Ein umfassendes Konzept für Druckersicherheit.

Drucker und Multifunktionsgeräte sind heute in der Lage, zentrale Aufgaben im geschäftlichen Alltag zu übernehmen. Angesichts der exponentiellen Zunahme von WLAN-Geräten, cloudgestützter Software und Clouddiensten muss ein Drucker nicht nur für diese Technologien gerüstet, sondern auch gegen die Gefahren gewappnet sein, die von ihnen ausgehen können.

GANZHEITLICHER SCHUTZ FÜR IHREN DRUCKER

Wir bei Xerox haben den technologischen Wandel und die sich ändernden Anforderungen am Arbeitsplatz schon vor langer Zeit erkannt und uns darauf eingestellt. Wir bieten umfassende Sicherheitsfunktionen, damit Ihre Drucker und Daten sicher sind. Darüber hinaus schützen wir jeden Teil der Datenkette, einschließlich **Drucken, Kopieren, Scannen, Fax, Dateidownloads** und **Systemsoftware**. Unser mehrschichtiger Ansatz umfasst vier Schlüsselaspekte.

VORBEUGUNG

Die erste und naheliegendste Schwachstelle ist die Bedienungsoberfläche und die Kontrolle darüber, wer physischen Zugriff auf Ihren Drucker und seine Funktionen hat. Die Sicherheitsmaßnahmen von Xerox beginnen mit der Verhinderung von Angriffen durch **Benutzerauthentifizierung**. So wird gewährleistet, dass nur autorisierte Personen Zugriff auf die Geräte haben. Nach der Anmeldung wird durch die **rollenbasierte Zugriffssteuerung** sichergestellt, dass jedes Teammitglied nur die Funktionen sieht, die Sie freigegeben haben. Die Aktivierung **starker und komplexer Kennwörter** schützt vor Hackern und schadhafter Software. Die Unterstützung der **Multi-Faktor-Authentifizierung**[1] bietet eine weitere Sicherheitsebene. Jede Aktion eines jeden Benutzers wird protokolliert, wodurch ein vollständiger **Audittrail** gewährleistet ist.

Danach kümmern wir uns um weniger offensichtliche Schwachstellen – was wird an den Drucker gesendet und wie? Unsere Systemsoftware ist **digital signiert**. Jeder Versuch, eine infizierte, nicht signierte Version zu installieren, führt dazu, dass die Datei automatisch abgelehnt wird. Verschlüsselte Schlüssel werden auf TPM-Chips gespeichert, um Drucker vor Cyberangriffen zu schützen.

xerox™

ERKENNUNG

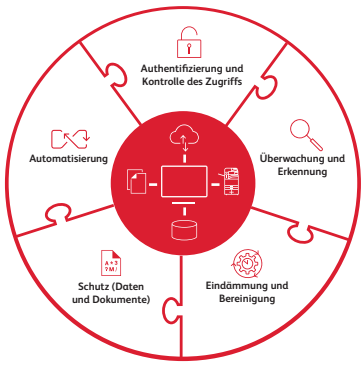
Im unwahrscheinlichen Fall, dass die Daten- und Netzwerkschutzmechanismen überwunden werden, führt die Xerox® ConnectKey® Technologie einen umfassenden **Test zur Firmware-Verifizierung** aus. Dies geschieht entweder beim Systemstart oder auf Anforderung durch einen autorisierten Benutzer. Hierbei werden Sie gewarnt, wenn schädliche Änderungen an Ihrem Drucker erkannt wurden. Unsere hochmodernen, integrierten Lösungen verwenden die **Trellix Allowlisting**[2]-Technologie. Damit wird das System permanent auf Malware überprüft und automatisch verhindert, dass diese ausgeführt werden kann. 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. Xerox®-Geräte werden in marktführende SIEM-Softwaretools[3] integriert, um Sicherheitsereignisdaten in Echtzeit zu kommunizieren. Dies hilft bei der frühzeitigen Erkennung von Sicherheitsverletzungen und verhindert oder mindert potenziellen Schaden durch Sicherheitsbedrohungen für das Unternehmen.

SCHUTZ

Mit unseren umfassenden Sicherheitslösungen sind Ihre gedruckten und gescannten Dokumente vor unbefugter Offenlegung bzw. unbefugten Änderungen geschützt. Die Xerox® ConnectKey® Technologie dient dazu, die absichtliche oder versehentliche Übertragung wichtiger Daten an Personen zu sperren, die für den Zugriff darauf nicht autorisiert sind.

Wir schützen die Druckausgabe mit einem **PIN-Code** oder einem **kartenbasierten** Freigabesystem. Wir beschränken den Zugriff Unbefugter auf Scaninformationen, indem wir **digital signierte, verschlüsselte und kennwortgeschützte Dateiformate** verwenden. Bei Druckern mit ConnectKey Technologie können Sie die **E-Mail**-Felder **An/Kopie/Blindkopie** sperren, um das Scanziel auf **interne Adressen** zu begrenzen.

Wir schützen Ihre gespeicherten Informationen mit einer **Verschlüsselung** auf höchstem Niveau. Nicht mehr benötigte Daten, die auf dem Gerät verarbeitet oder gespeichert wurden, werden mithilfe von Algorithmen zur **Datenbereinigung** und **Datenlöschung** gelöscht. Diese erfüllen die strikten Vorgaben des US-amerikanischen National Institute of Standards and Technology (NIST) und des US-Verteidigungsministeriums.[4]



XEROX UNTERSTÜTZT ZERO TRUST

Mit einer Kombination aus Hardware, Software und Prozessen unterstützen wir Ihre Zero-Trust-Initiativen, um die Implementierung einfacher und umfassender zu gestalten.

Erfahren Sie mehr unter: www.xerox.de/de-de/uber-uns/sicherheitslosungen/zero-trust-sicherheits

EXTERNE PARTNERSCHAFTEN

Wir arbeiten mit Organisationen zusammen, die Compliance-Tests durchführen, sowie mit branchenführenden Sicherheitsunternehmen wie **Trellix und Cisco**, um deren umfassende Standards und Expertise in die Angebote von Xerox zu integrieren.

Unabhängige Dritte – z. B. Zertifizierungsstellen wie **Common Criteria (ISO/IEC 15408)** und **FIPS 140-2/140-3** 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.

Unser Programm „Bug Bounty“[5] mit HackerOne ist ein weiterer Beweis dafür, wie wichtig Sicherheit für uns ist und stellt eine unabhängige Ressource zur Technologievalidierung dar.

Trellix cisco splunk> LogRhythm hackerone

EINFACH ZU IMPLEMENTIERENDE UND ZU VERWALTENDE SICHERHEIT

Wählen Sie eines der vordefinierten Sicherheitsprofile (Standard, Erhöht oder Hoch) und der Drucker konfiguriert automatisch die entsprechenden Sicherheitseinstellungen. Überwachen Sie bis zu 75 Sicherheitseinstellungen mit Configuration Watchdog. Werden nicht autorisierte Änderungen erkannt, werden diese Einstellungen automatisch zurückgesetzt. Dadurch spart das IT-Personal Zeit und muss sich keine Gedanken mehr über die Implementierung und Einhaltung von Sicherheitsvorschriften machen.

[1] Multi-Faktor-Authentifizierung wird über Xerox® Workplace Solutions und Cloud IdPs aktiviert

[2] Xerox® AltaLink®-Geräte, Xerox® VersaLink® C415 Multifunktions-Farbdrucker / B415 Multifunktionsdrucker und C625 Multifunktions-Farbdrucker / B625 Multifunktionsdrucker, Xerox® VersaLink® C620 Multifunktions-Farbdrucker / B620 Drucker, Multifunktionsdrucker der Xerox® VersaLink® 7100-Serie und Multifunktionsdrucker der Xerox® EC7800/8000-Serie

[3] Trellix Enterprise Security Manager, LogRhythm und Splunk SIEM Tools

[4] Gilt nur für Geräte mit Festplattenlaufwerken

[5] „Bug Bounty“ wird über HackerOne auf Multifunktionsdruckern der Xerox® AltaLink®-Serie angeboten, wobei in Zukunft weitere Produkte, Lösungen und Dienstleistungen hinzugefügt werden sollen

Erfahren Sie mehr unter: **www.xerox.de/de-de/uber-uns/sicherheitslosungen**