Xerox und Informationssicherheit

Ihre Daten, Ihr Unternehmen:
das Wesentliche durch
Partnerschaften schützen

Inhalt

Überblick

Informationen sind das Kapital jedes Unternehmens und müssen geschützt werden. Datensicherheit im Office-Bereich ist daher für Dokumente und Geräte mit Netzwerkanschluss, darunter Drucker und Multifunktionsdrucker, unerlässlich. Und im 21. Jahrhundert finden praktisch alle Geschäftsaktivitäten in Netzwerkumgebungen statt.

Nahezu jedes Unternehmen, einschließlich sämtlicher Mitarbeiter, ist mit dem Internet verbunden. Ihr Unternehmen – und jedes andere, mit dem Sie zusammenarbeiten – ist Teil eines globalen Systems von miteinander verbundenen Netzwerken und Servern. Zahllose Benutzer führen gleichzeitig Aufgaben aus, greifen auf Informationen zu und teilen diese, kaufen und verkaufen Waren und Services und kommunizieren über E-Mail, Instant Messaging, Skype™, Twitter sowie viele andere Dienste.

Die Sicherheitsbedrohung ist durchaus real, und die Risiken wachsen exponentiell. Eine Sicherheitsverletzung bei den Unternehmensdokumenten kann dazu führen, dass vertrauliche oder proprietäre Informationen von unbefugten Dritten abgerufen und genutzt werden. Mögliche Folgen sind Diebstahl und schädigende Offenlegung von geistigem Eigentum und Betriebsgeheimnissen. Und auf viele Unternehmen kommen durch solche Sicherheitsverletzungen Strafzahlungen und Kosten für Rechtsstreitigkeiten in Millionenhöhe zu.

Moderne Sicherheitsbedrohungen treten in zahlreichen Formen und Schweregraden auf. Der explosive Wildwuchs von vernetzten Geräten bringt eine ständig wachsende Anzahl von potenziellen Angriffspunkten mit sich. Und die Bedrohung durch „Hacker" ist konstant, da rund um die Uhr Programme im Einsatz sind, um automatisch Schwachstellen in Netzwerken und Sicherheitsmaßnahmen zu ermitteln.

Sicherheitsbedrohungen reichen von relativ harmlosen Spam-Nachrichten bis hin zu permanenten Gefährdungen, die ganze Netzwerke in die Knie zwingen können.

Angesichts der kontinuierlichen Netzwerkaktivitäten müssen Sie sich darauf verlassen können, dass die vertraulichen Daten Ihres Unternehmens jederzeit geschützt sind. Aber die Anforderungen ändern sich täglich.

Besonders bei vernetzten Druckern und Multifunktionsdruckern (MFD), die über das Netzwerk drucken, kopieren und scannen, E-Mail-Anhänge versenden sowie ein- und ausgehende Faxübertragungen handhaben können, besteht ein erhöhtes Risiko.

Wer in der Informationssicherheit arbeitet, muss in Bezug auf die Sicherheit des Unternehmensnetzwerks vor allem dafür sorgen, dass Sicherheitsverletzungen über vernetzte Drucker und MFD – oder am Gerät selbst – ausgeschlossen sind. Schließlich sind Angriffe meist unerwartet:

- Über das Telefonkabel, mit dem ein MFD angeschlossen ist, besteht die Gefahr des Zugriffs auf das Netzwerk.
- Der Webserver, über den MFD und Drucker verwaltet werden, könnte anfällig für Angriffe sein.
- Unbefugte können auf der Festplatte oder während der Übertragung vom/auf das Gerät auf ungeschützte elektronische Daten zugreifen.
- Schadhafte E-Mails können ohne Prüfprotokoll von einem MFD gesendet werden.

Drucker und Multifunktionsdrucker sind fortschrittliche IT-Plattformen mit mehreren Subsystemen, weshalb sinnvolle Sicherheitsmaßnahmen jede Komponente der Plattform abdecken müssen.

Moderne Drucker und MFD unterscheiden sich erheblich von PCs und Servern.

- Drucker und MFD werden von mehreren Benutzern und Administratoren gemeinsam genutzt.
- Drucker und MFD sind integrierte Geräte:
  - Das System kann mit einem echten Betriebssystem ausgestattet sein.
  - Das Betriebssystem kann über eine direkte externe Schnittstelle verfügen.
  - Das Betriebssystem ist möglicherweise proprietär.
  - Beim Betriebssystem handelt es sich möglicherweise um Microsoft® Windows®.

Überblick

- Drucker und MFD verfügen über folgende Ausstattung, die in der Regel bei fortschrittlicheren Computern zu finden ist:
  - Netzwerkprotokolle
  - Funktionen für Authentifizierung und Autorisierung
  - Verschlüsselung
  - Geräteverwaltung
  - Webserver

Heterogene Umgebungen mit unterschiedlichen Druckern und MFD stellen Herausforderungen dar.

- Höhere Diversität als bei herkömmlichen PCs
- Hohe Diversität bei Betriebssystemen auf Geräten unterschiedlicher Hersteller und sogar Produktlinien des gleichen Herstellers

Auf herkömmliche PCs und Server ausgelegte Steuerung ist nicht für Drucker und MFD optimiert.

- Virenschutz
  - Möglicherweise nicht für das auf dem Drucker/MFD verwendete Betriebssystem verfügbar
  - In Bezug auf Malware ohnehin auf verlorenem Posten
  - Komplexität der Verwaltung von Datendatei-Updates in verteilten Umgebung
- Patches für Drucker und MFD
  - Uneinheitliche Versionskontrolle für Software auf Druckern und MFD
  - Hoher Betriebsaufwand durch Konfigurationsmanagement
- Security Information & Event Management (SIEM)
  - Uneinheitliche Warn- und andere Hinweise von Druckern und MFD
  - Nicht standardisierte Wiederherstellung von Druckern und MFD

Die Situation ist anders als bei früheren Druckern und Kopierern.

Ohne geeignete Sicherheitsmaßnahmen, die den physischen und elektronischen Zugriff auf Drucker und Multifunktionsdrucker sicher kontrollieren und schützen, können sich nahezu beliebige Personen unbefugten Zugang zum Netzwerk und zu den Daten eines Unternehmens verschaffen und die Datensicherheit bedrohen. Dabei kann es sich um einfache Dinge handeln, wie das Mitnehmen von Dokumenten, die im Ausgabefach des Druckers oder Multifunktionsdruckers vergessen wurden, oder um Schadsoftware, wie etwa Würmer, die vertrauliche Dokumente im Netzwerk abrufen.

Das gesamte System von Druckern und Multifunktionsdruckern sowie die Gerätemanagementsoftware im Netzwerk müssen evaluiert und zertifiziert werden, damit die Informationssicherheit und alle Mitarbeiter einer Organisation sich sicher sein können, dass ihre Dokumente und das Netzwerk sicher und vor Hackern oder gar vor internen Datenschutzverstößen geschützt sind.

In dieser Hinsicht sind Drucker und MFD durchaus unterschiedlich. Ein umfassender Ansatz, der auf grundlegender, funktioneller, fortschrittlicher und praxisrelevanter Sicherheit basiert, ist daher unverzichtbar, um die Daten moderner Unternehmen zu schützen.

Glücklicherweise kann Xerox die entsprechenden Sicherheitsfunktionen zur Verfügung stellen. Seit 20 Jahren ist Xerox weltweit führender Anbieter von sicheren Dokumentenlösungen in unterschiedlichen Branchen. Jedes Produkt und jede Dienstleistung von Xerox® ist auf Sicherheit ausgelegt und für die nahtlose Integration in vorhandene Sicherheitsframeworks konzipiert. Darüber hinaus wird die Sicherheit über den gesamten Produktlebenszyklus hinweg verwaltet – von Anforderungsanalyse und Design über Entwicklung, Fertigung und Bereitstellung bis hin zur Entsorgung –, damit Sie und Ihre Kunden umfassend und zuverlässig geschützt sind.

Xerox schützt Ihre Daten an jeder potenziellen Schwachstelle, um Ihnen diese Arbeit abzunehmen. Wir konzentrieren uns auf unsere Kernkompetenzen, damit Sie sich auf Ihre Kernkompetenzen konzentrieren können.

Xerox-Sicherheitsziele

Im Rahmen unserer Bemühungen, jedem einzelnen unserer Kunden sichere Lösungen bereitzustellen, haben wir fünf zentrale Ziele in Bezug auf Sicherheit identifiziert:

VERTRAULICHKEIT

- Keine unbefugte Weitergabe von Daten bei der Verarbeitung, Übertragung oder Speicherung

INTEGRITÄT

- Keine unbefugten Datenänderungen
- Das System arbeitet wie beabsichtigt ohne Manipulationen durch Unbefugte.

VERFÜGBARKEIT

- Das System arbeitet zuverlässig
- Keine Dienstverweigerung bei autorisierten Benutzern
- Schutz vor Benutzung durch Unbefugte

VERANTWORTLICHKEIT

- Aktionen einer bestimmten Stelle/Person lassen sich direkt zu dieser Stelle/Person zurückverfolgen.

NICHTABSTREITBARKEIT

- Gegenseitige Gewährleistung der Authentizität und Integrität der Kommunikation im Netzwerk

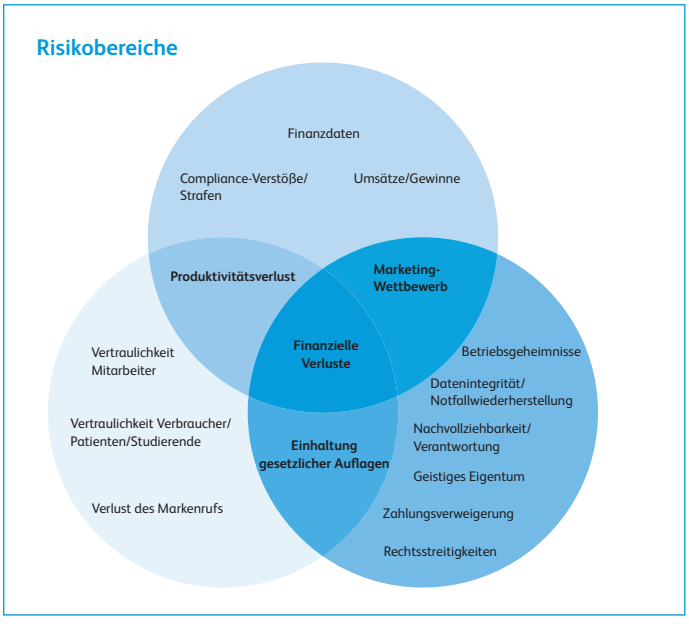
Sicherheitslücken: Branchenrisiken und Kosten

Unternehmen jeder Größe verfügen über vertrauliche Informationen, die vor Cyberkriminellen geschützt werden müssen. Und die Bedrohungslandschaft verändert sich ständig. Mit der zunehmenden Verbreitung von BYOD-Initiativen (Bring Your Own Device, die Verwendung eigener Geräte am Arbeitsplatz), Wearables zur Überwachung von Gesundheitsdaten, mobilen Zahlungssystemen, Cloud-Speicherung und Internet der Dinge nehmen auch die Risiken zu.

Cyberkriminelle konzentrieren sich mehr und mehr auf kleine und mittlere Unternehmen (KMU), weil diesen in der Regel die Ressourcen fehlen, um sich so gut zu schützen wie große Konzerne. Datenschutzverletzungen bei Großunternehmen sind immer wieder in den Schlagzeilen, jedoch hört man kaum von den Cyberangriffen auf KMU.

Dabei steht für KMU sogar noch mehr auf dem Spiel als für Konzerne. Kundendaten sind in KMU eine wertvolle Ressource, deren Verlust für ein KMU katastrophale Folgen haben kann. Laut einer 2015 von IBM und dem Onemon Institute durchgeführten Umfrage sind die durchschnittlichen von Datenschutzverletzungen verursachten Kosten bei den befragten Unternehmen über zwei Jahre um 23 % auf 3,79 Millionen US-Dollar gestiegen.[1] Die durchschnittlichen Kosten für jeden verloren gegangenen oder gestohlenen Datensatz mit vertraulichen Informationen stieg von 145 US-Dollar im Jahr 2014 auf 154 US-Dollar im Jahr 2015 an.[1]

Und dabei sind potenzielle Strafzahlungen, Imageverlust und Betriebsunterbrechungen noch nicht eingerechnet. Sicherheit mag auf der geschäftlichen Prioritätenliste nicht immer ganz oben stehen, doch ist Datenschutz für den Fortbestand jedes Unternehmens unverzichtbar.



Gesundheitswesen

Aufgrund des Fortschritts in der Informationstechnologie – einschließlich der Verbreitung von Handheld-Computern – ist es erforderlich geworden, wichtige medizinische und Patientendaten elektronisch zu übermitteln, wodurch das Sicherheitsrisiko deutlich erhöht wird.

In den USA soll der Health Insurance Portability and Accountability Act (HIPAA, US-Krankenversicherungsgesetz von 1996) alle Unternehmen im Gesundheitswesen zwingen, einheitliche Datenverwaltungspraktiken einzuführen, damit die Daten von Patienten und ihr Recht auf Privatsphäre zuverlässig geschützt sind. Im Rahmen des HIPAA muss ein Prüfprotokoll angelegt werden, um jederzeit nachvollziehen zu können, wer wann und mit welcher Autorisierung auf Daten zugegriffen hat.

Durch den Health Information Technology for Economic and Clinical Health Act (HITECH, Gesetz für IT im Gesundheitswesen) weitete die US-Regierung ihre Bemühungen zur Einführung eines nationalen Systems für elektronische Patientenakten im Gesundheitswesen aus. HITECH wurde im Rahmen des American Recovery and Reinvestment Act (Amerikanisches Aufschwungs- und Reinvestitionsgesetz) von 2009 umgesetzt, um die sinnvolle Nutzung von Informationstechnologie im Gesundheitswesen zu fördern.

Verstöße gegen HIPAA können auch dann zivil- und strafrechtliche Folgen haben, wenn es nicht zu Datenschutzverletzungen gekommen ist.

Behörden

Bei kommunalen, regionalen und Bundesbehörden liegt der Schwerpunkt auf der Vereinfachung von Prozessen und der Verbesserung der amtsübergreifenden Zusammenarbeit, um Bürgerservices zu optimieren. Dazu wurden verschiedene Initiativen umgesetzt, um von der neuesten Technologie profitieren zu können und gleichzeitig über strenge gesetzliche Vorschriften für einen zuverlässigen Schutz sämtlicher Daten zu sorgen. Ein Beispiel hierfür ist das Datenschutzgesetz im US-Bundesstaat Massachusetts, das eines der strengsten in den USA ist. Systeme, Software und Services von Xerox® erfüllen diese und andere strenge Vorgaben.

2014 übernahm das US-Verteidigungsministerium den Standard 800-53 des National Institute of Standards and Technology (NIST), in dem Sicherheitskontrollen für nationale Informationssysteme und -unternehmen sowie Kontrollen für Dokumentensicherheit in allen nationalen Informationssystemen mit Ausnahme der für die nationale Sicherheit relevanten empfohlen werden.

1. „2015 Cost of Data Breach Study: Global Analysis“, IBM und Ponemon Institute, Mai 2015

Sicherheitslücken: Branchenrisiken und Kosten

Das US-Verteidigungsministerium sorgt zudem mit der Einführung von Common Access Cards (CAC) und ihrem Gegenstück für zivile Behörden, den Personal Identity Verification (PIV) Cards, für zusätzliche Sicherheit. Für diese Karten ist eine PKI-Infrastruktur erforderlich, um Sicherheit für Authentifizierung und Kommunikation gewährleisten zu können. Darüber hinaus haben die meisten Bundesbehörden den Standard FIPS 140-2 zur Zertifizierung von in Druckern und MFD eingesetzten Verschlüsselungsmodulen eingeführt. Nicht zuletzt müssen viele Kunden in Bundesbehörden Produkte nach Common Criteria zertifizieren lassen.

Finanzdienstleister

Direkteinzahlung, Online-Banking, Debit-Karten und andere Fortschritte in der Informationstechnologie revolutionieren den Finanzdienstleistungsbereich. Zwar steigert all diese Technologie den Komfort für Kunden und Anbieter, jedoch ergeben sich dadurch auch ganz spezielle Sicherheitsrisiken.

Der sichere Austausch von Kreditkartendaten ist unverzichtbar, und Compliance mit PCI DSS (Payment Card Industry Data Security Standard) beseitigt Schwachstellen und schützt die Daten der Karteninhaber. PCI DSS ist ein proprietärer Informationssicherheitsstandard für Unternehmen, die mit Kreditkarten arbeiten, darunter Visa®, MasterCard®, American Express®, Discover® und JCB.

Der Gramm-Leach-Bliley Act (GLBA) von 1999, ein US-amerikanisches Gesetz zur Modernisierung von Finanzdienstleistungen, soll gewährleisten, dass Finanzinstitute, die private Kundendaten erfassen, über einen entsprechenden Sicherheitsplan zum Schutz dieser Daten verfügen. Um die Vorgaben dieses Gesetzes zu erfüllen, müssen Unternehmen ihre bestehenden Prozesse einer Risikoanalyse unterziehen, Firewalls implementieren, den Benutzerzugriff einschränken, die Druckausgabe überwachen und vieles mehr.

Der Dodd-Frank Wall Street Reform and Consumer Protection Act von 2010, ein US-amerikanisches Gesetz zur Reform des Finanzmarkts, unterstreicht zusätzlich die Notwendigkeit von fehlerfreier Erfassung und Präsentation von Finanzdaten. Daten werden vom Office of Financial Research und angeschlossenen Behörden erfasst und analysiert, um neue wirtschaftliche Risiken zu identifizieren und zu überwachen und diese Informationen in regelmäßigen Berichten und jährlichen Aussagen vor dem US-Kongress zu veröffentlichen.

Bildungswesen

In modernen Bildungsinstituten – darunter Schulen, Fachhochschulen und Universitäten – sind Vorlesungsunterlagen, Anträge und sogar Unterrichtsnotizen online zu finden. Da einige Schulen auch über eigene Krankenstationen verfügen, müssen dort auch Patientendaten elektronisch gespeichert werden. Diese interaktive Umgebung verbessert die Erfahrung der Lernenden und steigert die Produktivität von Lehrkräften, setzt die Schulen aber auch einem erhöhten Sicherheitsrisiko aus.

Da in diesen Instituten Informationen unterschiedlichster Art verwaltet werden, kommen zahlreiche Gesetze zur Anwendung, darunter Computer Fraud and Abuse Act, USA Patriot Act, HIPAA und GLBA. Für das Bildungswesen am relevantesten dürfte jedoch der Family Education Rights and Privacy Act (FERPA) sein. Dieses Gesetz verbietet die Offenlegung von personenbezogenen Informationen im Bildungsbereich ohne schriftliche Genehmigung des Lernenden bzw. seines Vormunds.

Angesichts so vieler Bestimmungen und Compliance-Vorgaben orientiert sich Xerox an den Anforderungen der US-Bundesregierung und anderer Behörden. Da wir Lösungen entwickeln, die den höchsten Sicherheitsstandards entsprechen, können wir allen unseren Kunden, unabhängig von der Branche, höchst sichere Lösungen anbieten.

Sicherheitsüberblick

Auf unserer stark auf Sicherheit ausgerichteten Unternehmensphilosophie gründet die Entwicklung von Produkten, Dienstleistungen und Technologien, die auf allen Ebenen von sicherheitsrelevanten Merkmalen durchzogen sind.

Vor allem bei unseren Smart-MFD dreht sich alles um Sicherheit. Xerox spielt eine führende Rolle bei der Entwicklung digitaler Technologien und hat durch die Aufdeckung potenzieller Sicherheitslücken sowie die proaktive Beseitigung solcher Lücken die Risiken minimiert und bewiesen, welchen Stellenwert wir der Sicherheit und dem Schutz digitaler Daten beimessen. Die Kunden haben dies honoriert und sehen Xerox als zuverlässigen Anbieter sicherer Lösungen mit zahlreichen hochmodernen Sicherheitsmerkmalen als Standard oder optionales Zubehör.

Unsere Sicherheitsstrategie

Die Entwicklung von Xerox®-Produkten erfolgt im Rahmen eines sicheren Entwicklungszyklus und unter Berücksichtigung des Software-Reifegradmodells OWASP (Open Web Application Security Project) sowie der Richtlinien des SANS-Instituts. Dies umfasst das Definieren von Sicherheitsanforderungen, die Risikobewertung, Analyse von Schwachstellen und Penetrationstests sowie Informationen aus dem OWASP und vom SANS-Institut. Diese Strategie ruht auf drei Eckpfeilern:

Hochmoderne Sicherheitsmerkmale

Drucker und Multifunktionsdrucker sind komplexe Netzwerkplattformen mit mehreren Subsystemen, und Xerox bietet die breiteste Palette von Sicherheitsfunktionen auf dem Markt, darunter Verschlüsselung, Authentifizierung, Autorisierung nach Benutzer sowie Audits.

Zertifizierung

Common Criteria for Information Technology Security Evaluation nach ISO 15408 (kurz „Common Criteria“ oder CC) ist der einzige international anerkannte Standard für die Sicherheitszertifizierung. Xerox war der erste Hersteller, der MFD-Komplettsysteme zertifizieren ließ. Da jede Komponente der Multifunktionsplattform eine potenzielle Angriffsstelle ist, sind nur solche Sicherheitszertifizierungen sinnvoll, die alle Komponenten umfassen, darunter Betriebssystem, Netzwerkschnittstelle, Festplatte(n), Webserver, PDL-Interpreter, MFD-Bedienungsoberfläche, lokale Hardware-Anschlüsse und Faxsystem.

Wartung

Die Gewährleistung der Sicherheit unserer Drucker und Multifunktionsdrucker während ihrer gesamten Lebensdauer erfordert eine kontinuierliche Überwachung, um dauerhaften Schutz vor neu entdeckten Bedrohungen zu gewährleisten. Unsere Bemühungen umfassen Folgendes:

- Kontinuierliche Bereitstellung von Software-Updates
- Bereitstellung neuer Sicherheitsberichte über RSS-Feeds
- Reaktion auf identifizierte Schwachstellen
- Bereitstellung von Richtlinien für sichere Installation und Bedienung
- Bereitstellung von Common Criteria-Informationen
- Bereitstellung von Patches unter www.xerox.com/security

Das Xerox Sicherheitsmodell in Kombination mit dem sicheren Entwicklungszyklus ist unsere ausdrückliche Verpflichtung, dafür zu sorgen, dass sämtliche Merkmale und Funktionen des Systems sicher und geschützt sind.

Umfassendes Konzept für Drucker- und MFD-Sicherheit

Xerox hat diesen technologischen Wandel und die sich ändernden Anforderungen am Arbeitsplatz schon vor langer Zeit erkannt und sich darauf eingestellt. Wir bieten umfassende Sicherheitsfunktionen, damit Ihre Drucker/MFD und Daten sicher sind. Xerox schützt jeden Teil der Datenkette, einschließlich Drucken, Kopieren, Scannen, Fax, Dateidownloads und Systemsoftware. **Unser mehrschichtiger Ansatz umfasst vier Schlüsselaspekte:**

1. Schutz vor unbefugtem Zugriff

Die erste und naheliegendste Schwachstelle ist das Gerätedisplay – wer hat physischen Zugriff auf Ihren Drucker und seine Funktionen? Benutzerauthentifizierung ist die Grundlage für den Zugriff auf Xerox®-Drucker und Multifunktionsdrucker durch autorisierte lokale und Netzwerkbenutzer. Nach erfolgter Authentifizierung können Benutzer je nach ihrer Rolle auf die Betriebsarten des Geräts sowie auf Kundendaten zugreifen. Drucker und MFD von Xerox® nutzen verschiedene Technologien, um zu gewährleisten, dass nur autorisierte Benutzer und andere Netzwerkgeräte auf Gerätefunktionen zugreifen können. Danach kümmern wir uns um weniger offensichtliche Schwachstellen – was wird an den Drucker gesendet und wie? Die Xerox® ConnectKey®-Technologie fängt Angriffe von beschädigten Dateien und bösartiger Software ab. Unsere Systemsoftware, einschließlich DLM und Weblets, ist digital signiert: Jeder Versuch, eine infizierte, nicht signierte Version zu installieren, führt dazu, dass die Datei automatisch abgelehnt wird. Darüber hinaus werden Druckdateien gelöscht, wenn ein Teil nicht als legitim erkannt wird.

NETZWERK-AUTHENTIFIZIERUNG

Über die Netzwerk-Authentifizierung können sich Benutzer durch Eingabe von Benutzername und Kennwort am Gerät authentifizieren. Nach erfolgter Netzwerk-Authentifizierung ist eine Person berechtigt, auf eine oder mehrere der folgenden Betriebsarten zuzugreifen: Drucken, Kopieren, Faxfunktion, Serverfax, Nachdruck, E-Mail, Internet-Fax und Workflow-Scannen. Außerdem kann Benutzern die Berechtigung zum Zugriff auf eines oder mehrere der folgenden Gerätemenüs gewährt werden: Betriebsarten, Auftragsstatus oder Gerätestatus.

1. Schutz vor unbefugtem Zugriff

Verhindern des allgemeinen Zugriffs auf bestimmte Geräte durch Benutzerzugriffssteuerung und interne Firewall auf dem Drucker

2. Geräteerkennung

Benachrichtigung beim Systemstart oder auf Abruf, wenn schädliche Änderungen am Drucker erkannt wurden

3. Dokumenten- und Datenschutz

Schutz von personenbezogenen und vertraulichen Informationen durch Festplattenverschlüsselung (AES 256-Bit, FIPS für viele Produkte validiert) und Festplattenüberschreibung

4. Externe Partnerschaften

Schützen Sie Ihre Daten und Geräte vor unbefugtem Zugriff mit der McAfee Whitelisting-Technologie, der integrierten Cisco® Identity Services Engine (ISE), Zertifizierungsstellen und Prüfungsorganisationen

MICROSOFT® ACTIVE DIRECTORY® SERVICES

Dank Microsoft Active Directory Services (ADS) ist es möglich, Benutzerkostenstellen anhand einer zentralen Datenbank für das Gerät zu authentifizieren, statt nur die lokal auf dem Gerät gespeicherte Kostenstellendatenbank zu verwenden.

LDAP-AUTHENTIFIZIERUNG

LDAP-Authentifizierung (BIND) wird unterstützt, um die Authentifizierung über LDAP-Server zur Informationssuche und für den Zugang zu ermöglichen. Wenn ein LDAP-Client eine Verbindung zum Server herstellt, wird der Authentifizierungsstatus der Sitzung standardmäßig auf „anonymous“ eingestellt. Über den BIND-Vorgang wird der Authentifizierungsstatus für eine Sitzung eingerichtet.

SMTP-AUTHENTIFIZIERUNG

Diese Funktion validiert das E-Mail-Konto des Benutzers und verhindert das Versenden von E-Mails über das Gerät durch unbefugte Benutzer. Systemadministratoren können TLS für alle Sende- (SMTP) und Empfangsvorgänge aktivieren.

POP3-AUTHENTIFIZIERUNG VOR SMTP

Als zusätzliche Sicherheitsebene können Systemadministratoren auf Xerox®-MFD die POP3-Authentifizierung vor SMTP aktivieren bzw. deaktivieren. Ist diese Funktion aktiviert, muss eine Anmeldung bei einem POP3-Server erfolgt sein, bevor E-Mails per SMTP gesendet werden können.

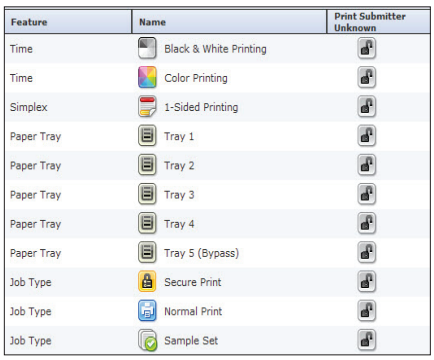
ROLLENBASIERTE ZUGRIFFSSTEUERUNG (RBAC)

Die RBAC-Funktion sorgt dafür, dass authentifizierten Benutzern die Rolle „Nicht angemeldeter Benutzer“, „Angemeldeter Benutzer“, „Systemadministrator“ oder „Kostenzähleradministrator“ zugewiesen wird. Jede Rolle verfügt entsprechende Berechtigungen für den Zugriff auf Funktionen, Aufträge und Warteschlangenattribute. So können Administratoren präzise festlegen, welche Funktionen für eine bestimmte Rolle zur Verfügung stehen. Nachdem sich ein Benutzer mit Benutzername und Kennwort beim Gerät angemeldet hat, ermittelt das System, welche Rollen diesem Benutzer zugewiesen sind. Entsprechend diesen Rollen werden Einschränkungen angewendet. Wenn eine Einschränkung für eine ganze Funktion gilt, wird diese dem Benutzer nach der Anmeldung als gesperrt oder überhaupt nicht angezeigt.

Nicht angemeldeter Benutzer/ Angemeldeter Benutzer	Systemadministrator	Kostenzähleradministrator

BENUTZERRECHTE FÜR DRUCKFUNKTIONEN

Die Xerox-Benutzerrechte bieten die Möglichkeit, den Zugriff auf Druckfunktionen nach Benutzer, Arbeitsgruppe, Tageszeit oder Anwendung einzuschränken. Für Benutzer und Arbeitsgruppen können verschiedene Stufen für den Zugriff auf die Druckfunktionen festgelegt werden. So können Sie mithilfe von Limits festsetzen, dass Farbdruckaufträge nur zu bestimmten Tageszeiten, Microsoft® PowerPoint®-Präsentationen automatisch im Duplex-Modus oder Microsoft Outlook®-E-Mails stets in Schwarzweiß ausgedruckt werden.



Legen Sie Farbdruck-Benutzerrechte und andere Druckeinschränkungen über die intuitiv verständliche Benutzeroberfläche fest.

SMARTCARD-AUTHENTIFIZIERUNG

Die Authentifizierung über Smartcards und Transponderkarten schützt Ihre Drucker und Multifunktionsdrucker vor dem Zugriff durch unbefugte lokale Benutzer. Xerox®-Geräte unterstützen verschiedene verbreitete Smartcards (CAC/PIV, .NET, Rijkspas und andere Formate), etwa 30 Arten von Kartenlesegeräten und 65 unterschiedliche Transponderkarten. Dank Smartcard-Authentifizierung können Benutzer über eine Zwei-Faktor-Identifizierung authentifiziert werden – Besitz der Karte und Eingabe einer PIN am Touchscreen des Geräts –, um Zugriff auf die lokalen Funktionen am Gerät und im Netzwerk zu erhalten.

Common Access Card/Personal Identity Verification (CAC/PIV) ist eine vom US-Verteidigungsministerium herausgegebene Smartcard für Militärpersonal im aktiven Dienst, Reservisten, zivile Angestellte, andere Nichtregierungsmitarbeiter und berechtigte Fremdfirmen. Die CAC/PIV-Karte kann zur allgemeinen Identifizierung, zum kontrollierten Gebäudezugang und zur Authentifizierung von privaten Computern sowie den damit verbundenen Druckern/MFD und Netzwerken verwendet werden.

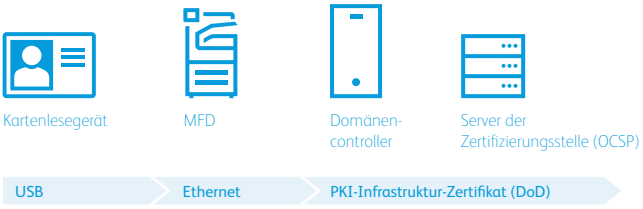
Sicherheitsüberblick

144k CAC/PIV ist eine weitere Smartcard-Version. Benutzer können über die Zwei-Faktor-Authentifizierung Zugriff auf lokale Betriebsarten am Gerät erhalten.

Die 144k CAC/PIV-Karte bietet folgende Vorteile:

- S/MIME-Verschlüsselung für „Scanausgabe: E-Mail“ an sich selbst oder beliebige Empfänger im lokalen Adressbuch des MFD bzw. im globalen LDAP-Adressbuch
- Digitale Signatur über das E-Mail-Signatur-Zertifikat auf der Karte des Benutzers
- Automatisches Eintragen des Empfängers beim Verwenden der Funktion „Scanausgabe: E-Mail“ des MFD
- Zertifizierungsschlüssel mit bis zu 2.048 Bit
- Einschränkung von Übertragungen an Empfänger mit gültigen Zertifikaten
- Empfangen von Bestätigungen per E-Mail und Führen von Überwachungsprotokollen
- Einmalige Anmeldung für Scanausgabe an eigenen Ordner und LDAP

Konfigurationsdiagramm für Common Access Card/Personal Identity Verification (CAC/PIV)



1. Eine Karte wird ins Lesegerät eingeführt, und der Benutzer wird aufgefordert, am MFD eine PIN einzugeben.
2. Der MFD bestätigt über den OCSP-Server, dass das Zertifikat der Karte gültig ist, und verifiziert über eine bekannte Zertifizierungsstelle die „Vertrauenskette“.
3. Der MFD initiiert einen verschlüsselten Challenge/Response-Dialog zwischen dem Domänencontroller und der Common Access Card. Ist dies erfolgreich, stellt der Domänencontroller ein „Ticket Granting Ticket“ aus, und die Autorisierung ist abgeschlossen.
4. Autorisierung schaltet lokale MFD-Funktionen frei:
   - Scanausgabe: E-Mail
   - Kopieren
   - Fax
   - Benutzerdefinierte Betriebsarten
   - Workflow-Scannen

Sicherheitsüberblick

XEROX® PRINTSAFE-SOFTWARE

Die Xerox® PrintSafe-Software bietet sichere Druckauthentifizierung für Druckdaten auf den meisten Druckern und Multifunktionsdruckern von Xerox® und anderen Herstellern. Sie ist mit einer Vielzahl handelsüblicher sicherer Lesegeräte und Karten kompatibel.

Sichere, komfortable und flexible Druckworkflows

Der Anwender übermittelt ein Dokument.

Nach Auswahl des Druckbefehls wird das Dokument bis zur Authentifizierung in der Warteschlange gehalten.

Der Benutzer kann sich einen beliebigen Drucker oder Multifunktionsdrucker im Netzwerk aussuchen, der für die Annahme von PrintSafe-Aufträgen eingerichtet ist, und sich mit einer ID-Karte oder durch PIN-Eingabe authentifizieren.

Nach der Authentifizierung kann der Benutzer am Drucker oder Multifunktionsdrucker einen oder alle Aufträge mit geschützter Ausgabe freigeben.

Die Xerox® PrintSafe-Software ist nicht auf Xerox®-Geräte beschränkt. Alle Drucker oder Multifunktionsdrucker*, die in der Xerox® PrintSafe-Software registriert sind, können für die Ausgabe von PrintSafe-Aufträgen verwendet werden.

Flexible Workflows ermöglichen es Anwendern, Software für Direktdruck auf Ihren PC oder einen vorhandenen Druckserver zu laden, und die Konfiguration der Xerox® PrintSafe-Software ist ein Kinderspiel.

*Für herstellerfremde Geräte wird eine Network Appliance benötigt. Weitere Informationen zu den unterstützten Fabrikaten und Modellen erhalten Sie von Ihrem Xerox-Partner.

ZUGRIFF AM GERÄT UND ÜBER DAS REMOTE USER INTERFACE

Systemadministratoren können unbefugte Benutzer am Zugriff auf die Geräteeinrichtung über das Steuerpult und das Remote User Interface hindern, um die Konfigurationsdaten zu schützen.

2. Geräteerkennung

Falls die Sicherheitsmechanismen für ein Netzwerk und Daten wider Erwarten doch einmal umgangen werden sollten, führt die Xerox® ConnectKey®-Technologie entweder beim Start oder bei der Aktivierung durch autorisierte Benutzer eine umfassende Firmware-Verifizierung durch. Hierbei werden Sie gewarnt, wenn schädliche Änderungen an Ihrem Drucker oder MFD erkannt wurden. Treten Anomalien auf, wird der Benutzer über eine Meldung am Gerät aufgefordert, die Firmware erneut zu installieren. Unsere fortschrittlichsten integrierten Lösungen verwenden die Whitelisting-Technologie** von McAfee®, die Geräte kontinuierlich auf potenzielle Malware überwacht und deren Ausführung automatisch verhindert.

Gemeinsam mit dem Partner Cisco hat Xerox seine Profilerstellung für Geräte in der Cisco® Identity Services Engine (ISE) implementiert. Die Integration mit Cisco Identity Services Engine (ISE) ermöglicht es, Xerox® Geräte im Netzwerk zu erkennen und als Drucker zu klassifizieren, um die Implementierung von Sicherheitsrichtlinien und Compliance-Anforderungen zu erleichtern.

Weitere Informationen finden Sie in den folgenden Whitepapers:

Whitepaper zu McAfee Whitelisting (nur auf Englisch):
http://www.office.xerox.com/latest/SECWP-03.PDF

Whitepaper zu Cisco ISE (nur auf Englisch):
http://www.office.xerox.com/latest/SECWP-04.PDF

* Xerox® VersaLink® Drucker und Multifunktionsdrucker
** Xerox® AltaLink®- und i-Serie-Multifunktionsdrucker

3. Dokumenten- und Datenschutz

Dokumentenschutz

Selbst wenn alle erforderlichen Maßnahmen zur Netzwerksicherheit umgesetzt wurden, um geschäftskritische Daten bei der Übertragung zwischen Computern und Drucksystemen effektiv zu schützen, müssen Sicherheitstechnologien zusätzlich dafür sorgen, dass vertrauliche Druckdokumente nur von den gewünschten Empfängern eingesehen werden können. Xerox setzt modernste Technologie ein, um Ihre Druckausgabe zu schützen, seien es gedruckte Dokumente oder elektronische Dateien.

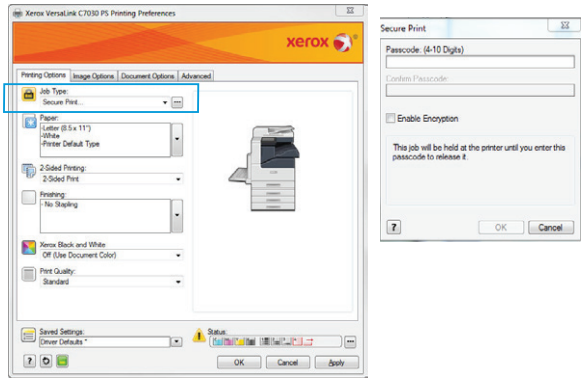
SCANDATENVERSCHLÜSSELUNG

Benutzer der Xerox® ConnectKey®-fähigen Smart-MFD der Modelle i-Serie, VersaLink® und AltaLink® haben bei der Nutzung der Funktion „Scanausgabe: E-Mail“ außerdem die Möglichkeit, PDF-Dateien mit einem Kennwort zu verschlüsseln.

- Schutz außerhalb der Firewall
  - Datensicherung in einer unsicheren Umgebung
  - Einsatz von Branchenstandardprotokollen wie TLS und Secure PDF

VERSCHLÜSSELUNG DES DRUCKDATENSTROMS

Der Xerox® Global Print Driver® sowie einige produktspezifische Treiber unterstützen ab sofort die Dokumentenverschlüsselung bei der Übermittlung von geschützten Druckaufträgen an ConnectKey-fähige Geräte. Xerox® AltaLink und i-Serie Multifunktionsdrucker unterstützen die Verschlüsselung darüber hinaus auch bei Standard-Druckaufträgen. Für die Verschlüsselung über den Druckertreiber ist keine zusätzliche Hardware erforderlich.



GESCHÜTZTE AUSGABE

Vertrauliche Druckaufträge werden am Drucker bzw. Multifunktionsdrucker gehalten, bis der Dokumenteigentümer sie durch Eingabe seiner individuellen PIN am Display des Geräts freigibt. Dadurch wird gewährleistet, dass der vorgesehene Empfänger des Dokuments die vertraulichen Dokumente persönlich unmittelbar am Gerät ausdruckt und sofort aus dem MFD entnimmt, bevor andere Nutzer sie einsehen können.

Bei der geschützten Ausgabe auf der Grundlage von CAC/PIV-Technologie (Common Access Card/Personal Identity Verification) wird dem Druckauftrag das Identitätszertifikat des Auftraggebers angehängt. Am Gerät muss der Benutzer sich dann mit der entsprechenden CAC/PIV-Karte authentifizieren, bevor der Auftrag freigegeben wird.

VERSCHLÜSSELTES/KENNWORTGESCHÜTZTES PDF

Beim Scannen von gedruckten Dokumenten über die Funktion „Scanausgabe: E-Mail“ zur elektronischen Weiterleitung können Xerox®-MFD über AES (128 oder 256 Bit) verschlüsselte oder kennwortgeschützte PDF-Dateien erstellen, die dann sicher über das Netzwerk übertragen werden und erst nach Eingabe des richtigen Kennworts geöffnet, gedruckt oder bearbeitet werden können.

FAXWEITERLEITUNG AN E-MAIL UND NETZWERK

Xerox®-MFD mit Faxweiterleitungsfunktion können eingehende Faxnachrichten an bestimmte E-Mail-Adressen und/oder sichere Netzwerk-Ablagebereiche weiterleiten, wo sie nur von entsprechend autorisierten Personen aufgerufen werden können.

BESTÄTIGUNG VON FAXZIELEN

Der Absender einer Faxnachricht erhält automatisch eine Bestätigung, dass die Nachricht beim gewünschten Empfänger eingegangen ist.

Sicherheitsüberblick

DIGITALE SIGNATUREN

Eine digitale Signatur ist ein mathematisches Schema zum Belegen der Authentizität von digitalen Nachrichten oder Dokumenten. Digitale Signaturen dienen dazu, die Geräte-Firmware vor unerwünschten Änderungen zu schützen und den Ursprung der Daten zu verifizieren. Mit Smartcards können E-Mails mit dem Zertifikat des Absenders digital signiert werden. Eine gültige digitale Signatur dient als Nachweis für den Empfänger, dass eine Nachricht von einem bekannten Absender erstellt und auf dem Übertragungsweg nicht verändert wurde.

SICHERE AUFDRUCKE

Einige Xerox®-Drucker und -MFD verfügen über die Funktion „Sicherer Aufdruck“, die verhindert, dass Original-Ausdrucke mit vertraulichen Informationen kopiert werden. Beim Kopieren eines Dokuments mit sicherem Aufdruck wird der Aufdruck sichtbar. Dadurch wird ersichtlich, dass das Dokument vertrauliche Informationen enthält und widerrechtlich kopiert wurde.

BENUTZER-/ZEIT-/DATUMSANGABEN

Über die Xerox®-Treiber können Benutzer-/Zeit-/Datumsangaben mit jedem vernetzten Gerät auf beliebigen Dokumenten ausgedruckt werden. Dadurch ist jederzeit zuverlässig nachvollziehbar, welches Dokument wann von wem gedruckt wurde.

IP-ADRESSFILTER

Mithilfe von IP-Filtern können Systemadministratoren Regeln erstellen, um am MFD eingehende Daten nach IP-Adressen oder -Adressbereichen zuzulassen oder abzulehnen. So haben sie Kontrolle darüber, wer auf das Gerät zugreifen darf und wer nicht.

Registrierte IP-Adressen:
Verfügbar

Nicht registrierte IP-Adressen:
Nicht verfügbar

SECURE SOCKETS LAYER (SSL)/TRANSPORT LAYER SECURITY (TLS)

Viele Unternehmen sind zur Einhaltung von Sicherheitsrichtlinien verpflichtet und müssen durch die Absicherung des Web-, Datei- und E-Mail-Verkehrs dafür sorgen, dass alle Transaktionen zwischen Clients und Druckern bzw. Multifunktionsdruckern sicher sind. Daten, die unverschlüsselt über das Netzwerk übertragen werden, können von beliebigen „Schnüfflern“ im Netzwerk eingesehen werden. Xerox entschärft dieses Problem durch den Einsatz von Secure Sockets Layer/ Transport Layer Security für Datenübertragungen über bestimmte Protokolle, wie etwa HTTPs und IPP.

IPSEC-VERSCHLÜSSELUNG

Internet Protocol Security (IPsec) sichert die gesamte Kommunikation auf der IP-Ebene ab und wird vorrangig eingesetzt, um an das Gerät übermittelte Druckdaten zu verschlüsseln. Der Datenverkehr zwischen Punkt A und Punkt B wird derart verschlüsselt, dass nur vertrauenswürdige Benutzer Informationen senden und empfangen, die Daten auf dem Übertragungsweg nicht verändert werden und nur autorisierte Benutzer die Informationen empfangen und lesen können.

IPsec bietet die folgenden Sicherheitsvorteile:

- Verschlüsselung des Datenverkehrs (unbefugte Dritte werden am Lesen von privater Kommunikation gehindert)
- Integritätsprüfung (Sicherstellen, dass der Datenverkehr während der Übertragung nicht verändert wurde)
- Peerauthentifizierung (Sicherstellen, dass der Datenverkehr aus einer vertrauenswürdigen Quelle stammt)
- Anti-Replay (Schutz vor Angriffen durch Wiedereinspielung einer sicheren Sitzung)

AKTIVIEREN/DEAKTIVIEREN VON NETZWERK-PORTS

Dank der Möglichkeit, Netzwerk-Ports zu aktivieren bzw. zu deaktivieren, können nicht genutzte Ports und Dienste deaktiviert werden, um den Zugriff durch Unbefugte zu verhindern. Bei kleineren Desktop-Geräten können diese Optionen über das Steuerpult oder mithilfe von PC-basierter Konfigurationssoftware angepasst werden. Bei größeren MFD stehen Tools zum Festlegen von Sicherheitsstufen und Deaktivieren bestimmter Ports und Dienste zur Verfügung.

Sicherheitsüberblick

DIGITALE ZERTIFIKATE

Digitale Zertifikate sind elektronische Dokumente, die eine digitale Signatur verwenden, um einen öffentlichen Schlüssel mit einer Identität zu verknüpfen. Sie umfasst Informationen wie den Namen einer Person bzw. Organisation, ihre Anschrift usw. Das Zertifikat kann verwendet werden, um zu verifizieren, dass ein öffentlicher Schlüssel zu einer Person gehört.

MFD können digitale Signaturen hinzufügen, um die Quelle und Authentizität eines PDF-Dokuments zu bestätigen. Wenn ein Empfänger eine PDF-Datei öffnet, die mit einer digitalen Signatur gespeichert wurde, kann er den Inhalt der Signatur in den Dokumenteigenschaften einsehen, darunter die Zertifizierungsstelle, der Produktname des Systems, die Seriennummer sowie der Zeitpunkt der Erstellung. Wenn es sich um eine Gerätesignatur handelt, enthält diese auch den Namen des Geräts, mit dem das Dokument erstellt wurde, während eine Benutzersignatur die Identität des autorisierten Benutzers bestätigt, von dem das Dokument gesendet oder gespeichert wurde.

Auf Xerox®-MFD kann ein bestimmtes von einer Zertifizierungsstelle ausgestelltes Zertifikat gespeichert werden, oder der Systemadministrator kann ein selbstsigniertes Zertifikat auf dem Gerät erstellen. Durch die Einrichtung eines Zertifikats auf dem Gerät kann die Verschlüsselung für bestimmte Workflow-Arten aktiviert werden.

SNMPV3

Simple Network Management-Protokoll (SNMP) ist ein Internet-Standardprotokoll für die Verwaltung von Geräten in IP-Netzwerken, das durch den Schutz von Daten vor unbefugten Zugriffen, die Einschränkung des Zugriffs auf autorisierte Benutzer und Datenverschlüsselung in Netzwerken für mehr Sicherheit sorgt.

Zu den Geräten, die SNMP in der Regel unterstützen, zählen Router, Switches, Server, Arbeitsstationen, Drucker, Modem-Racks und vieles mehr. Das Protokoll wird überwiegend in Netzwerkmanagementsystemen zur Überwachung der an das Netzwerk angeschlossenen Geräte auf Konditionen, die administrativen Aufwand erfordern, verwendet. SNMP ist eine Komponente der Internetprotokollfamilie gemäß Definition der Internet Engineering Task Force (IETF). Das Protokoll SNMPv3 bietet deutlich optimierte Sicherheitsfunktionen, darunter Nachrichtenverschlüsselung und Authentifizierung.

SNMP-COMMUNITYNAME-ZEICHENFOLGEN

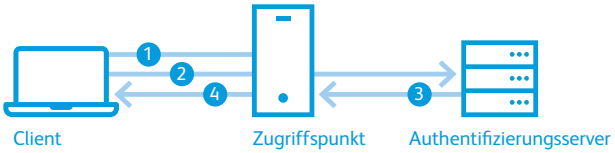
Typische schreibgeschützte MIB-Daten (Management Information Base) verwenden die Zeichenfolge „public“, während die Community-Zeichenfolgen mit Lese-Schreib-Zugriff auf „private“ eingestellt sind. Bei Verwendung der Communityname-Zeichenfolgen mit Lese-Schreib-Zugriff kann eine Anwendung die Konfigurationseinstellungen des Geräts mithilfe von MIB-Variablen ändern. Die Communityname-Zeichenfolge mit Lese-Schreib-Zugriff auf Xerox®-Geräten kann vom Systemadministrator geändert werden, um die Sicherheit beim Verwalten von MFD über SNMP zu erhöhen.

802.1X-AUTHENTIFIZIERUNG

IEEE 802.1X ist ein IEEE-Standard für portbasierte Netzwerkzugriffssteuerung (PNAC, Port-based Network Access Control). Er gehört zur IEEE 802.1-Gruppe der Netzwerkprotokolle. Er stellt einen Authentifizierungsmechanismus für die Einbindung von Geräten in ein lokales Netzwerk (LAN) oder Drahtlosnetzwerk (WLAN) bereit. IEEE 802.1X-Funktionalität wird von vielen Ethernet-Switches unterstützt und kann verhindern, dass Gast-, Rogue- oder nicht verwaltete Systeme sich erfolgreich für den Zugriff auf Ihr Netzwerk authentifizieren.

Funktionsweise: 802.1X-Authentifizierung

802.1X-Authentifizierung für WLAN bietet eine zentrale, serverbasierte Authentifizierung von Endbenutzern.



1. Ein Client sendet einen „start“-Befehl an einen Zugriffspunkt, der die Identität des Clients anfordert.
2. Der Client sendet seine Identität in einem Antwortpaket, das der Zugriffspunkt an einen Authentifizierungsserver weiterleitet.
3. Der Authentifizierungsserver sendet ein „accept“-Paket an den Zugriffspunkt.
4. Der Zugriffspunkt versetzt den Client-Port in den Status „autorisiert“ und gibt den Datenverkehr frei.

Sicherheitsüberblick

Durch die fortschreitende Verbreitung von Drahtlosnetzwerken setzt sich auch das 802.1X-Protokoll immer stärker durch. Viele Unternehmen nutzen dieses Protokoll, um den Port-Zugriff auf ihre internen Netzwerke zu sperren. Dadurch gelangen nur solche Informationen ins Netzwerk, deren Quelle authentifiziert wurde. In Bezug auf das Risikomanagement ist dies günstig, da sowohl drahtlos als auch per Kabel vernetzte Geräte zunächst ihre Identität belegen müssen, bevor ihre Informationen ins Netzwerk weitergeleitet werden. Bei einem nicht autorisierten Zugriffsversuch wird der Port gesperrt, bis die Sperre vom Systemadministrator aufgehoben wird.

Extensible Authentication Protocol (EAP) ist ein Authentifizierungs-Framework, das auf der 802.1X-Authentifizierung basiert. Folgende EAP-Arten werden derzeit von Xerox®-MFD unterstützt:

- EAP-MD5
- PEAPv0/EAP-MS-CHAPv2
- EAP-MS-CHAPv2
- EAP-TLS (AltaLink® und i-Serie)

FIREWALL

Eine Firewall schützt Geräte in Computersystemen oder Netzwerken vor externen Bedrohungen und Zugriff durch Unbefugte und lässt autorisierte Kommunikation passieren. Das Gerät kann so konfiguriert werden, dass Netzwerkübertragungen anhand von bestimmten Regeln und Kriterien zugelassen oder blockiert werden. Netzwerkadministratoren können den Zugriff auf Netzwerksegmente, Dienste und Ports des Geräts einschränken, um die Geräte abzusichern.

TRENNUNG VON FAX UND NETZWERK

Die Faxschnittstelle wird vom Netzwerk-Controller getrennt, damit Hacker keine Möglichkeit haben, über die Faxleitung in ein Büronetzwerk einzudringen.

Der MFD stellt keine Funktion zum Zugriff auf das Netzwerk über die Faxleitung bereit. Das auf dem MFD eingesetzte Faxprotokoll Klasse 1 reagiert nur auf Faxbefehle, die den Austausch von Faxdaten zulassen. Bei den vom Client-PC übertragenen Daten kann es sich nur um komprimierte Bilddaten mit Zielinformationen handeln. Werden andere Daten übermittelt (wie etwa Viren, Sicherheitscode oder Steuerungscode, der direkt auf das Netzwerk zugreift), wird die Verbindung vom MFD sofort unterbrochen. Daher ist es nicht möglich, über die Faxleitung auf das Netzwerk-Subsystem zuzugreifen.

Datenschutz

Technologie hat die Arbeitsabläufe in Unternehmen revolutioniert. Heute liegen Dokumente nicht nur in der herkömmlichen gedruckten Form vor, darunter auch handschriftliche Notizen und Entwürfe, sondern auch in elektronischer Form auf Computern und in E-Mails. Da diese elektronischen Dokumente anders erstellt, abgelegt, weitergegeben und verteilt werden als Papierdokumente, sind sie völlig neuartigen Risiken ausgesetzt. Um wettbewerbsfähig bleiben zu können, müssen Unternehmen auf diese Bedrohungen reagieren und sowohl Dokumente als auch Dokumentenmanagementsysteme schützen, die die wichtigste Ressource eines Unternehmens enthalten – Wissen.

Informations- und Dokumentenmanagementsysteme sind zahlreichen Sicherheitsbedrohungen ausgesetzt. Dazu zählen vorsätzliche Spionagetätigkeiten, wie etwa Computer-Hacking, Diebstahl, Betrug und Sabotage, sowie unbeabsichtigte Tätigkeiten, wie menschliches Versagen und Naturkatastrophen. Bei Informationssicherheit geht es um mehr als um reinen Schutz. Es geht darum, die zeitnahe Verfügbarkeit von Dokumenten und Inhalten sicherzustellen, um Geschäftsabläufe und Business Performance zu verbessern. Darüber hinaus müssen die Originalinhalte verwaltet und Compliance mit gesetzlichen Vorgaben gewährleistet werden.

Seit der Einführung der ersten digitalen Produkte ist Xerox sich der Gefahr bewusst, dass aufbewahrte Daten von unbefugten Personen aus dem Permanentspeicher abgerufen werden könnten, und schützt die Daten der Kunden daher mithilfe von in die Geräte integrierten Funktionen und Gegenmaßnahmen.

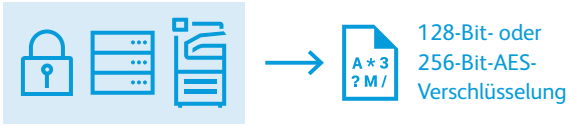
BILDDATENVERSCHLÜSSELUNG

Viele Xerox®-Geräte bieten AES-Datenverschlüsselung mit 128 oder 256 Bit für Aufträge, Bilddaten und Kundendaten, sodass die Daten Ihres Xerox®-MFD effektiv vor unbefugten Zugriffen geschützt sind. Dabei wird auf der partitionierten Festplatte nur die Partition mit den Benutzerdaten verschlüsselt. Die Verschlüsselung der Partition mit dem Betriebssystem ist nicht möglich.

- AES-Verschlüsselung mit 128 oder 256 Bit, die nach FIPS 140-2 (Federal Information Processing Standard) zertifiziert ist
- Sämtliche Benutzerbilddaten auf der Festplatte werden verschlüsselt.

Sicherheitsüberblick

AES ist als kompakter, schneller und relativ angriffssicherer Verschlüsselungsstandard für zahlreiche Geräte und Anwendungen geeignet. Dieser Standard ist die ideale Kombination aus Sicherheit, Leistung, Effizienz, einfacher Implementierung und Flexibilität. Viele Xerox®-Geräte können in einem FIPS 140-2-Modus betrieben werden, in dem sie ausschließlich gemäß FIPS 140-2 zertifizierte Verschlüsselungsalgorithmen nutzen.



FESTPLATTENÜBERSCHREIBUNG

Bei der Festplattenüberschreibung werden nicht mehr benötigte Daten effektiv von der Festplatte des Xerox®-Geräts gelöscht. Diese Funktion kann automatisch nach jeder Auftragsverarbeitung, regelmäßig zu einem bestimmten Zeitpunkt sowie manuell auf Anforderung des Systemadministrators ausgeführt werden. Auf Xerox®-Geräten stehen die Sofortüberschreibung und die Bedarfsüberschreibung zur Auswahl.

FLÜCHTIGER UND PERMANENTSPEICHER

In jedem Xerox®-MFD umfasst der Controller sowohl flüchtigen Speicher (RAM) als auch Permanentspeicher (Festplatte). Beim flüchtigen Speicher sind alle Bilddaten nach dem Herunterfahren sowie nach einem Systemneustart verloren. Beim Permanentspeicher werden Bilddaten in der Regel entweder im Flash-Speicher oder auf der Festplatte des MFD gespeichert, bis sie aktiv gelöscht werden.

Kunden machen sich immer mehr Gedanken über Datensicherheit und möchten wissen, wie und wo Daten gefährdet sind. Hinweise zu flüchtigem Speicher sind Dokumente, die erläutern, wo genau in Xerox®-Geräten die Bilddaten von Kunden gespeichert werden. Im Hinweis zu flüchtigem Speicher werden Speicherort, Funktionsumfang und Inhalte von flüchtigem und Permanentspeicher im entsprechenden Xerox®-Gerät beschrieben.

Hinweise zu flüchtigem Speicher stehen sicherheitsbewussten Kunden für zahlreiche Xerox®-Geräte zur Verfügung. Diese Dokumente sind beim zuständigen Xerox-Supportteam verfügbar (für Bestandskunden), bei Xerox-Vertriebsmitarbeitern (für Neukunden), oder sie können unter www.xerox.com/security abgerufen werden.

GESCHÜTZTES FAX

Eingehende Faxnachrichten mit vertraulichen Inhalten werden gehalten, bis sie vom Systemadministrator freigegeben werden.

SCANAUSGABE: MAILBOX – KENNWORTSCHUTZ

Bei Verwendung der MFD-Funktion „Scanausgabe: Mailbox" kann die Ziel-Mailbox mit einem Kennwort geschützt werden, sodass die darin gespeicherten Scans nur von autorisierten Personen abgerufen werden können. Die Sicherheit der Funktion „Scanausgabe: Mailbox" wird zusätzlich durch die Verschlüsselung der Bilddatenpartition der Festplatte verbessert.

SCANAUSGABE: E-MAIL – S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) ist ein Standard, der die folgenden kryptografischen Sicherheitsdienste für die Funktion „Scanausgabe: E-Mail" bereitstellt: Authentifizierung, Integrität von Nachrichten, Nichtabstreitbarkeit des Ursprungs (mithilfe von digitalen Signaturen) sowie Datenschutz und Datensicherheit (über Verschlüsselung).

Beim Senden von Daten in das Netzwerk über S/MIME wird jeder E-Mail-Nachricht eine Signatur angehängt, die auf den im Gerät gespeicherten Zertifikatsinformationen basiert. Die gesendeten Daten werden anhand des Zertifikats und der jeweiligen Empfängeradresse verschlüsselt. Das Zertifikat wird bei der Eingabe der Datenübertragungsdaten sowie unmittelbar vor dem Versenden der Daten verifiziert. Die S/MIME-Verarbeitung erfolgt nur dann, wenn die Gültigkeit des Zertifikats bestätigt wurde.

SCANAUSGABE: E-MAIL – VERSCHLÜSSELUNG

Dank der Verschlüsselung von E-Mails mittels Smartcard-Authentifizierung können Benutzer über die öffentlichen Schlüssel der jeweiligen Empfänger bis zu 100 E-Mails an verschiedene Empfänger aus dem LDAP-Verzeichnis senden. Die meisten Xerox®-MFD, die Smartcard-Authentifizierung verwenden, sind auch in der Lage, E-Mails digital zu signieren. Benutzer können die Zertifikate potenzieller Empfänger vor dem Versenden von E-Mails einsehen. Der MFD lässt Empfänger ohne Verschlüsselungszertifikat nicht zu. Darüber hinaus protokolliert der MFD sämtliche E-Mail-Sendevorgänge, und optional können Bestätigungen an den Administrator gesendet werden.

VERBERGEN DES AUFTRAGSPROTOKOLLS

Die Standardfunktion zum Verbergen des Auftragsprotokolls sorgt dafür, dass vom Gerät verarbeitete Aufträge weder von lokalen Benutzern noch über das Remote User Interface eingesehen werden können. Obwohl die Daten des Auftragsprotokolls verborgen sind, k ann der Systemadministrator nach wie vor darauf zugreifen und das Auftragsprotokoll auch drucken, um die Nutzung der Kopier-, Fax-, Druck- und Scanfunktion auf dem Gerät zu überprüfen.

HARD DRIVE RETENTION (FESTPLATTENSICHERHEIT)

Xerox bietet Kunden mit vertraulichen oder sogar als geheim eingestuften Bilddaten auf den Festplatten ihrer Xerox®-Geräte das optionale „Hard Drive Retention" an. Im Rahmen dieses Service können Kunden gegen eine Gebühr die Festplatten von geleasten Geräten behalten, um sie entsprechend ihren eigenen Sicherheitsanforderungen sicher zu löschen oder zu zerstören.

FERNSERVICE-DATENVALIDIERUNG

Bei vielen Xerox®-Geräten wird vor der Übermittlung von personenbezogenen und Kundendaten über den Fernservice an Xerox eine Genehmigung des Kunden eingeholt.

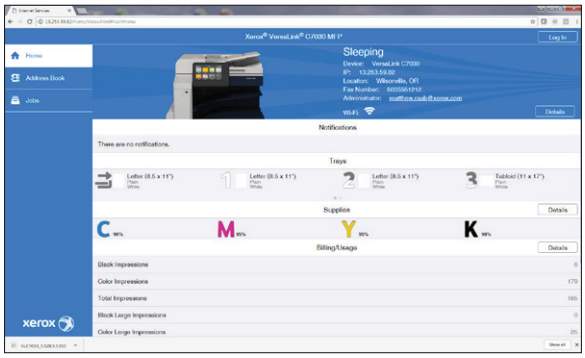
POSTSCRIPT-KENNWÖRTER

Ein weiterer Risikobereich ist das Drucken über die Seitenbeschreibungssprache (PDL) Adobe® PostScript®. PostScript umfasst Befehle, über die Druckaufträge das Standardverhalten eines Geräts ändern und dadurch das Gerät gefährden können. Da die PostScript-Sprache über sehr leistungsstarke Dienstprogramme verfügt, mit denen die Sicherheit von Geräten beeinträchtigt werden kann, ist es Administratoren möglich, das Gerät so zu konfigurieren, dass PostScript-Aufträge zur Änderung des Geräteverhaltens ein Kennwort enthalten müssen. Die grundlegenden Rechte des PostScript-Interpreters im Controller sind ab Werk eingeschränkt, jedoch haben Administratoren einige Möglichkeiten, den Betrieb des PostScript-Subsystems zu verwalten.

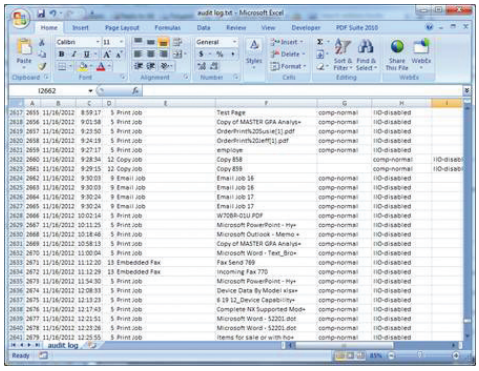
PRÜFPROTOKOLL

Xerox®-MFD und viele unserer Drucker können Überwachungsprotokolle anlegen, um Aktivitäten nach Dokument, Benutzer und Funktion zu überwachen. Auf neueren Geräten ist das Überwachungsprotokoll standardmäßig aktiviert und kann vom Systemadministrator nach Bedarf deaktiviert oder aktiviert werden. Dabei werden Zugriffe und Zugriffsversuche auf das Gerät aufgezeichnet, und Überwachungsprotokolle können an ein SIEM-System oder einen entsprechenden Protokollserver übermittelt werden. Ein Beispiel für einen Eintrag im Überwachungsprotokoll: „Anmeldung von Benutzer xx bei Xerox® AltaLink® MFD um 00:48 Uhr; Faxversand von 10 Seiten an 0123 1234 567".

Bei Xerox® ConnectKey®-fähigen Multifunktionsdruckern kann das Überwachungsprotokoll automatisch und sicher an ein SIEM-System übermittelt werden, um die kontinuierliche Überwachung des MFD zu gewährleisten.



Die Einstellungen für das Überwachungsprotokoll können an der Arbeitsstation des Systemadministrators über einen Standard-Webbrowser aufgerufen werden.



Das Protokoll kann dann in eine TXT-Datei exportiert und in Microsoft® Excel® geöffnet werden.

4. Externe Partnerschaften

Xerox arbeitet mit Organisationen zusammen, die Compliance-Tests durchführen, sowie mit branchenführenden Sicherheitsunternehmen, wie etwa McAfee, um deren umfassende Standards und Expertise mit unseren zu kombinieren. Die folgenden Malwareschutz-Funktionen sind auf Xerox® ConnectKey®-fähigen MFD (Xerox® AltaLink® und i-Serie Multifunktionsdrucker) verfügbar.

MCAFEE® EMBEDDED CONTROL – ENHANCED SECURITY

Xerox®-MFD mit Xerox® ConnectKey®-Technologie verfügen über integriertes McAfee Embedded Control powered by Intel® Security. Dadurch finden Sie bei uns die branchenweit ersten Multifunktionsdrucker, die sich selbst vor potenziellen Bedrohungen von außen schützen. Die Whitelisting-Technologie von McAfee erkennt unbefugte Lese- und Schreibversuche in geschützten Dateien und Verzeichnissen und meldet diese. Darüber hinaus ist dank der nahtlosen Integration mit Xerox® CentreWare® Web-Software, dem Xerox® MPS-Toolset und McAfee ePolicy Orchestrator® (McAfee ePO™) die Überwachung über die bevorzugte Konsole möglich.

MCAFEE EMBEDDED CONTROL – INTEGRITY CONTROL

Integrity Control basiert auf den Funktionen der Enhanced Security Suite und verhindert, dass neue Dateien an beliebigen Speicherorten über nicht vertrauenswürdige Methoden ausgeführt werden. Da nur genehmigte Software ausgeführt werden kann, werden sowohl allgemeine als auch gezielte Angriffe verhindert. Xerox und Intel Security sorgen mithilfe von Whitelisting-Technologie dafür, dass nur die wirklich benötigten Funktionen verfügbar sind, was vor allem bei unternehmensweiten Implementierungen sinnvoll ist. Mithilfe der gleichen Technologie werden Server, Geldautomaten, Kassenterminals und integrierte Systeme, wie etwa Mobilgeräte, geschützt.

MCAFEE EPOLICY ORCHESTRATOR (EPO)

McAfee ePolicy Orchestrator (ePO) ist ein Sicherheitsmanagement-Tool, das Risiko- und Compliance-Management für Unternehmen jeder Größe einfacher macht. Es bietet Benutzern Drag&Drop-Dashboards mit Sicherheitsinformationen über verschiedene Endpunkte hinweg – Daten, Mobilgeräte und Netzwerke – und verkürzt durch Echtzeit-Einblicke die Reaktionszeiten. ePolicy nutzt vorhandene IT-Infrastrukturen durch die Verknüpfung der Verwaltung von Sicherheitslösungen von McAfee und anderen Herstellern mit LDAP, IT-Abläufen und Tools zur Konfigurationsverwaltung.

Unabhängige Dritte – z. B. Zertifizierungsstellen wie Common Criteria (ISO/ IEC 15408) und FIPS 140-2 – messen unsere Leistung auf Basis internationaler Standards und liefern den Beweis, dass wir Top-Compliance-Werte erreichen. Sie schätzen uns für unseren umfassenden Ansatz in Bezug auf die Druckersicherheit.

INTEGRIERTE CISCO® IDENTITY SERVICES ENGINE (ISE)

Zentrale Bereitstellung und Verwaltung von Druckersicherheitsrichtlinien. Die Partnerschaft mit Cisco ermöglicht bessere Erkennungsfunktionen für Xerox®-Drucker und dadurch eine umfassendere Durchsetzung von Sicherheitsrichtlinien. Die automatische Erkennung und Einstufung von Xerox®-Geräten durch die Cisco ISE ermöglicht die Netzwerkzugriffskontrolle und eine effizientere Verwaltung, weil Druckerattribute nicht manuell eingegeben werden müssen. Die Druckerprofilerstellung mithilfe der Cisco ISE verhindert Spoofingangriffe und den Zugriff auf sensible Netzwerke durch Unbefugte. Durch die Einbindung der Cisco ISE in die Xerox®-Gerätetechnologie ist eine betrieblich effiziente Umsetzung der angestrebten Sicherheitsrichtlinien gewährleistet.

Compliance mit Vorschriften und Richtlinien

Bei modernen Druckern und MFD ist aufgrund der personenbezogenen und sensiblen Daten, die mit ihnen abgerufen, gespeichert und übermittelt werden, die Konformität mit Standards und Bestimmungen besonders wichtig. Ihre Nichteinhaltung kann zu eingebüßten Verkaufschancen und Kundenabwanderung führen oder sogar rechtliche Folgen haben. Die Anforderungen an die Regelkonformität sind je nach Land und vertikalem Markt unterschiedlich.

Das US-amerikanische Gesetz HIPAA (Health Insurance Portability and Accountability Act) für das Gesundheitswesen und das britische Datenschutzgesetz „Data Protection Act" sind Beispiele für Vorschriften, die von Unternehmen zwingend eingehalten werden müssen.

Die Zertifizierung nach Common Criteria ist ein internationaler Sicherheitsstandard, der den Vorgaben des US-Verteidigungsministeriums entspricht.

Dank branchenführender Sicherheitsmerkmale und einem flexiblen Ansatz bei der Konfiguration und Bereitstellung können Xerox®-Geräte jedem Standard entsprechen und lassen sich mit ihren Steuerelementen beliebigen Anforderungen anpassen.

Die Systeme, Softwareanwendungen und Serviceleistungen von Xerox® entsprechen branchenweit anerkannten Standards und den neuesten behördlichen Sicherheitsbestimmungen. Mit den Funktionen unserer Produkte sind unsere Kunden in der Lage, diese Standards zu erfüllen. Nachfolgend sind Beispiele für solche Standards aufgelistet:

- Payment Card Industry (PCI) Data Security Standard Version 3.0
- Sarbanes-Oxley
- Basel-II-Eigenkapitalvorschriften
- Health Insurance Portability and Accountability Act (HIPAA)
- EU-Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG)
- Gramm-Leach-Bliley Act
- Family Educational Rights and Privacy Act (FERPA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Dodd-Frank Wall Street Reform and Consumer Protection Act
- Common Criteria for Information Technology Security Evaluation (ISO 15408)
- Information Security Management System Standards (ISO 27001)
- Control Objectives for Information and Related Technology (COBIT)
- Statement on Auditing Standards No. 70 (SAS 70)
- NIST 800-53, 2014 von der US-Regierung und dem US-Verteidigungsministerium übernommen
- Federal Risk and Authorisation Program (FedRAMP)

Produktsicherheitsbewertung

Dokumentensicherheit bedeutet stressfreies Arbeiten. Eines der Markenzeichen des Xerox®-Produktportfolios ist die Verpflichtung zur Gewährleistung von Informationssicherheit. Die Systeme, Softwareanwendungen und Serviceleistungen von Xerox erfüllen branchenweit anerkannte Standards und die neuesten behördlichen Sicherheitsbestimmungen.

Zertifizierung nach Common Criteria

Die Common Criteria-Zertifizierung stellt eine objektive Prüfung der Zuverlässigkeit, Qualität und Vertrauenswürdigkeit von IT-Erzeugnissen durch unabhängige Dritte dar. Auf diesen Standard können Kunden vertrauen, um bei der Anschaffung von IT-Ausrüstung eine fundierte Entscheidung zu treffen. Die Common Criteria-Standards verlangen und bewerten die Erfüllung bestimmter Anforderungen an die Informationssicherheit und prüfen unter anderem die Integrität, Vertraulichkeit und Verfügbarkeit von Systemen und Daten sowie die individuelle Verantwortlichkeit in Bezug auf das Erreichen sämtlicher Ziele. Die Common Criteria-Zertifizierung ist eine Hardware- und Software-Anforderung für Sicherheitssysteme, die von Regierungsbehörden auf nationaler Ebene eingesetzt werden.

Erreichen der Common Criteria-Zertifizierung

Die Common Criteria-Zertifizierung ist ein rigoroses Verfahren, das Produkttests nach Sicherheitsanforderungen durch ein vom National Voluntary Laboratory Accreditation Program (NVLAP) akkreditiertes Fremdlabor umfasst. Die Produkte werden anhand von Anforderungen für Sicherheitsfunktionen gemäß vordefinierter EAL (Evaluation Assurance Level) oder spezialisierter Bewertungsanforderungen getestet.

Nicht weniger wichtig ist Sicherheit im Gesundheitswesen sowie im Finanzdienstleistungsbereich und anderen Branchen. Ob es um Kundendaten, geistiges Eigentum oder Anlagevermögen geht – der zuverlässige Schutz von Netzwerken, Festplatten und Telefonleitungen vor Angriffen durch Hacker, Viren und andere geschäftsschädigende Aktivitäten muss jederzeit gewährleistet sein. Zwar ist die Common Criteria-Zertifizierung außerhalb von Regierungsbehörden keine offizielle Auflage, jedoch kann sie unabhängige Bestätigung bieten.

Mit etwa 150 Geräten, für die das Zertifizierungsverfahren abgeschlossen wurde, verfügt Xerox über eines der umfangreichsten Portfolios von MFD mit Common Criteria-Zertifizierung. Darüber hinaus war Xerox der erste Hersteller, der das ganze Gerät zertifizieren ließ, und lässt bis heute als einziger Hersteller immer das gesamte Gerät zertifizieren.

Unter www.xerox.com/information-security/common-criteria-certified sind sämtliche Xerox®-MFD mit Common Criteria-Zertifizierung aufgelistet.

Risikobewertung und -minderung

Proaktiver Schutz vor neuen Bedrohungen

Die Bereitstellung der sichersten heute auf dem Markt verfügbaren Produkte und Lösungen ist nur ein Teil unserer Bemühungen. Unsere Wissenschaftler und Techniker arbeiten unermüdlich an der Entwicklung innovativer Sicherheitstechnologien der nächsten Generation, um zukünftige Bedrohungen zu bekämpfen und für zuverlässigen Dokumentenschutz zu sorgen. Mikro-Druck, FluorescentMark und Infrarot-Drucksicherheit, Xerox® GlossMark® und CorrelationMark sind nur einige dieser Innovationen. Weitere Informationen zu diesen Technologien finden Sie unter www.xerox.com/security.

Andere Initiativen von Xerox:

Beobachtung aktueller Risiken

Wir halten uns jederzeit über vorhandene und neue Schwachstellen auf dem Laufenden, um Ihnen diese Arbeit abzunehmen.

Herausgeben von Sicherheitsberichten

Wir stellen Ihnen proaktiv notwendige Sicherheitspatches und Updates bereit, damit Ihre Geräte jederzeit aktuell und Ihre Daten sicher sind.

Bereitstellen von RSS-Feeds

Minutenaktuelle Informationen werden automatisch an die RSS-Feedreader der Kunden übermittelt.

Umfassende Informationen für Sie

Wenn Sie selbst mehr lernen möchten, bieten wir Ihnen eine ständig erweiterte Bibliothek von sicherheitsrelevanten Artikeln, Whitepapers und Leitfäden.

Unter www.xerox.com/security finden Sie unser vollständiges Angebot von Sicherheitsressourcen.

Zusätzlich zu den eigenen intensiven Produkttests informiert sich Xerox kontinuierlich bei externen Organisationen und Ressourcen über Schwachstellen, wie etwa US-CERT und Oracle® Critical Patch Updates, Microsoft® Security Bulletins zu verschiedenen Anwendungen und Betriebssystemen sowie bugtraq, SANS.org und secunia.com für den Open-Source-Bereich. Unser robustes internes Sicherheitstestprogramm umfasst Schwachstellenanalyse und Penetrationstests, um vollständig getestete Patches bereitstellen zu können. Unter www.xerox.com/security finden Sie unsere Richtlinien zu Risikomanagement und Offenlegung.

Bereitstellung von Sicherheitsberichten und Patches

Die Entwicklungsarbeit bei Xerox folgt einem formellen Sicherheitsentwicklungszyklus, in dessen Rahmen Sicherheitsprobleme durch Identifizierung, Analyse, Priorisierung, Programmierung und Tests verwaltet werden. Wir bemühen uns, Patches je nach Art, Ursprung und Schweregrad der Schwachstelle so schnell wie möglich bereitzustellen. Abhängig vom Schweregrad der Schwachstelle, von der Patch-Größe und vom Produkt, wird der Patch möglicherweise separat als neue Softwareversion für dieses Produkt bereitgestellt.

Für bestimmte Xerox®-Produkte können Sicherheitspatches unter www.xerox.com/security heruntergeladen werden. Bei anderen Xerox®-Produkten werden Sicherheitspatches im Rahmen einer neuen Version der Systemsoftware bereitgestellt. Sie können Sicherheitsberichte abonnieren, um sie regelmäßig zu erhalten. In den USA sollten Kunden den RSS-Feed zu Sicherheit abonnieren. Kunden außerhalb der USA können sich an den Xerox-Kundendienst wenden.

Über die Website www.xerox.com/security können Sie jederzeit auf aktuelle Informationen und wichtige Ressourcen zugreifen:

- Sicherheitsberichte
- RSS-Feed: „Get Security Bulletins“
- Häufig gestellte Fragen zu Xerox®-Produktsicherheit
- Unterlagen zu Informationsgewährleistung und Offenlegung
- Produkte mit Common Criteria-Zertifizierung
- Richtlinien zu Risikomanagement und Offenlegung
- Produktsicherheitsleitfaden
- Artikel und Whitepapers
- Hinweise zu flüchtigem Speicher
- Übersichtstabelle zu Softwareversionen
- FTC-Leitfaden zu digitalen Kopierern und Multifunktionsdruckern

www.xerox.com/security ist Ihr Portal zu zahlreichen sicherheitsrelevanten Informationen und Updates, darunter Sicherheitsberichte, Whitepapers, Patches und vieles mehr.

Sicherheitspraktiken von Zulieferern in der Fertigung

Xerox und unsere wichtigsten Produktionspartner sind Mitglieder der Electronic Industry Citizenship Coalition (http://www.eicc.info). Durch die Verpflichtung zur Einhaltung des EICC-Verhaltenskodex belegen Xerox und andere Unternehmen, dass sie ihre Produktionsverfahren strengen Kontrollen unterstellen.

Darüber hinaus bestehen vertragliche Vereinbarungen zwischen Xerox und seinen primären und sekundären Zulieferern, in deren Rahmen Xerox vor Ort Audits zur Gewährleistung der Prozessintegrität bis hin zur Komponentenebene durchführen darf.

Zudem ist Xerox Mitglied der US-Initiative C-TPAT (Customs-Trade Partnership Against Terrorism), bei der es um die Sicherheit in der Lieferkette geht. Im Rahmen dieses Programms von Xerox implementierte Praktiken dienen der Vermeidung von Diebstahl und Entführungen. Innerhalb von Nordamerika werden sämtliche Lastanhänger zwischen Fertigungsstätten und Verteilzentren sowie zwischen Verteilzentren und Logistik-Zentren an ihrem Ausgangspunkt versiegelt. Sämtliche Lkw sind mit GPS-Ortungssystemen ausgestattet und werden kontinuierlich überwacht.

Produktretouren und Entsorgung

Hard Drive Retention (Festplattensicherheit) für Xerox®-Produkte

In den USA können Kunden beim Abgeben von geleasten Xerox®-Geräten deren Festplatten gegen eine Gebühr behalten. Dies ist sinnvoll für Kunden mit äußerst vertraulichen oder sogar geheimen Daten oder mit spezifischen internen Richtlinien oder Vorgaben zur Entsorgung von Festplatten.

Im Rahmen dieses Service besucht ein Xerox-Kundendiensttechniker den Kundenstandort, baut die Festplatte aus und übergibt sie unverändert einem Kundenvertreter. Dabei sorgt Xerox weder für eine sichere Löschung noch für eine Zerstörung der Festplatte. Kunden sind für die endgültige Entsorgung des Festplattenlaufwerks, das sie vom Techniker erhalten, selbst verantwortlich.

Um festzustellen, ob Ihr Xerox®-Produkt eine Festplatte enthält, oder um sich über verfügbare Funktionen zur Absicherung von Daten auf Festplatten zu informieren, besuchen Sie www.xerox.com/harddrive.

Weitere Informationen zu diesem Programm erhalten Sie von Ihrem Xerox-Partner, oder klicken Sie unter www.xerox.com/security im Abschnitt „Security Resources“ (Sicherheitsressourcen) auf den Link „Articles and White Papers“ (Artikel und Whitepapers).

Darüber hinaus bieten nahezu alle neuen Xerox®-Drucker und -MFD standardmäßig AES-Festplattenverschlüsselung mit 256 Bit sowie Festplattenüberschreibung mit drei Durchläufen, damit die Daten unserer Kunden auf ihren neuen Geräten von Anfang an zuverlässig geschützt sind.

Zusammenfassung

Netzwerk- und Datensicherheit zählen zu den größten täglichen Herausforderungen für Unternehmen. Und da es sich bei modernen Druckern und MFD um geschäftskritische Netzwerkgeräte handelt, die wichtige Daten über verschiedene Funktionen empfangen und senden, ist umfassende Sicherheit ein Muss.

Das gesamte System von Multifunktionsdruckern sowie die Gerätemanagementsoftware im Netzwerk müssen evaluiert und zertifiziert werden, damit die Informationssicherheit und alle Mitarbeiter einer Organisation sich sicher sein können, dass ihre Dokumente und das Netzwerk sicher und vor Hackern oder gar vor internen Datenschutzverstößen geschützt sind. In dieser Hinsicht sind Xerox®-MFD führend. Unser umfassender Ansatz, der auf grundlegender, funktioneller, fortschrittlicher und praxisrelevanter Sicherheit basiert, ist daher unverzichtbar, um die Informationsressourcen unserer Kunden zu schützen.

Aus diesem Grund achtet Xerox bei Entwicklung und Design sämtlicher Produkte darauf, an allen potenziellen Schwachstellen größtmögliche Sicherheit zu gewährleisten. Wir verpflichten uns dem Schutz Ihrer Daten, damit Sie sich voll und ganz auf Ihr Kerngeschäft und den Erfolg Ihres Unternehmens konzentrieren können.

Weitere Informationen zu den zahlreichen Sicherheitsvorteilen von Xerox finden Sie unter www.xerox.com/security.

Sicherheitscheckliste

IT-Sicherheitsmanager werden schon jetzt stark beansprucht, wenn es darum geht, die Sicherheitsanforderungen zu erfüllen. Kleine Unternehmen müssen sich in diesem Bereich auf effektive Systeme und Sicherheitssoftware verlassen. Was Sie und Ihre Mitarbeiter am wenigsten gebrauchen können, sind aufwendige manuelle Verfahren, um jedes Gerät und jeden Datenstrom in Ihrer Umgebung, darunter auch Ihre MFD und Drucker, zu überwachen und zu aktualisieren.

Ein umfassendes Konzept für Netzwerksicherheit muss drei Schwerpunkte abdecken, um in der Praxis funktionieren zu können:

1. Vollautomatisch und ohne Eingreifen vor neuen Angriffen geschützte Geräte
2. Compliance mit den neuesten Sicherheitsstandards und -richtlinien
3. Vollständige Transparenz im Netzwerk

Der neue Sicherheitsstandard für ein neues Zeitalter

- Sicherheit darf kein Nebengedanke sein.
- Informationen gewinnen als geistiges Eigentum zunehmend an Wert.
- Firewalls reichen nicht aus – Sicherheitsrichtlinien müssen ganzheitlich und umfassend sein.
- Der Schutz von integrierten Geräten ist ein zentraler Bestandteil moderner Sicherheitskonzepte.

Xerox bietet umfassende, mehrstufige Sicherheit, die sich einfach bereitstellen und implementieren lässt und für die Compliance Ihres Unternehmens mit Branchenstandards und gesetzlichen Vorgaben sorgt. Xerox®-Technologie wird umfassend getestet und überprüft, um Daten und Identitäten zuverlässig vor dem Zugriff durch Unbefugte zu schützen.

Mithilfe der folgenden Checkliste können Sie MFD von Xerox® mit denen anderer Hersteller vergleichen und ermitteln, ob die Geräte der Mitbewerber eine ähnlich umfassende Sicherheit bereitstellen.

		Mitbewerber		
	Xerox	**1**	**2**	**3**
IP-/MAC-Adressfilterung	✓			
IPsec-Verschlüsselung	✓			
IPv6	✓			
802.1X-Authentifizierung	✓			
Geschützte Ausgabe	✓			
Scanausgabe: E-Mail – Verschlüsselung	✓			
Verschlüsseltes/ kennwortgeschütztes PDF	✓			
Digitale Signaturen	✓			
256-Bit-AES-Festplattenverschlüsselung	✓			
Festplattenüberschreibung	✓			
Geschütztes Fax	✓			
Portsperre	✓			
Scanausgabe: Mailbox – Kennwortschutz	✓			
Hard Drive Retention (Festplattensicherheit)	✓			
Druckeinschränkungen	✓			
Prüfprotokoll	✓			
Rollenbasierte Zugriffssteuerung	✓			
Smartcard-Authentifizierung	✓			
Common Access Card/ Personal Identity Verification (CAC/PIV)	✓			
Benutzerberechtigungen	✓			
Common Criteria-Zertifizierung (ganzes System)	✓			
Integration mit Standardtools für Netzwerkmanagement	✓			
Sicherheitsupdates über RSS-Feeds	✓			
Embedded McAfee Protection Powered by Intel® Security	✓			
McAfee® Integrity Control	✓			
McAfee® ePolicy Orchestrator® Integration	✓			
Integration der Cisco® Identity Services Engine (ISE)	✓			

Weitere Informationen finden Sie unter **www.xerox.com**.

05/18 BR21699 SECGD-01GC