¹			•	•	•	•	•								• ¹		•	•	•	•	•	•	•			
IPSec			•	•	•					•	•	•	•	•																			
Secure SMTP			•	•	•					•	•	•	•	•																			
Trennung von Fax und Netzwerk															•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•			
Sichern von Daten auf der Festplatte																																	
Festplattenverschlüsselung (2)				•	•					•	•	•	•	•										•	•	•	•	•	•	•			
Hard Disk Wiping (2)				•	•					•	•	•	•	•										•	•	•	•	•	•	•			
Physischer Schutz	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		
Sicherer Zugriff																																	
Geschützte USB-Ports (USB-Geräte planen)			•	•	•					•	•	•	•	•										•	•	•	•	•	•	•			
LDAP-Adressbuchsuche															•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•			
Sicheres LDAP																																	
Authentifizierung			•	•	•					•	•	•	•	•																			
Autorisierung			•	•	•					•	•	•	•	•																			
Automatisches Einfügen der Absender-Adresse in E-Mails																																	
Sicherheitsvorlagen			•	•	•					•	•	•	•	•																			
Zugriffssteuerungen			•	•	•					•	•	•	•	•																			
Anmeldebeschränkungen			•	•	•					•	•	•	•	•																			
Sperren des Bedienpanels			•	•	•					•	•	•	•	•																			
Vertraulicher Druck			•	•	•					•	•	•	•	•																			
PrintCrypton-Karte (optional)			•	•	•					•	•	•	•	•																			
Halten eingehender Faxe																																	
Common Criteria-zertifiziert (MFP)																																	

¹Nur DW-Modelle

²Für ausgewählte Modelle mit standardmäßig enthaltener Festplatte oder optionaler Festplattenerweiterung

³Optional für Modelle X463 und X86xdV3

Sicherheitsfunktionen von Lexmark

Sicherheitsfunktionen von Lexmark

Das Thema Ausgabesicherheit ist sehr komplex und schließt eine Vielzahl wichtiger Aspekte ein. Drucker und Multifunktionsgeräte von Lexmark sind mit verschiedenen hochwertigen Funktionen ausgestattet, die Ihre Geräte, Ihre Infrastruktur, Ihre Dokumente und Ihre vertraulichen Daten schützen.

Unternehmensstempel

Weitere Informationen zu Lexmark Produkten und Services finden Sie unter www.lexmark.com

Lexmark behält sich das Recht vor, Spezifikationen oder andere Produktinformationen ohne Ankündigung zu ändern. Hinweise in dieser Veröffentlichung auf Lexmark Produkte oder Services bedeuten nicht, dass Lexmark diese in allen Ländern, in denen Lexmark tätig ist, anbietet. LEXMARK STELLT DIESE VERÖFFENTLICHUNG OHNE MÄNGELGEWÄHR UND OHNE ANSPRUCH AUF EXPLIZITE ODER IMPLIZITE GARANTIELEISTUNG BEREIT. DAZU ZÄHLT AUCH DIE IMPLIZITE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND DIE EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. Käufer sollten zur Beurteilung der Leistung einer Lösung, deren Kauf sie planen, weitere Informationsquellen wie Benchmark-Daten heranziehen. Lexmark und Lexmark mit dem Diamantsymbol sind in den Vereinigten Staaten und/oder anderen Ländern eingetragene Marken von Lexmark International, Inc. Alle anderen Marken sind Eigentum ihrer jeweiligen Besitzer. © 2011 Lexmark International, Inc. 740 W. New Circle Rd. Lexington, KY 40550.

LEXMARK
TM