bitkom


Neuauflage
2024

# Sicherheit von Drucksystemen

Die Sicherheit von Drucksystemen und Multifunktionsgeräten

# Inhalt

# Vorwort

Die Sicherheit von Drucksystemen und Multifunktionsgeräten (im Folgenden kurz »Drucker« genannt) wird oftmals in Unternehmen vernachlässigt. Dabei ist ein hoher Sicherheitsstandard im Kontext seiner wirtschaftlichen Nutzung zwingend vorgeschrieben. Denn Druckern werden vertrauliche Informationen anvertraut, die auch häufig personenbezogene Daten beinhalten, deren Vertraulichkeit gewahrt bleiben muss. Gesetze und Vorschriften wie beispielsweise BDSG, § 203 StGB oder EU-DSGVO regeln dies sogar sehr genau, und Verstöße können nicht nur kostspielig werden, sondern sind teilweise auch mit Haftstrafen belegt.

Dieser Leitfaden ist eine Neuauflage des 2019 veröffentlichten Leitfadens. Bei der Aktualisierung haben wir die veränderten geopolitischen Rahmenbedingungen berücksichtigt und die Kapitel überarbeitet.

# 1 Die Wahrnehmung von Drucksystemen

Grundsätzlich hängt die Sicherheit von Drucksystemen stark von deren Konfiguration ab. Daher sollte schon bei der Beschaffung von Druckern auf vorhandene Sicherheitsfunktionen geachtet werden und diese nach dem benötigten Sicherheitsniveau ausgewählt bzw. konfiguriert werden. Nicht jeder Drucker ist für jedes Sicherheitsbedürfnis geeignet.

Der vorliegende Leitfaden beschreibt typische, in der Praxis vorkommende Sicherheitsrisiken und beschreibt Maßnahmen, wie man diesen Bedrohungen (proaktiv) begegnen kann.

Bevor wir auf die Details einzelner Bedrohungsszenarien eingehen, muss klar herausgestellt werden, dass es drei übergeordnete Aspekte gibt, die diese Bedrohungen in Kombination oder einzeln erst ermöglichen bzw. begünstigen:

1. Drucker werden nicht als integraler Teil der IT-Infrastruktur angesehen

Seit geraumer Zeit sind Drucker technisch betrachtet ebenso IT-Systeme wie z. B. Server. Sie unterscheiden sich nur dadurch, dass sie auch drucken können und in der Regel nicht so leistungsfähig sind. Auch auf Druckern laufen Betriebssysteme, die Software ausführen; oftmals sind auch Festplatten verbaut, auf denen häufig sensible und/oder personenbezogene Daten (Druckjobs, Adressbücher, Protokolle usw.) gespeichert sind. Daraus folgt, dass Drucker ebenfalls in das IT-Sicherheitskonzept des Unternehmens eingebunden werden müssen.

Jedoch werden Drucker bis heute als »harmlose« technische Geräte angesehen, die nichts mit der »richtigen« IT-Infrastruktur zu tun haben. Hinzu kommt, dass die Verantwortlichkeit für Drucker im Unternehmen in vielen Fällen nicht klar geregelt ist und sie schwebt zwischen Zentralen Diensten, Fachbereichen und IT.

2. Die Mächtigkeit von Seitenbeschreibungssprachen wird unterschätzt

Um die zu druckenden Inhalte einem Drucker verständlich zu machen, werden spezielle Programmiersprachen – sogenannte Seitenbeschreibungssprachen – verwendet. Neben PCL (Printer Command Language) hat sich auch Postscript (PS) zu einem Industriestandard entwickelt. Doch die Mächtigkeit vieler dieser Sprachen ist den meisten Anwendern nicht bewusst. Sie sind nicht nur Seitenbeschreibungssprachen, sondern »Turing-vollständige« Programmiersprachen. Das bedeutet, dass sie unabhängig von Druckanwendungen für jede Art der Programmierung genutzt werden kann – auch für Schadsoftware.

3. Datenschutzgerechte Dokumentenausgabe wird nicht / unzureichend unterstützt

Nicht zuletzt seit Inkrafttreten der DSGVO endet der Druckprozess nicht mehr schon mit der Ausgabe des Druckerzeugnisses im Auslagefach, sondern erst dann, wenn der tatsächlich Berechtigte sein Dokument in Empfang nimmt. Analoges gilt für die Entgegennahme einer Fax-Nachricht.

Um dieses Ziel zu erreichen, sind verschiedene organisatorische Lösungen denkbar, deren durchgängige Durchsetzung aber oftmals in der Praxis kaum möglich ist; erfolgversprechend sind sog. »Secure- oder Pull-Printing«-Lösungen. Dabei werden Druckjobs zwar sofort verarbeitet, aber dann zunächst nur in einer Queue

zwischengespeichert. Der eigentliche Ausdruck erfolgt erst dann, wenn sich der Berechtigte am Drucker seiner Wahl authentifiziert hat. Diese Authentifizierung kann über die persönliche Unternehmenszugangskarte, das Smartphone oder biometrische Merkmale erfolgen. Die singuläre Verwendung eines PIN-Codes entspricht nicht mehr dem Stand der Technik.

# 2 Die neuen Realitäten

Seit der ersten Veröffentlichung dieses Leitfadens hat sich die geopolitische Lage dramatisch verändert. Mit dem Beginn des russischen Angriffskrieges auf die Ukraine hat nicht nur die »kinetische« Bedrohung ein neues Niveau erreicht. Auch im Sinne einer hybriden Kriegsführung sind die Cyberangriffe auf einem nie dagewesenen Niveau; sowohl in Quantität und Qualität. Die Cyberattacken treffen uns permanent auf allen Ebenen des öffentlichen Lebens, der Verwaltung und des Wirtschaftslebens.

In diesem Kontext ist auch das Kommando CIR der Bundeswehr, die sich um die »staatstragenden« Bedrohungen in der Cyberwelt kümmert, zu einer eigenen »Dimension« (ehemals: Waffengattung) aufgestiegen. In diesem kritischen Umfeld ist für Unternehmen jeder Größe besonders wichtig, sich mit allen Mitteln gegen Cyberbedrohungen aller Art zu schützen.

Dies gilt auch ganz besonders für Drucksysteme. Denn schon in der ersten Ausgabe dieses Leitfadens haben wir festgestellt, dass »Drucker bis heute als ‚harmlose' technische Geräte angesehen werden, die nichts mit der ‚richtigen' IT-Infrastruktur zu tun haben.« Diese fatale Haltung wird zurzeit durch ein weiteres Paradigma sogar noch deutlich verstärkt:

»Es wird doch nichts mehr gedruckt.«

Auch wenn dieses Statement oft »nur« plakativ einen hohen Stand der Digitalisierung dokumentieren soll, hat es auch eine fatale psychologische Dimension. Denn dadurch werden Drucker eher noch weniger ernst genommen – ebenso wie die erforderlichen Sicherungsmechanismen – »für die paar Seiten«...

> Drucksysteme als Ziel von Angriffen werden oft unterschätzt, obwohl Drucker für Unternehmen weiterhin essenziell bleiben.

**71%**

der Unternehmen sehen das Drucken als »sehr wichtig« oder »kritisch" für ihr Unternehmen an.

Aber das Gegenteil ist der Fall: 71 % der Unternehmen sehen das Drucken als »sehr wichtig« oder »kritisch" für ihr Unternehmen an[1]; d. h. wir müssen auf allen Ebenen unsere Abwehrmaßnahmen stabilisieren und stärken – auch bei Druckern. Erst wenn wirklich »die letzte Seite gedruckt ist« und die Drucker vom Netz gehen, gibt es kein diesbezügliches Bedrohungsszenario mehr.

Die folgenden Kapitel beschreiben typische, in der Praxis vorkommende Sicherheitsrisiken und Maßnahmen, wie man diesen Bedrohungen (proaktiv) begegnen kann.

# 3 Der Inhalt von zu druckenden Dokumenten kann ausgelesen werden

Grundsätzlich kann jegliche Art von unverschlüsselter Kommunikation in Netzwerken (LAN / WLAN) durch Dritte »abgehört« und interpretiert werden. Dazu zählt auch die Eingabe von Passwörtern bzw. die Übertragung von vertraulichen Druckdaten oder auch gescannten Dokumenten.

Daher sollte die Verschlüsselung sowohl die Druckdateien selbst (Dateiverschlüsselung) als auch die Datenübertragung (Transportverschlüsselung) umfassen. Allgemein haben sich in der Praxis Transportverschlüsselungen bewährt, die einen geschützten Kanal auch für (ungeschützte) Nutzdaten bereitstellen. Bekannt sind hier die Protokolle SSL / TLS oder IPSec. Nur eine Kombination aus Transport- und Nutzdatenverschlüsselung bietet zuverlässigen Schutz.

Weiterhin könnten Druckdaten aus dem Drucksystem ausgelesen werden. Dieses gilt auch für verschlüsselt übertragene, aber im Gerät wieder entschlüsselte Druckdaten. Das System muss also auch gegen das Auslesen von Dateien gesichert werden; die jeweiligen Verfahrensweisen sind jedoch gerätespezifisch.

[1] Print Security Landscape, 2024, Quocirca

# 4 Das Drucken kann behindert oder verhindert werden

Manipulierte Druckaufträge können zu Störungen des Drucksystems führen (beispielsweise Auslösen von Massenausdrucken, unendliche Schleifen, etc.). Die Quellen dieser Druckaufträge können sowohl organisationsintern als auch extern (etwa der Angriff aus dem Internet, Cross-Site-Scripting (s. u.) etc.) sein.

Die generelle Verhinderung von Massenausdrucken kann unter Umständen schwierig sein, da in diesem Fall eventuell eine notwendige Funktion wie die Druckwiederholung missbraucht wird. Daher sollte darauf geachtet werden, dass Drucker ihre Aufträge nur von vorher zugelassenen Quellen annehmen. Dieses kann zum Beispiel über ein separiertes Druckernetzwerk mit einem zentralen Druckserver oder vordefinierten IP-Adressen geschehen. Keinesfalls sollten Drucker ungeschützt über das Internet erreichbar sein; die Drucker gehören grundsätzlich hinter die Firewall.

# 5 Schutz des Druckers und der Daten durch Authentifikation

## Administrator / Maintenance Zugang

Der Zugang sollte über verschiedene Rollen geregelt werden (z. B. Systemadministration, Sicherheitsadministration, Service etc.), um die allumfassend berechtigte Administratorrolle nicht inflationär benutzen zu müssen. Generell sollten alle Zugangsdaten in regelmäßigen Abständen geändert werden, um einen Missbrauch zu erschweren.

## Zugriff auf Drucker-Konfigurationsoberfläche via eingebauten Webserver

Moderne Drucksysteme lassen sich in der Regel über eine Weboberfläche konfigurieren und administrieren. Das ermöglicht grundsätzlich folgende Angriffe:

- Login über werkseitig vergebenes Passwort, das nicht geändert wurde
- Brute-Force-Angriff auf Anmeldedaten (d. h. automatisiertes Durchprobieren)
- Ausspähen von Anmeldedaten über das Netzwerk bei unverschlüsselten Verbindungen
- Ausnutzen von IT-Sicherheitslücken des internen Webservers des Druckers

Folgende Gegenmaßnahmen sind zur (proaktiven) Abwehr dieser Angriffe zu empfehlen:

- Die Drucksysteme müssen durch Firmware und Sicherheits-Updates stets auf dem aktuellen Stand gehalten werden
- Brute-Force-Angriffe auf Username und Passwort verhindern, indem der Webserver so konfiguriert wird, dass die Anzahl der fehlgeschlagenen Login-Versuche begrenzt und die Zeitdauer zwischen möglichen Login-Versuchen schrittweise vergrößert oder nur eine kleine Anzahl von Falscheingaben überhaupt zugelassen wird
- Verschlüsselung der Kommunikation mit dem Webserver aktivieren (= HTTPS-Zugriff) und unverschlüsselte Kommunikation (= HTTP-Zugriff) deaktivieren, beispielsweise per Konfiguration des Webservers oder »Redirect« auf die verschlüsselte Verbindung
- Generell nur individuelle und hinreichend komplexe Passwörter zulassen; zur Generierung sicherer Passwörter sollten verbindliche Passwortregeln (inklusive der Häufigkeit des Wechselns) vorgegeben werden. Es ist unbedingt darauf zu achten, dass das im Auslieferungszustand bereits vorhandene Passwort unverzüglich geändert wird.
- So weit möglich empfiehlt es sich, eine Beschränkung auf bestimmte IP- oder MAC-Adressen oder Netzsegmente vorzunehmen. Diese Konfiguration kann meistens am Drucker selbst oder sonst in der Konfiguration des Netzwerks, an das der Drucker angeschlossen ist, vorgenommen werden.

- Soweit technisch zutreffend sollte es in der Nutzerverwaltung zumindest eine Aufteilung in eine Administratorrolle und eine »normale« Nutzerrolle mit abgestuften Rechten geben. Hierfür sind getrennte Logins notwendig.
- Wenn möglich, Verwendung einer 2-Faktor-Authentifizierung zumindest für Administrator-/Sicherheitsadministrator – Passwort / PIN – am besten zufallsgenerierte PINs (z. B. via Smartphone und Authenticator-App, auch um die Phishing-Problematik zu umgehen)

## Zugriff auf die Konfiguration des Druckers über alternative Protokolle

Oft werden weitere Protokolle wie SSH, RSH, Telnet, VNC von den Systemen unterstützt. Generell ist zu empfehlen, sich für ein favorisiertes Protokoll zu entscheiden und alle Alternativen zu deaktivieren.

## Unberechtigte Nutzung von Drucksystemen

Generell sollte die Nutzung zumindest von Gruppen und Abteilungssystemen nur nach erfolgter Authentifizierung zugelassen werden.

### Passwörter und Timeouts

Nur aktuelle Passwortrichtlinien und -regeln sollten vorgegeben und triviale Passwörter generell nicht zugelassen werden. Ferner erhöhen kurze Timeouts mit einer automatischen Abmeldung die Sicherheit. Hier muss ein Kompromiss zwischen dem Sicherheitsbedarf und Komfort bei der Nutzung gefunden werden.

### Audiovisuelle Hinweise

Fehleingaben bei Authentifizierungsversuchen am Drucksystem sollten möglichst sicht- und hörbar signalisiert werden, damit die Umgebung auf mögliche Missbrauchsversuche hingewiesen wird. Bei vielen Geräten lässt sich konfigurieren, wie oft etwa ein Passwort falsch eingegeben werden darf, bevor eine Sperrung erfolgt. Unabhängig davon muss ein angemeldeter Benutzer nach einer angemessenen Zeitspanne nach Verlassen des Gerätes automatisch abgemeldet werden.

## (Zugangs-) Karten und Dongle

Eine komfortable Anmeldemethode ist die Verwendung von Karten oder Dongles, bei denen ohnehin verfügbare Authentifikationsmittel Verwendung finden. Dazu muss der (Multifunktions-) Drucker mit einem Kartenlesegerät ausgestattet werden.

## Detailliertes Rechtemanagement auf Anwender- oder Funktionsebene

Rechte in der Nutzung der Systeme sollten so beschränkt werden, dass eine Minimierung der individuellen Rechte am System erfolgt (nicht jeder braucht jede Funktion), z. B. nur Secure Print – in welcher Form auch immer – sollte möglich sein, Scannen an die eigene E-Mail-Adresse oder an fest definierte Ziele – nicht an jede Adresse, weiterhin ein limitierter Adressbuchzugriff oder Rufnummern-Bestätigung beim Faxen, um einen ungewollten Datenabfluss zu verhindern.

Es gibt folgende Formen des Rechtemanagements:

- Zutrittskontrolle: Sicherstellen, dass Unbefugten der physische Zutritt zu den Geräten verwehrt wird
- Zugangskontrolle: Sicherstellen, dass Unbefugten die Nutzung der Geräte oder einzelner Funktionen verwehrt wird
- Zugriffskontrolle: Sicherstellen, dass Nutzer ausschließlich auf die Daten zugreifen können, für die sie eine Berechtigung haben
- Weitergabekontrolle: Sicherstellen, dass Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, verändert, kopiert oder gelöscht werden können

## Flexible Anwender-Authentifikation und -Anmeldung bei mobilen Endgeräten

Der Zugang zu Netzwerkdruckern kann entweder am Gerät bzw. Bedienpanel (lokale Authentifizierung) oder über das Netzwerk bzw. die Weboberfläche (Netzwerkauthentifizierung) erfolgen.

Beide Zugangsmöglichkeiten werden in der Regel von den Herstellern mit Tastenkombinationen sowie mit PIN und / oder Benutzernamen / Passwort versehen. Hier gilt es, die Standard-Pins / -Passwörter durch eigene zu ersetzen, da sich die Standard-Pins / -Passwörter meistens leicht im Internet finden lassen.

Die Netzumgebung sollte so konfiguriert sein, dass sie nur autorisierte IT-Systeme als Quelle von Druckaufträgen zulässt.

Die Nutzung am Gerät (Drucken, Scan, Faxen, Kopieren, Menübedienung) sollte auf berechtigte Personen beschränkt sein. Eine Authentifizierung kann beispielsweise über eine auf der Maschine befindliche Datenbank, über einen Druckserver oder eine zusätzliche Software (z. B. Secure-/ Pull-Printing) erfolgen. Eine zentrale Verwaltung bietet den Vorteil, dass mit eigenen Active-Directory-Richtlinien, LDAP oder Kerberos gearbeitet werden kann. Wegen der zunehmenden Nutzung von Cloud-Services und dem Datenzugriff auch von unterwegs werden zudem die Druckanforderungen immer »mobiler«. Mitarbeitende drucken von unterwegs oder von externen Standorten über Geräte außerhalb ihrer Abteilung. Das Drucken soll dabei über jedes beliebige Gerät innerhalb eines Unternehmens bzw. an verschiedenen Unternehmensstandorten auf sichere Weise möglich sein. In allen Fällen muss gewährleistet werden, dass kein Schadcode von mobilen Endgeräten auf die Drucker gelangen kann. Ein Einfallstor stellt die von vielen Druckern angebotene direkte Funkverbindung (z. B. Bluetooth oder ad-hoc-WLAN, oft in Verbindung mit der Verbindungssuche über NFC) dar. Diese Verbindungen sollten nur so lange aktiviert werden, wie sie auch tatsächlich benötigt werden. Es sollte darauf geachtet werden, dass insbesondere Multifunktionssysteme nicht über ungeschützte Schnittstellen erreichbar sind.

Mitarbeitende können mit ihrem eigenen Mobilgerät (das Konzept des »bring your own device«, BYOD) im Firmennetz eingebucht sein. Dadurch ist der Zugriff auf die Drucker im Firmennetz möglich, da diese Mobilgeräte bereits autorisiert sind. Wichtig ist dabei, dass diesen Endgeräten die zum betreffenden Mitarbeitenden gehörenden Rechte und Unternehmensrichtlinien zugewiesen werden. Nur so lassen sich die Gefahren, die durch eine Nutzung der Drucker über das Unternehmensnetzwerk hinaus entstehen können, wirkungsvoll abwenden.

## Gastzugang

Gästen kann man über einen eigenen Zugang (z. B. Bluetooth, gesichertes WLAN, ggf. mit Verbindungssuche über NFC) ohne Verbindung zum Firmennetz das Drucken über deren Mobilgeräte ermöglichen. Alternativ kann auch eine Print-Management-Lösung mit Gästedruckfunktion verwendet werden.

## Verhinderung eines Datenverlustes durch Authentifikation am Drucksystem

Um offen in der Ablage liegende Ausdrucke zu vermeiden oder das Scannen und Versenden an unautorisierte Adressen zu unterbinden, ist eine Authentifikation des Nutzers notwendig.

### Authentifikation und sicheres Drucken

Nur mit seiner Authentifizierung an einem Drucker sieht ein Nutzer ausschließlich seine eigenen Druckjobs, die dann automatisch oder nach individueller Freigabe in seiner Anwesenheit gedruckt werden.

### Authentifikation und sicheres Scannen

Nur mit einer Authentifikation lassen sich sichere Scan-Ziele (z. B. Senden an die eigene E-Mail-Adresse oder das eigene Verzeichnis) mit dem Anwender verknüpfen. Meistens reicht dann die Auswahl einer einzelnen Funktionstaste, um den Scan-Vorgang auszuführen.

# 6 Schutz des Datenträgers

## Sichere Löschung von Druck-/Scan-Jobs bei Systemen mit Festplatte (HDD)

Der Drucker sollte so konfiguriert sein, dass nach Abschluss des Druckjobs die temporären Druck-/Scan-Daten auf dem eingebauten Datenträger automatisch sicher gelöscht werden, d. h. nicht wiederherstellbar sind. Dann laufen auch Attacken auf den Datenträger ins Leere. Hinweis: Systeme mit SSD sind technologiebedingt automatisch so konfiguriert – eine separate Löschung von temporären Daten ist häufig nicht nötig.

## Festplattenverschlüsselung

Moderne Drucksysteme verwenden zur Sicherung der gespeicherten Daten eine permanente, nicht abschaltbare Festplattenverschlüsselung, um den nicht autorisierten Zugriff auf abgelegte Daten zu verhindern. Als zusätzliche Maßnahme kommen bei vielen Herstellern eigene proprietäre Dateisysteme oder die Entkopplung von Index- und Nutzdaten zum Einsatz. Das marktübliche Verschlüsselungsverfahren (Stand 2024) ist AES256.

Auf jeden Fall sollte darauf verzichtet werden, Druck- und Scanjobs unverschlüsselt auf der Systemfestplatte zu speichern.

## Physische Entfernbarkeit des Datenträgers

Generell ist die Entfernbarkeit der internen Festplatte eine zusätzliche Sicherheitsoption, damit nach Nutzungsende (beispielsweise auch Miet- oder Leasingende) die Hoheit über die Festplatte auch nach Rückgabe oder Verkauf des Gerätes erhalten bleibt. Die Nutzung dieser Option wird vor allem in besonders sicherheitsrelevanten Bereichen empfohlen. Einige Hersteller nutzen zusätzlich eine Datenträgersperre, die bei der Entnahme des Datenträgers zusätzlich ein Auslesen der Inhalte erschwert.

## Festplattenverschlüsselung

Moderne Drucksysteme verwenden zur Sicherung der gespeicherten Daten eine Festplattenverschlüsselung, um den nicht autorisierten Zugriff auf abgelegte Daten zu verhindern. Als zusätzliche Maßnahme kommen bei vielen Herstellern eigene proprietäre Dateisysteme oder die Entkopplung von Index- und Nutzdaten zum Einsatz. Der Aufwand lohnt sich natürlich nur, wenn ein wirksames Verschlüsselungsverfahren eingesetzt wird; in der Praxis (Stand Dezember 2018) hat sich hier AES256 bewährt.

Auf jeden Fall sollte auf bekannte bzw. extern lesbare Dateisysteme ohne Verschlüsselung generell verzichtet werden.

## Schutz kritischer Daten auf der HDD/SSD

Kritische Daten wie z. B. Passwörter oder System- & Anwenderzertifikate sollten besonders geschützt durch ein TPM-Modul gespeichert werden.

## Datenlöschung am Ende der Nutzungsdauer

Aktuelle Drucksysteme mit HDD/SSD verfügen über eine Löschfunktionalität, die es dem Nutzer ermöglicht, am Ende der Nutzungsdauer selbst alle relevanten Daten nicht wiederherstellbar zu löschen und damit DSGVO-konform zu handeln.

# 7 Schutz des Drucksystems und damit des Netzwerks vor Malware

Moderne Drucksysteme sind heute spezialisierte PCs mit angeschlossenen Druckwerken und Scanner-Einheiten, Betriebssystemen sowie vielen Schnittstellen (Netzwerk, USB, Fax, WiFi – Schutzmaßnahmen s. Kapitel 10), auf denen zudem Anwendungssoftware läuft. Ebenso gibt es Internet- bzw. Cloudanbindung.

## Überprüfung beim Systemstart

Das Drucksystem sollte dazu in der Lage sein, die Integrität der verwendeten Softwarekomponenten (z. B. Firmware) in einem abgesicherten Modus selbst zu überprüfen. Im Falle einer Korrumpierung, darf sich das System nicht mit dem Netzwerk verbinden, um eine weitere Infektion zu vermeiden.

## Schutz im laufenden Betrieb

Um Drucksysteme im laufenden Betrieb zu schützen, gibt es zwei Möglichkeiten – entweder durch einen Virenscanner, der eine höhere Flexibilität bietet, aber nur bei bekannten Bedrohungen reagieren kann oder ein White-Listing, das exakt definiert was ausgeführt werden darf und alles andere ausschließt. Dieses Vorgehen ist wesentlich restriktiver, bietet aber auch Schutz für APTs.

# 8 Unberechtigte Nutzung von Drucksystemen

## Passwörter und Timeouts

Nur aktuelle Passwortrichtlinien und -regeln sollten vorgegeben und triviale Passwörter generell nicht zugelassen werden. Ferner erhöhen kurze Timeouts mit einer automatischen Abmeldung die Sicherheit. Hier muss ein Kompromiss zwischen dem Sicherheitsbedarf und Komfort bei der Nutzung gefunden werden.

## Audiovisuelle Hinweise

Fehleingaben bei Authentifizierungsversuchen am Drucksystem sollten möglichst sicht- und hörbar signalisiert werden, damit die Umgebung auf mögliche Missbrauchsversuche hingewiesen wird. Bei vielen Geräten lässt sich konfigurieren, wie oft etwa ein Passwort falsch eingegeben werden darf, bevor eine Sperrung erfolgt. Unabhängig davon muss ein angemeldeter Benutzer nach einer angemessenen Zeitspanne nach Verlassen des Gerätes automatisch abgemeldet werden.

## Flexible Anwender-Authentifikation und -Anmeldung bei mobilen Endgeräten

Der Zugang zu Netzwerkdruckern kann entweder am Gerät bzw. Bedienpanel (lokale Authentifizierung) oder über das Netzwerk bzw. die Weboberfläche (Netzwerkauthentifizierung) erfolgen.

Beide Zugangsmöglichkeiten werden in der Regel von den Herstellern mit Tastenkombinationen sowie mit PIN und / oder Benutzernamen / Passwort versehen. Hier gilt es, die Standard-Pins / -Passwörter durch eigene zu ersetzen, da sich die Standard-Pins / -Passwörter meistens leicht im Internet finden lassen.

Die Netzumgebung sollte so konfiguriert sein, dass sie nur autorisierte IT-Systeme als Quelle von Druckaufträgen zulässt.

Die Nutzung am Gerät (Drucken, Scan, Faxen, Kopieren, Menübedienung) sollte auf berechtigte Personen beschränkt sein. Eine Authentifizierung kann beispielsweise über eine auf der Maschine befindliche Datenbank, einen Druckserver oder eine zusätzliche Software (z. B. Secure-/ Pull-Printing) erfolgen. Eine zentrale Verwaltung bietet den Vorteil, dass mit eigenen Active-Directory-Richtlinien, LDAP oder Kerberos gearbeitet werden kann. Wegen der zunehmenden Nutzung von Cloud-Services und dem Datenzugriff auch von unterwegs werden zudem die Druckanforderungen immer »mobiler«. Mitarbeitende drucken von unterwegs oder von externen Standorten über Geräte außerhalb ihrer Abteilung. Das Drucken soll dabei über jedes beliebige Gerät innerhalb eines Unternehmens bzw. an verschiedenen Unternehmensstandorten auf sichere Weise möglich sein. In allen Fällen muss gewährleistet werden, dass kein Schadcode von mobilen Endgeräten auf die Drucker gelangen kann. Ein Einfallstor stellt die von vielen Druckern angebotene direkte Funkverbindung (z. B. Bluetooth oder ad-hoc-WLAN, oft in Verbindung mit der Verbindungssuche über NFC) dar. Diese Verbindungen sollten nur so lange aktiviert werden, wie sie auch tatsächlich benötigt werden. Es sollte darauf geachtet werden, dass insbesondere Multifunktionssysteme nicht über ungeschützte Schnittstellen erreichbar sind.

Mitarbeitende können mit ihrem eigenen Mobilgerät (das Konzept des »bring your own device«, BYOD) im Firmennetz eingebucht sein. Dadurch ist der Zugriff auf die Drucker im Firmennetz möglich, da diese Mobilgeräte bereits autorisiert sind. Wichtig ist dabei, dass diesen Endgeräten die zum betreffenden Mitarbeitenden gehörenden Rechte und Unternehmensrichtlinien zugewiesen werden. Nur so lassen sich die Gefahren, die durch eine Nutzung der Drucker über das Unternehmensnetzwerk hinaus entstehen können, wirkungsvoll abwenden.

Gästen kann man über einen eigenen Zugang (z. B. Bluetooth, gesichertes WLAN, ggf. mit Verbindungssuche über NFC) ohne Verbindung zum Firmennetz das Drucken über

deren Mobilgeräte ermöglichen. Alternativ kann auch eine Print-Server-Lösung mit Gästedruckfunktion verwendet werden.

## Verarbeitung von digitalen Dokumenten

Neben der Papierausgabe beherrschen aktuelle Drucksysteme den Umgang mit digitalen Dokumenten, z. B. Scan-to-Fax, Scan-to-Email, Scan-to-Folder, Scan-to-Business-App, Scan-to-USB, Senden vom USB-Stick etc. Analog zu den Sicherheitsmaßnahmen bei Druckjobs sollte eine Verarbeitung erst nach einer Authentifizierung eines berechtigten Nutzers erfolgen. Wichtig ist, die Nutzerrechte so spezifisch wie möglich zu vergeben; d. h. beispielsweise Scan-to-Folder zu erlauben und Scan-to-Email zu untersagen.

In der Regel erlauben Drucksysteme das Versenden von Dokumenten, z. B. per Fax oder E-Mail. Grundsätzlich besteht die Möglichkeit der rollenbezogenen Beschränkung auf bestimmte Sendeziele. Dieses kann erforderlich werden, um den Anforderungen der DSGVO (Transparenz, Zweckbindung, Datenminimierung, Integrität, Vertraulichkeit) gerecht zu werden.

# 9 Das Drucksystem kann »gehackt« werden

## Druckermissbrauch zur Attacke auf »höhere« IT-Ziele

Drucksysteme können als Ausgangspunkt für Manipulationen im Unternehmensnetzwerk verwendet werden. Der Zugriff ist wie bei anderen IT-Systemen zu reglementieren (Passwörter, Zugriffsrechte). Jede vorhandene oder neu zu installierende Firmware sowie mögliche Zusatzapplikationen müssen auch gegen Manipulationen geschützt sein (z. B. durch Signierung).

## Druckermanipulation via verfügbare Funktionalitäten

Grundsätzlich zur Verfügung stehende Funktionalitäten sollten für den individuellen Bedarf geprüft und nicht benötigte Funktionalitäten deaktiviert werden, wie z. B. verschiedene Druckvarianten oder Scanliefermethoden. Das reduziert mögliche Angriffsvektoren, denn jede nicht aktivierte Funktion kann auch nicht für einen Angriff missbraucht werden.

Die Nutzungsmöglichkeiten sollten den betrieblichen und sicherheitstechnischen Erfordernissen auf Nutzerebene entsprechen und die Mitarbeitenden darin unterwiesen werden, das System sachgemäß zu nutzen. Betriebliche Sicherheitserfordernisse sollten den Vorrang haben.

Beispiel WLAN: Die unternehmensinterne Sicherheitsrichtlinie schreibt vor, dass eine WLAN-Nutzung nur innerhalb der eigenen Netzinfrastruktur erfolgen darf. Damit wird untersagt, dass eine direkte WLAN-Verbindung zu externen Geräten hergestellt werden darf. Das bedeutet, dass vom Gerät verfügbare WLAN-Direktverbindungen (Wifi-Direct) zu deaktivieren sind.

# 10 Allgemeine Sicherheitsmaßnahmen

## Internet

Das Drucksystem sollte nicht aus dem Internet erreichbar sein. Dazu sollte die Firewall des Unternehmens so konfiguriert sein, dass keine externen Verbindungen zum Drucker aufgebaut werden können.

## Jobprotokollierung

Bei vielen Geräten lassen sich die Verarbeitungsprotokolle der Druck-/ Scan-/ Kopier- oder Fax-Vorgänge pseudonymisieren oder ausblenden, bzw. Kriterien definieren, dass angemeldete Benutzer nur ihre eigenen Metadaten sehen. Denn beispielsweise können die Titel der gedruckten Dokumente bereits Hinweise auf deren Inhalte geben, was zu unerwünschten, oder gar rechtswidrigen Informationsflüssen führen kann.

## Deaktivierung von Anschlüssen und (physischen) Systemzugängen

Heutige Drucksysteme haben in der Regel folgende Anschlüsse bzw. Zugänge:

- Netzwerk inkl. WLAN, Bluetooth, NFC etc.
- Serielle oder parallele Schnittstelle
- Fax
- USB
- Speicherkarten

Alle Anschlüsse und Zugänge erlauben mannigfaltige Missbrauchsmöglichkeiten. Daher sollte in jedem Einzelfall genau geprüft werden, ob bzw. in welchem Umfang Zugänge für den Geschäftsbetrieb unbedingt notwendig sind. Bedarfsweise können Sonderregelungen bei notwendigen Firmware-Updates vorgenommen werden.

## Deaktivierung von Protokollen

Die o.g. Anschlüsse werden von einer Vielzahl von Protokollen genutzt, z. B. im Netzwerk

- HTTP (TCP Port 80)
- RAW (TCP Port 9100)

Diese Protokolle stellen »Eingangstüren« mit entsprechenden Missbrauchsmöglichkeiten dar. Daher sollten immer alle nicht genutzten Protokolle durchgehend deaktiviert sein.

## Automatische Kontroll- und Korrektursysteme

Um sicherzugehen, dass nicht genutzte physische Systemzugänge und Netzwerkprotokolle deaktiviert sind beziehungsweise bei kurzfristiger Nutzung wieder deaktiviert werden, sollten die IT bzw. die verantwortlichen Administratoren die Sicherheitseinstellungen der Multifunktionssysteme und Drucker regelmäßig kontrollieren und – falls notwendig – korrigieren (Sicherheitsrichtlinien-Management). Um das IT-Personal bei dieser Aufgabe zu entlasten, haben sich automatische Kontroll- und Korrektursysteme bewährt, welche die sicherheitsrelevanten Einstellungen der Drucksysteme regelmäßig, also z. B. tagesaktuell, überprüfen und im Fall von Abweichungen den Administrator informieren und/oder auch gleich die abweichenden

Einstellungen automatisch korrigieren. Der Einsatz solcher Systeme ist für den erhöhten Schutzbedarf vom BSI empfohlen (siehe SYS 4.1 A21). Allgemein lässt sich hier jedoch festhalten, dass alle Kunden von solchen Sicherheitslösungen profitieren.

## Authentifizierung von Dokumenten durch digitale Signaturen

Einige Drucksysteme ermöglichen besonders wichtige Dokumente beim Scannen digital zu signieren. Dies gewährleistet einen kryptografisch abgesicherten Nachweis, wer das Dokument eingescannt hat und dass das Dokument nicht nachträglich verändert wurde. Dies kann durch Anwender-Signaturen erreicht werden, die auf Smartcards, im Active Directory oder direkt auf dem Drucksystem gespeichert sind. Der Einsatz dieser Technologie erfordert meistens eine zusätzlich zu implementierende Authentifizierungslösung auf dem Drucksystem und eine Public Key Infrastructure (PKI, ein System zur Ausstellung, Verteilung und Prüfung von Zertifikaten).

Mit dem gleichen technischen Verfahren bieten einige Drucksysteme auch die Möglichkeit, eine Signatur durch das Gerät anbringen zu lassen. Dies ermöglicht es, festzustellen, auf welchem Gerät der Scan durchgeführt wurde und damit auch, ob das gescannte Dokument nachträglich verändert wurde.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.


Herausgeber
Bitkom e. V.
Albrechtstr. 10 | 10117 Berlin



Ansprechpartnerin
Janine Welsch | Bereichsleiterin Telekommunikationspolitik
T 030 27576-234 | j.welsch@bitkom.org



Verantwortliches Bitkom-Gremium
AK Printing Solution Services



Autorinnen und Autoren
Robert Duisberg | Insentis GmbH
Bernd Hausmann | ThinPrint GmbH
Christoph Losemann | Canon Deutschland GmbH
Stefan Rautenbach | Ricoh Deutschland GmbH
Derya Sayili-Ziber | Konica Minolta Business Solutions Deutschland GmbH
Philipp Wanner | TA Triumph-Adler GmbH