Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte

1. Einleitung

Zur Grundausstattung in Büros gehören typischerweise Kopierer, Drucker und Multifunktionsgeräte. Sehr häufig ist es aber nicht effizient, jeden einzelnen Arbeitsplatz mit einem Drucker auszustatten. Daher werden oft zentrale Drucker, Kopierer oder Multifunktionsgeräte eingesetzt, auf denen die Mitarbeiter ihre Dokumente ausdrucken oder vervielfältigen können.

Da es einige Nachteile hat, wenn Aufträge vom Arbeitsplatz-PC direkt an einen Netzdrucker verschickt werden, setzen die meisten Institutionen einen zentralen Druckserver ein, der die Aufträge annimmt und auf die verfügbaren Drucker verteilt.

Die Integration der papierverarbeitenden Geräte in ein Datennetz der Institution ist in vielen Fällen nicht nur auf Drucker beschränkt. Netzfähige Dokumentenscanner können beispielsweise für eine Vielzahl von Benutzern bereitgestellt werden, damit diese Papierdokumente digitalisieren können. In Verbindung mit einem Drucker kann ein Scanner beispielsweise wie ein Kopierer betrieben werden.

Als Multifunktionsgeräte werden in diesem Baustein Geräte bezeichnet, die mehrere verschiedene papierverarbeitende Funktionen bieten, etwa Drucken, Kopieren und Scannen oder auch Fax-Dienste. Aus Gründen der Lesbarkeit werden nicht alle Gerätetypen an jeder Stelle einzeln benannt. Da aber beispielsweise für digitale Kopierer ähnliche Sicherheitsempfehlungen wie für Netzdrucker zu beachten sind, gelten für sie die Anforderungen analog.

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte aufgeführt.

Alle Maßnahmen (gekennzeichnet mit M) sind aufsteigend nummeriert und korrespondieren mit den entsprechenden Anforderungen (gekennzeichnet mit A).

2.1 Maßnahmen zum Baustein SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte

SYS.4.1.M1 Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten (B)

Eine grundlegende Voraussetzung für den sicheren Einsatz von Druckern, Kopierern und Multifunktionsgeräten ist eine angemessene Planung im Vorfeld. Der Einsatz der Geräte kann in mehreren Schritten nach dem Prinzip des Top-Down-Entwurfs geplant werden. Ausgehend von einem Grobkonzept für das Gesamtsystem werden konkrete Planungen für Teilkomponenten in spezifischen Teilkonzepten festgelegt (siehe auch SYS.4.1.M4 *Erstellung einer Sicherheitsrichtlinie für Drucker, Kopierer und Multifunktionsgeräte*). Im Grobkonzept sollten beispielsweise folgende Schwerpunkte behandelt werden:

- Wo sollen Drucker, Kopierer und Multifunktionsgeräte aufgestellt werden?
- Wer darf Räume mit Druckern, Kopierern und Multifunktionsgeräten betreten sowie auf die Geräte zugreifen? (Siehe auch SYS.4.1.M2 *Geeignete Aufstellung und Zugriff auf Drucker, Kopierer und Multifunktionsgeräte*)
- Wer erhält welche Zugriffsberechtigungen auf welche Netzgeräte für welche Aufgaben?
- Wie müssen Drucker, Kopierer und Multifunktionsgeräte vor Angriffen geschützt werden? Folgende Maßnahmen sind möglich:
    - Physischen Manipulationen sollte entgegengewirkt werden. Werden beispielsweise Schlösser oder Siegel an Wartungszugängen, wie z. B. Zugangsklappen angebracht, dann können unautorisierte Veränderungen erschwert oder zumindest erkannt werden.)
    - Angriffe über Netze sollten erschwert werden. Hierzu gehören beispielsweise unberechtigte Zugriffe auf Schnittstellen zur Fernadministration über das LAN (siehe auch SYS.4.1.M7 *Beschränkung der administrativen Fernzugriffe auf Drucker, Kopierer und Multifunktionsgeräte* sowie SYS.4.1.M11 *Einschränkung der Anbindung von Druckern, Kopierern und Multifunktionsgeräten*).
    - Die elektronischen Informationen müssen geschützt werden, sowohl bei der Übertragung zu den Geräten als auch bei der weiteren Verarbeitung.(Beispielweise sollte überlegt werden, alle Dokumente, die auf den Festplatten der Geräte (eventuell nur temporär) abgespeichert werden, zu verschlüsseln (siehe auch SYS.4.1.M15 *Verschlüsselung von Informationen bei Druckern, Kopierern und Multifunktionsgeräten* und SYS.4.1.M20 *Erweiterter Schutz von Informationen bei Druckern, Kopierern und Multifunktionsgeräten*).
    - Alle Entscheidungen, die in der Planungsphase getroffen wurden, müssen so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können. Dabei ist darauf zu achten, dass sie passend strukturiert und verständlich sind.

Die getroffenen Entscheidungen sollten geeignet in einem Basiskonzept festgehalten werden, auf das bei späteren Planungen und Entscheidungen zurückgegriffen werden kann.

Kriterien für die Beschaffung und geeignete Auswahl von Druckern, Kopierern und Multifunktionsgeräten

Wenn neue Drucker, Kopierer oder Multifunktionsgeräte beschafft werden, dann sollten diese von vornherein so ausgewählt werden, dass im späteren Betrieb mit geringem personellem und organisatorischem Zusatzaufwand ein hohes Maß an Sicherheit erreicht werden kann.

Viele Drucker und Kopierer sind modular aufgebaut. Das Grundgerät kann um zusätzliche Funktionen erweitert werden. Hierzu gehören beispielsweise auch zusätzliche Sicherheitsmechanismen, wie die Unterstützung einer Authentisierung über PINs oder Chipkarten. Bevor Drucker, Kopierer und ähnliche Geräte beschafft werden, sind daher neben den allgemeinen Anforderungen auch die Sicherheitsanforderungen festzulegen. Die Anforderungen und die auf dieser Basis getroffenen Entscheidungen sind zu dokumentieren. Nachfolgend werden einige grundsätzliche Anforderungen bei der Beschaffung von Druckern aufgelistet:

- **Grundlegende funktionale Anforderungen**
    - Sollen netzfähige Geräte beschafft werden?
    - Ist die Leistungsfähigkeit des Geräts der Größe des Benutzerkreises angemessen?
    - Was für ein Druckertyp mit welchem Druckverfahren soll angeschafft werden?
    - Kann das Gerät nachträglich durch zusätzliche Funktionen erweitert werden? (Viele Geräte können beispielsweise durch entsprechendes Zubehör auf Netzfähigkeit, Duplexdruck, zusätzliche Papierschächte und eine Authentisierung nachgerüstet werden.)
    - Kann akzeptiert werden, dass auf den Ausdrucken Wasserzeichen hinterlassen werden, die eine Zuordnung eines Ausdrucks zu einem konkreten Drucker zulassen ("Yellow Dots")?
- **Allgemeine Sicherheit**
    - Unterstützt das System sichere Protokolle zur Administration? (Damit die Geräte von zentraler Stelle aus administriert werden können, müssen netzfähige Geräte sichere Protokolle zur Administration unterstützen, bei einer Browser-basierten Konfiguration beispielsweise TLS.)
    - Können Informationen verschlüsselt gespeichert werden? (Um nach einem (unberechtigten) Ausbau der Festplatte den Zugriff auf die Daten zu verhindern, legen einige Geräte die Informationen verschlüsselt auf der Festplatte ab.)
    - Ist eine Möglichkeit der Authentisierung direkt am Gerät vorgesehen, z. B. über Passwort- oder PIN-Eingaben oder Chipkarten, oder kann diese Funktion nachträglich eingebaut werden? (Bei vielen Geräten ist eine Authentisierung vorgesehen, bei einigen allerdings nur für die Administration, um Zugriffe auf die Konfiguration abzusichern. Es gibt jedoch auch Geräte, bei denen sich alle Benutzerzugriffe absichern lassen, sodass Informationen erst ausgedruckt werden, wenn sich der Benutzer am Gerät authentisiert hat. Das dient als Schutz davor, dass an einen Netzdrucker übertragene oder an einem Kopierer eingescannte Informationen von Unberechtigten ausgedruckt werden können. Eine solche Funktion kann auch für eine Kostenkontrolle verwendet werden.)
    - Sind Ösen oder andere Möglichkeiten vorhanden, um die Geräte physisch vor Diebstahl zu schützen?
    - Können Manipulationen an der Hardware durch Gehäuseschlösser oder ähnliche Vorkehrungen erschwert werden? (Häufig kommt es beispielsweise vor, dass Speichermodule aus Druckern, Kopierern oder Multifunktionsgeräten gestohlen werden.)
- **Sicheres Löschen des Speichers**
    - Kann nach jedem Kopiervorgang der Speicher durch die Benutzer gelöscht werden? (In vielen Geräten sind Speicher, meist in der Form von Festplatten, eingebaut. Wenn Daten dort unverschlüsselt gespeichert werden, können diese eventuell von Unbefugten ausgelesen werden. Außerdem besteht die Gefahr, dass Angreifer die im Gerät gespeicherten Seiten erneut ausdrucken lassen. Einige Geräte bieten daher Funktionen zum Löschen des Speichers. Wenn möglich, sollten sie so eingestellt werden können, dass automatisch nach jedem Kopiervorgang gelöscht wird.)
    - Ist es möglich, die gesamte Festplatte zu löschen? (Für eine spätere Entsorgung sollte die gesamte Festplatte durch Überschreiben gelöscht werden können. Dies sollte nur nach

Eingabe eines entsprechenden Löschbefehls durch einen Berechtigten möglich sein. Alternativ sollte der Speicher ausgebaut und separat gelöscht werden können.)

- Werden Informationen zum Löschen auf dem Display angezeigt? (Auf dem Display des Geräts sollte es möglichst angezeigt werden, wenn die zuletzt gespeicherten Daten oder die gesamte Festplatte durch Überschreiben gelöscht wird.)

- **Netztechnische Sicherheit**
  - Besitzt das Gerät netztechnische Schutzmechanismen, wie IP- und Portfilter?
  - Muss das Gerät WLAN- oder Bluetooth-fähig sein oder ist ein kabelgebundener Anschluss ausreichend? (Der Einsatz von Funktechniken ist mit höheren Sicherheitsrisiken verbunden als der Anschluss über Kabel. Bei funkbasierten Lösungen müssen deshalb meist zusätzliche Sicherheitsmaßnahmen ergriffen werden.)
  - Unterstützt das Gerät die Verschlüsselung der Druckerkommunikation? (Werden die auszudruckenden Informationen über ein Netz übertragen, sollte verhindert werden, dass sie mitgelesen oder verändert werden können. Darum sollten Netzprotokolle eingesetzt werden, die eine Verschlüsselung der Informationen unterstützen, ein Beispiel hierfür ist das Internet Printing Protokoll (IPP) in Verbindung mit dem Transport-Layer-Security-Protokoll (TLS).)
  - Kann das Gerät in eine vorhandene IEEE 802.1X-Umgebung integriert werden? (IEEE 802.1X ermöglicht die Authentisierung der Endgeräte am Netz. Dies schützt davor, dass IT-Systeme unerlaubt am LAN betrieben werden.)
- **Wartbarkeit**
  - Bietet der Hersteller regelmäßige Updates und schnell verfügbare Sicherheitspatches an? (Es ist besonders wichtig, dass der Hersteller zeitnah auf bekannt gewordene Sicherheitsmängel reagiert.)
  - Können für das Produkt Wartungsverträge abgeschlossen werden? (Oft ist der Zugriff auf Updates und Unterstützungsleistungen des Herstellers nur in Verbindung mit einem gültigen Wartungsvertrag möglich. Können im Rahmen der Wartungsverträge maximale Reaktionszeiten für die Problembehebung festgelegt werden? Ein Wartungsvertrag ist nur dann geeignet, wenn mit den garantierten Reaktions- und Wiederinbetriebnahme-Zeiten die festgelegten Anforderungen an die Verfügbarkeit der Geräte abgedeckt werden können.)
  - Bietet der Händler oder Hersteller einen technischen Kundendienst (Hotline) an, der in der Lage ist, sofort bei Problemen zu helfen? (Dieser Aspekt sollte Bestandteil eines Wartungsvertrags sein. Beim Abschluss des Vertrags ist darauf zu achten, dass die Hotline- bzw. Support-Mitarbeiter auch die Sprache der Personen sprechen, die in der Regel dort anrufen werden.)
- **Kosten**
  - Wie hoch sind die Anschaffungskosten der Geräte?
  - Wie hoch sind die voraussichtlichen laufenden Kosten, einschließlich Wartung, Betrieb und Support? (Diese Kosten sollten bereits in der Beschaffungsphase mit berücksichtigt werden. Der Inhalt der Wartungs- und Supportverträge sollte geprüft werden, beispielsweise im Hinblick auf Reaktionszeiten, Hotline und Qualifikation des Personals.)

SYS.4.1.M2 Geeignete Aufstellung und Zugriff auf Drucker, Kopierer und Multifunktionsgeräte (B)

Um zu verhindern, dass Drucker, Kopierer oder Multifunktionsgeräte manipuliert werden oder die Druckausgaben von Unbefugten kopiert oder mitgelesen werden können, müssen die Geräte so aufgestellt werden, dass nur berechtigte Mitarbeiter Zugang zu ihnen haben. Zumindest sollten die Geräte nicht in Bereichen aufgestellt werden, in denen sich häufig externe Personen aufhalten, insbesondere also nicht in der Nähe von beispielsweise Besprechungs-, Veranstaltungs- oder Schulungsräumen. Hiervon ausgenommen

sind lediglich solche Geräte, die speziell für diese Bereiche vorgesehen sind, beispielsweise in Schulungsräumen.

Häufig stehen in Druckerräumen auch Kopierer. Aus Sicherheitssicht ist zu hinterfragen, ob hierdurch die Gefahr steigt, dass herumliegende Ausdrucke kopiert werden können. Um solche Probleme zu vermeiden, ist es sinnvoll, Drucker, Kopierer und Multifunktionsgeräte so aufzustellen, dass sie vom eigenen Personal gut eingesehen werden können. Besser ist es jedoch, die Geräte in einem geschlossenen Raum aufzustellen, zu dem nur Berechtigte Zutritt haben. Das ist besonders bei höherem Schutzbedarf zu empfehlen.

Noch besser kann es bei großen Druckern sein, wenn die Ausdrucke durch eine vertrauenswürdige Person in Fächer verteilt werden, die nur dem jeweiligen Empfänger zugänglich sind. Druckerausgaben müssen dann mit dem Namen des Empfängers gekennzeichnet sein. Dies kann automatisch durch die Druckprogramme erfolgen. Bei hohem Schutzbedarf sollte geprüft werden, ob diese Lösung geeignet ist.

Benutzer stellen häufig erst am Drucker fest, dass sie das falsche Dokument ausgedruckt haben oder dass noch eine Kleinigkeit geändert werden muss. Solche Ausdrucke werden dann häufig direkt beim Drucker in einen offenen Papierkorb geworfen. Da damit auch vertrauliche Dokumente in falsche Hände geraten können, empfiehlt es sich, einen Vernichter direkt neben Netzdruckern aufzustellen. Ersatzweise müssen die Benutzer darauf hingewiesen werden, dass solche Dokumente nicht liegen gelassen werden dürfen und anderweitig zu vernichten sind.

Beim Outsourcing übernehmen Outsourcing-Dienstleister Geschäftsprozesse und Dienstleistungen ganz oder teilweise von auslagernden Institutionen, den Outsourcing-Kunden. Outsourcing kann auch die Administration und Wartung von Druckern, Kopierern und Multifunktionsgeräten betreffen, wobei hier oft die Dienstleitungen in den Räumlichkeiten des Kunden erbracht werden. Durch das Outsourcing dürfen keine unkontrollierbaren Risiken für den Kunden hinsichtlich der Informationssicherheit entstehen. Neben Regelungen, dass institutionsfremde Personen in den Räumen der Institution beaufsichtigt werden müssen, müssen auch schriftliche Vertraulichkeitsvereinbarungen zwischen den Kunden und den Dienstleistern getroffen werden.

SYS.4.1.M3 Entfallen (B)

Die zugehörige Anforderung ist entfallen.

SYS.4.1.M4 Erstellung einer Sicherheitsrichtlinie für den Einsatz von Druckern, Kopierern und Multifunktionsgeräten (S)

Die Verantwortlichen sollten eine Sicherheitsrichtlinie für Drucker, Kopierer und Multifunktionsgeräte entwickeln. Darin sollten generell geregelt werden,

- welche Anforderungen an die Informationssicherheit der Geräte zu stellen sind,
- welche Vorgaben schon bei der Beschaffung der Geräte zu erfüllen sind,
- wie auf den Geräten gespeicherte oder damit verarbeitete Informationen technisch geschützt werden,
- wie die Geräte und Druckserver vor unbefugten Änderungen und Angriffen geschützt werden,
- wer damit arbeiten darf,
- welche Funktionen genutzt werden,
- wo Geräte aufgestellt werden dürfen,
- wer Geräte administrieren darf,
- wie der vorgegebene Sicherheitsstandard eingehalten wird und
- wie Benutzer über die Sicherheitsvorgaben informiert, eingewiesen und dazu verpflichtet werden, diese einzuhalten.

Die folgenden Aspekte sollten hierbei bei der Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten berücksichtigt werden:

- **Allgemeine Aspekte:**

- **Kaufen oder Mieten:** In einigen Fällen kann es sinnvoll sein, die benötigten Geräte nicht zu kaufen, sondern zu mieten. Werden sie gemietet, sollte sichergestellt werden, dass eventuell im Speicher abgelegte Dokumente sicher gelöscht werden, damit diese nicht vom nächsten Kunden, der das Gerät mietet, wieder hergestellt werden können. Hierbei sollte vorab überprüft werden, ob die Geräte ohne Speicher zurückgegeben werden können oder ob die Speicherbereiche zuverlässig gelöscht werden können, ohne diese physisch zu zerstören.
- **Lokale oder netzfähige Drucker:** Es ist zu entscheiden, wo lokale und wo netzfähige Drucker eingesetzt werden sollen. Häufig bietet auch eine Stufenlösung Vorteile: Benutzer, die oft vertrauliche Informationen ausdrucken müssen, erhalten für diese Ausdrucke einen lokalen Drucker. Für die Ausdrucke der restlichen Benutzer oder für Ausdrucke von Informationen mit einem geringeren Schutzbedarf sind bei der Zwischenlösung leistungsfähigere, zentrale Drucker verfügbar.
- **Druckserver:** Netzdrucker können direkt von den Clients oder über einen (oder mehrere) Druckserver angesteuert werden. Ein Druckserver nimmt die Druckaufträge von den IT-Systemen an und leitet sie an die gewünschten Drucker weiter. Neben einer zentralen Verwaltung und Protokollierung können die Drucker so effizienter gegen Angriffe geschützt werden, wenn nur noch die Druckserver auf die Netzdrucker zugreifen dürfen. Es ist eine geeignete Lösung auszuwählen.
- **Richtlinien für die Nutzung:** Um Drucker, Kopierer und Multifunktionsgeräte sicher und effektiv in Institutionen einsetzen zu können, müssen hierfür Sicherheitsvorgaben erstellt werden, die auf den vorhandenen Sicherheitszielen basieren sowie die Anforderungen aus den geplanten Einsatzszenarien einbeziehen. Diese spezifischen Sicherheitsvorgaben müssen mit dem übergreifenden Sicherheitskonzept der Institution abgestimmt sein.
  Darauf aufbauend ist die sichere Nutzung dieser Geräte zu regeln, und es müssen Sicherheitsrichtlinien dafür erarbeitet werden (siehe SYS.4.1.M5 *Erstellung von Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten*). Es ist darauf zu achten, dass Drucker, Multifunktionsgeräte und ähnliche Geräte in Sicherheitsaudits einbezogen werden und dass auch bei diesen Geräten regelmäßig kontrolliert wird, ob die Sicherheitsvorgaben umgesetzt sind.
- **Verteilung von Privilegien:** Es sollte entschieden werden, ob bestimmte Funktionen eines Druckers, Kopierers oder Multifunktionsgerätes auf ausgewählte Benutzer beschränkt werden sollen.
- **Nachfüllen von Verbrauchsgütern:** Bei Druckern, Kopierern und Multifunktionsgeräten müssen regelmäßig Verbrauchsgüter wie Tinte, Toner oder Papier nachgefüllt werden. Es sind Regelungen zu treffen, wer hierfür zuständig ist und welche Abläufe dabei eingehalten werden müssen.

- **Regelungen des Dokumentenzugriffs:** Es müssen Maßnahmen ergriffen werden, die den Zugriff auf fremde Dokumente erschweren:
  - **Sicherheitskritische Informationen:** Werden an Netzdruckern häufig sicherheitskritische Informationen ausgedruckt, sollte sichergestellt werden, dass nur befugte Personen auf die Ausdrucke zugreifen können. Hierfür können beispielsweise Netzdrucker und Kopierer eingesetzt werden, bei denen sich die Benutzer für einen Ausdruck direkt am Gerät authentisieren müssen (siehe SYS.4.1.M14 *Authentisierung und Autorisierung bei Druckern, Kopierern und Multifunktionsgeräten*). Alternativ könnte auch der Zutritt zum Drucker auf wenige vertrauenswürdige Personen beschränkt werden, die die Ausdrucke an die jeweiligen Empfänger verteilen.
  - **Weitere Restriktionen:** Es ist zu klären, ob und welche Restriktionen für Druckerzugriffe gelten sollen. Beispielsweise ist es normalerweise nicht sinnvoll, dass Mitarbeiter, die sich von außerhalb ins Netz einwählen, auf entfernte Drucker ausdrucken können, da sie ihre Ausdrucke nicht direkt abholen können. Auch für die Zeiten, in denen normalerweise nicht gedruckt wird, können entsprechende Restriktionen umgesetzt werden.

- **Schutz der Geräte:** Der Zugriff auf die Netzdrucker sollte beschränkt werden:
    - **Administration:** Damit unberechtigten Personen Druckereinstellungen nicht verändern können, sind entsprechende Schutzmaßnahmen für Netzdrucker umzusetzen. Diese umgesetzten Schutzmaßnahmen sollten regelmäßig überprüft werden.
    - **Physischer Schutz:** Es sollte überlegt werden, Maßnahmen gegen Manipulationen direkt am Gerät zu ergreifen. Hierzu gehören eine geeignete Aufstellung der Drucker sowie der Schutz der Schnittstellen.
    - **Netzspezifischer Schutz:** Bei netzfähigen Komponenten sind Mechanismen zum Schutz vor Angriffen aus dem Netz einzurichten. Wenn IEEE 802.1X oder ähnliche Verfahren zur netztechnischen Zugangskontrolle von den Netzdruckern und der Netzinfrastruktur unterstützt werden, sollten diese auch verwendet werden. Damit wird verhindert, dass IT-Systeme unberechtigt an das Netz angeschlossen werden. Weiterhin sollten Druckserver keine Verbindungen zu anderen IT-Systemen außer zu den voreingestellten Druckern aufbauen können.
- **Verfügbarkeit:** Es wird empfohlen, Vorkehrungen gegen einen Ausfall der Druckserver oder einzelner Geräte zu treffen. Durch entsprechende Wartungsverträge kann beispielsweise die Ausfallzeit reduziert werden, wenn technische Defekte auftreten (siehe SYS.4.1.M16 *Verringerung von Ausfallzeiten bei Druckern, Kopierern und Multifunktionsgeräten*).
- **Verschlüsselung:** Bei der Planung spielen folgende Punkte eine wichtige Rolle:
    - **Festplattenverschlüsselung:** Viele Drucker und digitale Kopiergeräte besitzen eingebaute Speichermedien, auf denen Informationen abgelegt werden. Falls das Gerät hierfür eine Verschlüsselung unterstützt, sollte diese benutzt werden.
    - **Verschlüsselung der Kommunikation:** Es sollte überlegt werden, die Kommunikation zwischen den Arbeitsplatz-PCs und den Druckservern sowie zwischen den Druckservern und den Druckern zu verschlüsseln.
- **Löschen des Gerätespeichers:** Als Zwischenspeicher für die temporäre Ablage der zu druckenden Informationen werden bei größeren Geräten häufig Festplatten verwendet. Je nach Konfiguration werden die Informationen im Zwischenspeicher nicht nur temporär, sondern permanent gespeichert. Es sollte gewährleistet werden, dass die Informationen nach dem Ausdruck aus dem Zwischenspeicher gelöscht werden. Hierfür besitzen viele Kopierer eine Löschfunktion. Wenn sich die Dokumente nicht automatisch löschen lassen, sollten alle Benutzer darauf hingewiesen werden, diese Funktion konsequent zu benutzen (siehe SYS.4.1.M5 *Erstellung von Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten*).

Alle Entscheidungen, die in der Planungsphase getroffen wurden, müssen so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können.

Erstellung einer Administrationsrichtlinie

In der Administrationsrichtlinie sollten alle umzusetzenden Sicherheitsmechanismen für Drucker, Kopierer und Multifunktionsgeräte beschrieben sein. Dieses Dokument richtet sich an das Fachpersonal der Institution.

SYS.4.1.M5 Erstellung von Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten (S)

Drucker, Kopierer und Multifunktionsgeräte lassen sich nicht allein mit technischen Maßnahmen absichern. Zusätzlich müssen entsprechende Sicherheitsrichtlinien für die Benutzer festgelegt werden. Die Sicherheitsrichtlinien für die Benutzer sollten in einem übersichtlichen Merkblatt zusammengefasst werden. Dieses Merkblatt sollte an allen Aufstellungsorten der Geräte aufgehängt werden.

Es sind folgende Aspekte zu berücksichtigen:

- **Zutritt zu den Kopier- und Druckerräumen:** Wenn möglich, sollte der Zutritt zu Räumen mit Druckern, Kopierern und Multifunktionsgeräten beschränkt werden (siehe auch SYS.4.1.M2 *Geeignete Aufstellung und Zugriff auf Drucker, Kopierer und Multifunktionsgeräte*). Es bietet sich an, den Zutritt beispielsweise auf die Mitarbeiter einer Abteilung oder auf die Benutzer einer Etage einzugrenzen. Die Benutzer sind über die Zutrittsbeschränkungen und die zugelassenen Personenkreise zu unterrichten.
- **Behandlung nicht abgeholter Dokumente:** Häufig werden ausgedruckte Dokumente nicht abgeholt, gedruckte Fax-Sendeberichte vergessen oder Fehldrucke nicht entsorgt. Alle Benutzer müssen darüber informiert sein, dass sie ihre Ausdrucke zeitnah abholen müssen. Dokumente, die keinem Benutzer zugeordnet werden können, sollten eingesammelt oder besser direkt mit einem Schredder vernichtet werden.
- **Umgang mit sensiblen Dokumenten:** Als "hoch vertraulich" klassifizierte Informationen sollten weder an allgemein zugänglichen Druckern ausgedruckt noch an allgemein zugänglichen Kopierern vervielfältigt werden. Amtlich geheim zu haltende Dokumente (Verschlusssachen) müssen gemäß der geltenden Vorschriften und Anweisungen geschützt werden.
- **Authentisierung am Gerät:** Soll eine Authentisierung direkt am Drucker, Kopierer oder Multifunktionsgerät erfolgen, müssen die Benutzer in dieses Verfahren eingewiesen werden (siehe SYS.4.1.M14 *Authentisierung und Autorisierung bei Druckern, Kopierern und Multifunktionsgeräten*).
- **Verteilung von Ausdrucken:** Werden an Netzdruckern oft sicherheitskritische Informationen ausgedruckt, sollte überlegt werden, die Ausdrucke an die jeweiligen Empfänger durch vertrauenswürdige Personen verteilen zu lassen. Dieser Ansatz ist eine Alternative zur Authentisierung am Gerät und hat den Vorteil, dass nur verteilende Personen Zutritt zu den jeweiligen Druckern benötigen. Allen weiteren Benutzern sollte dann in der Richtlinie der Zugang zum Drucker verwehrt werden.
- **Auswahl eines Standarddruckers:** Bei mehreren verfügbaren Druckern oder Multifunktionsgeräten können die Benutzer auf ihrem Client meist für alle Applikationen einen Standarddrucker vorauswählen. Als Standarddrucker sollte ein logisches (virtuelles) Gerät wie ein Druckvorschau-Programm oder ein PDF-Generator gewählt werden. Das schützt davor, dass Informationen unbemerkt ausgedruckt werden, beispielsweise weil unbeabsichtigt die Drucken-Schaltfläche in einer Applikation betätigt wurde.
- **Löschen des Kopierspeichers durch den Benutzer:** Ein Vorteil von digitalen Kopierern ist, dass ein einmal eingescanntes Dokument beliebig oft ausgedruckt werden kann. Damit Unbefugte nicht auf solche Informationen zugreifen können, sollte der hierfür verwendete temporäre Speicher nach der Benutzung gelöscht werden. Bei vielen Kopierern können die Benutzer das nur manuell veranlassen, daher müssen entsprechende Hinweise und Anweisungen an den Geräten angebracht werden. Jeder Benutzer sollte sich mit dem Merkblatt zum sicheren Umgang mit Druckern, Kopierern und Multifunktionsgeräten vertraut machen.
- **Versteckte Kennzeichnungen auf Ausdrucken:** Ergänzend können die Benutzer darüber informiert werden, dass viele Drucker auf den Ausdrucken Wasserzeichen hinterlassen, die eine Zuordnung eines Ausdrucks zu einem konkreten Drucker ermöglichen ("Yellow Dots").

SYS.4.1.M6 Entfallen (S)

Die zugehörige Anforderung ist entfallen.

SYS.4.1.M7 Beschränkung der administrativen Fernzugriffe auf Drucker, Kopierer und Multifunktionsgeräte (S)

Um Angriffe auf Drucker, Kopierer und Multifunktionsgeräte zu erschweren, sollte der Zugriff auf diese Geräte beschränkt werden. Im Folgenden werden einige Aspekte beschrieben, die für den sicheren Betrieb von Druckern und Kopierern berücksichtigt werden sollten:

- **Beschränkung auf notwendige Zugriffsrechte:** Wenn möglich, sollten nur so wenig Administratoren wie nötig vollständig auf die Drucker, Kopierer und Multifunktionsgeräte zugreifen können. Dabei

sollten immer nur die Zugriffsrechte vergeben werden, die für die Aufgabenwahrnehmung notwendig sind. Die vergebenen Zugriffsrechte sollten regelmäßig überprüft werden.

- **Absicherung der Administration bei Fernzugriff:** Falls Drucker, Kopierer oder Multifunktionsgeräte über ein Netz administriert werden, sollte sichergestellt sein, dass sich die Administratoren hierfür authentisieren müssen. Wenn systemseitig keine Authentisierung unterstützt wird, müssen geeignete Ersatzmaßnahmen ergriffen werden. Alle Administrationszugriffe sollten möglichst nur über einen verschlüsselten Kanal stattfinden, damit keine Passwörter oder andere schutzbedürftige Informationen mitgehört werden können. Beispielsweise kann bei einigen Gerätetypen die Übertragung der Konfigurationsdaten über HTTPS oder SNMPv3 verschlüsselt werden. In diesem Fall sollte die unverschlüsselte Kommunikation unterbunden werden, indem beispielsweise die HTTP-Schnittstelle für die Konfiguration deaktiviert wird.
- **Schutz der Anzeige des Bedienfelds:** In der Regel verfügen Drucker, Kopierer und Multifunktionsgeräte über Anzeigefelder, auf denen zahlreiche Informationen angezeigt werden. Hierzu können auch Informationen gehören, die Rückschlüsse auf die ausgedruckten Dokumente schließen lassen, wie beispielsweise Datei- und Benutzernamen (z. B. "Bewerbung_bei_Recplast.doc" von Benutzer XYZ). Bei einigen Geräten werden diese Anzeigen nicht nur lokal am Gerät dargestellt, sondern können über ein Datennetz übermittelt werden. Damit die dargestellten Informationen nicht missbraucht werden können, sollte festgelegt werden, ob die Anzeige des Bedienfelds über ein Datennetz überhaupt eingesehen werden soll. Wenn dies dennoch gewünscht wird, sollte die Anzeige des Bedienfelds nur an die Mitarbeiter des IT-Betriebs übertragen werden können. Den betroffenen Benutzern sollte im Vorfeld mitgeteilt werden, dass die Anzeige des Bedienfelds von weiteren Personen eingesehen werden kann.
- **Einsatz von Paketfiltern:** In einigen Druckern sind Paketfilter integriert, über die Verbindungen anhand von IP-Adressen oder Port-Nummern gefiltert werden können. Alle Port-Nummern, die nicht für den Druckbetrieb und zur Konfiguration des Druckers benötigt werden, sind möglichst zu blockieren. Unterstützt das Gerät eine verschlüsselte Kommunikation, sollte die unverschlüsselte Kommunikation mit dem Gerät so weit wie möglich unterbunden werden, beispielsweise über die entsprechenden Port-Nummern.
  Werden Druckserver eingesetzt, ist darauf zu achten, dass nur von diesen Servern eine Verbindung zu den Druckern aufgebaut werden darf. So wird der Verbindungsaufbau von unautorisierten IT-Systemen zu den Druckern erschwert. Eine Ausnahme bilden allerdings Systeme, von denen aus Drucker konfiguriert werden sollen. Diese Systeme müssen natürlich ebenfalls auf den Drucker zugreifen können. Die Paketfilter sind generell so restriktiv wie möglich zu konfigurieren. Das gilt auch für den Verbindungsaufbau von den Netzdruckern zu anderen IT-Systemen. Beispielsweise sollten die Paketfilter so konfiguriert werden, dass Netzdrucker keine Verbindungen zu einem IT-System außerhalb des LANs aufbauen können. Das erschwert den ungewollten Datenaustausch mit externen IT-Systemen, beispielsweise mit solchen im Internet. Unabhängig von lokalen Paketfiltern sollte am zentralen Sicherheitsgateway die Kommunikation zwischen den Druckern und externen Netzen blockiert werden.
- **Netzsegmentierung:** Oft ist es empfehlenswert, alle Drucker, Kopierer und Multifunktionsgeräte in einem logischen Netz zusammenzufassen. Das erleichtert es in vielen Fällen, sie zu konfigurieren und zu administrieren. Wird das konsequent umgesetzt, kann auf den zuständigen Routern und Gateways die Kommunikation zwischen den Druckern und anderen Netzsegmenten gezielt kontrolliert werden (sowohl Empfang als auch Versand von IP-Paketen).

SYS.4.1.M8 Entfallen (S)

Die zugehörige Anforderung ist entfallen.

SYS.4.1.M9 Entfallen (S)

Die zugehörige Anforderung ist entfallen.

SYS.4.1.M10 Entfallen (S)

Die zugehörige Anforderung ist entfallen.

SYS.4.1.M11 Einschränkung der Anbindung von Druckern, Kopierern und Multifunktionsgeräten (S)

Häufig ist es unter wirtschaftlichen oder praktischen Gesichtspunkten nicht zweckmäßig, separate Geräte zum Drucken, Scannen, Kopieren und Fax-Versand bzw. -Empfang einzusetzen. Als Alternative sind Multifunktionsgeräte, die auch als All-in-One-Geräte bezeichnet werden, erhältlich, die mehrere oder sogar alle diese Funktionen in einem Gerät unterstützen. Teilweise bieten diese Geräte auch zusätzliche Kommunikationsschnittstellen, beispielsweise für Webzugriffe.

Multifunktionsgeräte haben meist gegenüber Einzelgeräten einen geringeren Administrationsaufwand und benötigen weniger Anschlussleitungen (Energie- und eventuell auch Datenleitungen). Multifunktionsgeräte können in der Regel direkt oder über ein LAN an Arbeitsplatz-PCs angeschlossen werden.

Einige Geräte bieten eine Fax- und Modem-Funktionalität, die den Anschluss an ein Telefonnetz voraussetzt, sodass über die Kopplung mit anderen IT-Systemen eine physische Verbindung zwischen dem LAN und dem Telefonnetz entstehen kann. Falls diese Verbindung nicht von einem Sicherheitsgateway kontrolliert wird, sind hierüber unter Umständen unkontrollierte Internet-Zugriffe möglich, sodass beispielsweise Angreifer von außen auf das LAN zugreifen könnten. Der unberechtigte Aufbau von Datenverbindungen sowie ungewollten Fernwartungen sollten in jedem Fall unterbunden werden.

Eine Ausnahme sind Multifunktionsgeräte mit Fax-Funktionalität, die nicht an ein Telefonnetz angeschlossen werden müssen. Diese Geräte scannen Dokumente ein und senden sie über eine Datenverbindung an einen zentralen Faxserver, der sich typischerweise ebenfalls im LAN befindet. Erst der Faxserver, der an das Telefonnetz angeschlossen ist, versendet das Fax an den eigentlichen Empfänger. Wird ein Faxserver verwendet, sind die im Baustein NET.4.3 *Faxgeräte und Faxserver* empfohlenen Maßnahmen umzusetzen.

Wenn Multifunktionsgeräte an ein Telefonnetz angeschlossen werden können, sollte zunächst entschieden werden, ob dieser Anschluss tatsächlich erforderlich ist, das heißt, ob die entsprechende Fax- oder Modem-Funktionalität benötigt wird. Falls auf den Anschluss an das Telefonnetz verzichtet werden kann, sind möglichst folgende Schutzmaßnahmen zu ergreifen:

- Die Fax- bzw. Modem-Funktionalität ist auf dem Gerät zu deaktivieren.
- Das Kabel für den Anschluss an das Telefonnetz ist zu entfernen. Keinesfalls darf das Kabel in die Telefondose eingesteckt werden.
- Wenn sich das Gerät an einem frei zugänglichen Ort befindet, sollten möglichst die Telefondosen in dem jeweiligen Raum deaktiviert oder die Schnittstelle zum Telefonnetz aus dem Gerät ausgebaut werden. Ist beides nicht möglich, sollte regelmäßig kontrolliert werden, ob nicht unbefugt die Verbindung zum Telefonnetz hergestellt worden ist.

Wenn die Fax- oder Modem-Funktionalität des Multifunktionsgerätes genutzt werden soll, sollte sichergestellt sein, dass der hierfür erforderliche Anschluss an das Telefonnetz nicht zu unkontrollierten Datenverbindungen zwischen dem LAN und Fremdnetzen führen kann. Folgende Ansätze sind möglich:

- Das Multifunktionsgerät wird an einen Stand-Alone-PC angeschlossen, das heißt an ein IT-System, das nicht mit dem LAN verbunden ist. Nachteilig bei diesem Ansatz ist, dass Daten in vielen Fällen mithilfe von Datenträgern zwischen dem Stand-Alone-PC und dem LAN transportiert werden müssen (siehe auch SYS.4.5 *Wechseldatenträger*).
- Eine Alternative ist, das Multifunktionsgerät selbst oder das IT-System, an das ein Multifunktionsgerät angeschlossen ist, mithilfe eines zusätzlichen Sicherheitsgateways vom LAN zu trennen.
- Eine weitere Alternative ist, das Multifunktionsgerät selbst oder das IT-System, an das ein Multifunktionsgerät angeschlossen ist, in einer demilitarisierten Zone (DMZ) eines bestehenden Sicherheitsgateways zu platzieren.

Generell sollten netzfähige Drucker, Kopierer und Multifunktionsgeräte in anderen Netzen betrieben werden als diejenigen Server, Clients und weiteren IT-Systeme, die andere Aufgaben haben (z.B. auch VoIP-Telefone, IoT-Geräte). Hierzu gibt es verschiedene Möglichkeiten:

- **Trennung der Netze über VLANs:**
  Lokale Netze können logisch durch eine entsprechende VLAN-Konfiguration, also über virtuelle lokale Netze (Virtual Local Area Networks), segmentiert werden. VLANs alleine bieten jedoch keinen Schutz vor Angreifern, die sich mit ihrem IT-System physikalisch an ein VLAN anschließen. Da die Netzdose, also der VLAN-Port, des Druckers, Kopierers oder Multifunktionsgeräts jedem unmittelbar zugänglich ist, könnte ein Angreifer direkt die Drucker, Kopierer und Multifunktionsgeräte im VLAN angreifen, indem er z. B. anstatt eines Druckers sein IT-System mit dem VLAN verbindet.
  Aus diesem Grunde sollten weitere, über die logische Netztrennung hinausgehende Maßnahmen getroffen werden, um derartigen Angriffe zu begegnen.
- **Physikalische Trennung der Netze:**
  Bei erhöhten Sicherheitsanforderungen kann eine komplette physikalische Trennung des Druckernetzes vom Datennetz sinnvoll sein. Dies verringert deutlich die Angriffsmöglichkeiten. Außerdem kann bei dem Ausfall eines Netzes, beispielsweise durch den Ausfall der aktiven Netzkomponenten oder durch einen Kabelbruch, weiterhin über das verbleibende Netz kommuniziert werden.

Alle genannten Lösungsansätze müssen systematisch im Sicherheitskonzept berücksichtigt werden und erfordern zusätzliche Sicherheitsmaßnahmen, beispielsweise zum Schutz vor Schadprogrammen.

SYS.4.1.M12 Entfallen (B)

Die zugehörige Anforderung ist entfallen.

SYS.4.1.M13 Entfallen (B)

Die zugehörige Anforderung ist entfallen.

SYS.4.1.M14 Authentisierung und Autorisierung bei Druckern und Multifunktionsgeräten (H)

Im normalen Büroalltag ist es oft einfach, Ausdrucke vertraulicher Dokumente direkt am Drucker einzusehen, solange diese noch nicht abgeholt wurden. Daher müssen Maßnahmen ergriffen werden, die den Zugriff auf fremde Dokumente erschweren.

Generell sollten nur berechtigte Personen auf die ausgedruckten oder kopierten Dokumente zugreifen können. Der Kreis der berechtigten Personen ist so klein wie möglich zu halten. Kann der Zugang zu einem Netzdrucker nicht beschränkt werden, sollte überlegt werden, Geräte einzusetzen, die eine Authentisierungsfunktion für Benutzer bieten. Dies gilt insbesondere dann, wenn an Netzdruckern oder Kopierern häufig hochvertrauliche Dokumente gedruckt beziehungsweise vervielfältigt werden müssen.

Ist diese Funktion aktiviert, wird das Dokument erst ausgedruckt, nachdem sich der Benutzer, der den entsprechenden Druckauftrag abgesendet hat, am Gerät identifiziert und authentisiert hat. In der Praxis werden zur Authentisierung häufig Chipkarten oder PINs verwendet. Dabei können PINs je nach Gerätetyp benutzer- oder dokumentenspezifisch festgelegt werden. Bei letzterer Variante wird eine PIN festgelegt, wenn der Druckauftrag abgesendet wird. Erst nachdem diese PIN am Gerät eingegeben wurde, wird das Dokument, das der PIN zugeordnet ist, ausgedruckt. Druckaufträge, die zwar abgesendet, aber nicht abgeholt wurden, müssen regelmäßig gelöscht werden. Die Drucker sollten möglichst so konfiguriert werden, dass bei mehrmaliger Eingabe einer falschen PIN der Druckauftrag automatisch gelöscht wird.

Ein weiterer Sicherheitsgewinn kann erzielt werden, wenn das zu druckende Dokument vom Arbeitsplatz-PC verschlüsselt zum Drucker übertragen und verschlüsselt zwischengespeichert wird. Erst nach einer erfolgreichen Authentisierung direkt am Drucker wird das Dokument entschlüsselt und ausgedruckt.

Es gibt auch Kopierer, die eine ähnliche Authentisierungsfunktion bieten, meist als optionale Erweiterung. Erst nachdem eine Chipkarte eingelesen oder eine PIN eingegeben wurde, können die Benutzer kopieren. Obwohl diese Authentisierungsfunktionen hauptsächlich für Kostenabrechnungen angeboten werden, können Angreifer durch diese Erweiterungen schwerer unberechtigt Kopien erstellen.

SYS.4.1.M15 Verschlüsselung von Informationen bei Druckern, Kopierern und Multifunktionsgeräten (S)

Damit ein Ausdruck erstellt werden kann, müssen die erforderlichen Informationen vom Arbeitsplatz-PC zum Drucker übertragen werden. Bei Kopierern findet das meist intern zwischen Scannereinheit und

Speicher statt. Ein Angreifer könnte versuchen, auf den Speicher zuzugreifen oder die Informationen bei der Übertragung zum Drucker abzuhören.

Daher wird empfohlen, die Informationen in den internen Speichern verschlüsselt zu speichern. Zahlreiche Drucker, Kopierer und Multifunktionsgeräte bieten diese Funktion an. Wenn das eingesetzte Gerät eine verschlüsselte Speicherung unterstützt, sollte diese Funktion aktiviert werden.

Die Kommunikation zwischen Arbeitsplatz-PCs, Druckservern und Netzdruckern erfolgt meist über ein Datennetz, für das die gleichen Gefährdungen wie bei anderen Datenverbindungen zu beachten sind. Damit diese Kommunikation nicht abgehört werden kann, sollten daher die Druckaufträge möglichst verschlüsselt übertragen werden.

Einige Druckprotokolle, wie das besonders bei Unix-Systemen weit verbreitete LPR/LPD-Protokoll (Line Printer Remote / Line Printer Daemon), unterstützen keine Verschlüsselung. Ähnlich ist die Situation bei SMB/CIFS (Server Message Block / Common Internet File System) unter Windows.

Daher sollte ein Protokoll wie IPP (Internet Printing Protocol) gewählt werden, das eine Verschlüsselung unterstützt, beispielsweise TLS (Transport Layer Security) in Verbindung mit IPP.

Unter Unix-Systemen sollte beispielsweise das Common Unix Printing System (CUPS) eingesetzt werden, das bei neueren Versionen in der Voreinstellung zur Kommunikation zwischen Client und Druckserver das Protokoll IPP verwendet. Durch eine entsprechende Konfiguration kann dabei TLS aktiviert werden.

SYS.4.1.M16 Verringerung von Ausfallzeiten bei Druckern, Kopierern und Multifunktionsgeräten (H)

Fallen Drucker, Kopierer und Multifunktionsgeräte länger aus, ist das für die meisten Institutionen nicht tolerierbar. Besonders durch einen Ausfall zentraler Komponenten, die für die gesamte Drucker-Infrastruktur erforderlich sind, werden Geschäftsprozesse oder Fachaufgaben erheblich beeinträchtigt. Je nach Verfügbarkeitsanforderungen sind daher geeignete Maßnahmen zu ergreifen, um die Ausfallzeit beziehungsweise deren Auswirkungen zu verringern.

Es ist darauf zu achten, dass immer genügend Verbrauchsmaterial verfügbar ist, z. B. Toner und Papier. Ab einer bestimmten Restmenge, die vom Verbrauch abhängig ist, sollte neues Verbrauchsmaterial beschafft und bereitgestellt werden.

An jedem Kopierer, Drucker und Multifunktionsgerät sowie auch an anderen Komponenten des Drucksystems, müssen diverse Konfigurationseinstellungen vorgenommen werden. Um diese Einstellungen nach einem Ausfall oder Austausch schnell wieder korrekt einrichten zu können, müssen die Konfigurationen systematisch dokumentiert werden.

Je weniger Geräte verfügbar sind, desto gravierender ist es, wenn ein einzelnes ausfällt. Der Ausfall eines Druckservers ist besonders problematisch, da diese Geräte oft nur einmal oder wenige Male vorhanden sind.

Um auf Notfälle reagieren zu können, sollte zwischen zentralen Komponenten einerseits und Druckern, Kopierern und Multifunktionsgeräten andererseits unterschieden werden. Bei einem höheren Schutzbedarf bezüglich der Verfügbarkeit sollte überlegt werden, zentrale Komponenten, wie Druckserver, redundant auszulegen. Wenn der einzige zentrale Server ausfällt, könnte sonst eventuell im gesamten LAN nicht mehr gedruckt werden.

Dezentrale Komponenten, wie Drucker, sind häufig auf mehreren Etagen oder in verschiedenen Büros eines Gebäudes zu finden. Generell sollte die Druckerlandschaft so gestaltet werden, dass die Benutzer beim Ausfall eines Druckers problemlos einen anderen Drucker verwenden können.

- Es sollte überlegt werden, für lokale Drucker, die einen höheren Schutzbedarf bezüglich der Verfügbarkeit haben und direkt an einen Arbeitsplatz angeschlossen werden, Ersatzgeräte bereitzustellen (*Cold Standby*). Bei einem Ausfall könnte der defekte Drucker zeitnah gegen das Ersatzgerät ausgetauscht werden.
- Für große Kopierer, Drucker und Multifunktionsgeräte die von mehreren Personen benutzt werden, sollten Wartungsverträge mit einer dem Schutzbedarf angemessenen Reaktionszeit abgeschlossen werden.

- Es sollte eine Liste von Fachhändlern geführt werden, bei denen unproblematisch neue Geräte beschafft werden können.
- Bei Bedarf können Ersatzteile gelagert werden, die häufig benötigt werden. Das ist allerdings nur sinnvoll, wenn entsprechendes Fachwissen vorhanden ist, um die Ersatzteile selbstständig austauschen zu können.

SYS.4.1.M17 Schutz von Nutz- und Metadaten (S)

Es sollte gewährleistet werden, dass die Informationen nach dem Ausdruck aus dem Zwischenspeicher gelöscht werden (siehe SYS.4.1.M5 *Erstellung von Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten* und SYS.4.1.M1 *Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten*). Falls häufig Informationen mit einem höheren Schutzbedarf ausgedruckt oder kopiert werden, ist zu beachten, dass einfaches Löschen nicht ausreicht, um zu verhindern, dass gelöschte Daten wiederhergestellt werden können (siehe CON.6 *Löschen und Vernichten*). Einige Geräte besitzen hierfür Mechanismen zum „sicheren Löschen“. Hierbei handelt es sich um eine Löschfunktion, welche die Daten zusätzlich überschreibt. Falls eine solche Funktion vorhanden ist, sollte sie aktiviert werden. Andernfalls müssen adäquate Alternativlösungen gefunden werden.

Wenn möglich, sollten auch Maßnahmen ergriffen werden, die es einem Angreifer erschweren, auf den Speicher physisch zuzugreifen bzw. die Festplatten auszubauen. Um erkennen zu können, ob versucht wurde, den internen Speicher auszubauen oder zu manipulieren, sollten die Geräte versiegelt werden. Generell sollten Drucker, Kopierer und Multifunktionsgeräte so aufgestellt werden, dass sich niemand unbeobachtet an ihnen zu schaffen machen kann.

Generell sollten Nutz- und Metadaten wie Druckaufträge und Scandateien nur so kurz wie möglich auf den Geräten gespeichert werden. Die Daten sollten nach einer vordefinierten Zeit automatisch gelöscht werden. Dateiserver in den Geräten und Funktionen, wie Scan in den Gerätespeicher, sollten vom IT-Betrieb abgeschaltet werden. Die dafür benötigten Protokolle und Funktionen sollten, soweit möglich, gesperrt werden.

Generell sollte vom IT-Betrieb sichergestellt werden, dass alle Metadaten, z. B. von Druckaufträgen, nicht für Unberechtigte sichtbar sind. Einige Geräte hinterlassen z.B. auf den Ausdrucken Wasserzeichen, mit denen ein Ausdruck einem konkreten Drucker zugeordnet werden kann ("Yellow Dots"). Diese Funktion ist oft von dem Hersteller nicht dokumentiert und kann nicht abgeschaltet werden. Daher sollte von der Institution geregelt werden, wie mit Metadaten versehene Ausdrucke an Dritte weitergegeben werden.

SYS.4.1.M18 Konfiguration von Druckern, Kopierern und Multifunktionsgeräten (S)

Alle Drucker und Multifunktionsgeräte sollten geeignet vom IT-Betrieb konfiguriert werden. Sie bieten oft mehr Funktionen, als im normalen Betrieb benötigt werden. Dadurch können sich unnötige Risiken ergeben. Daher sollten alle nicht benötigten Funktionen deaktiviert bzw. deren Nutzung so weit wie möglich eingeschränkt werden.

Die Geräte sollten ausschließlich über verschlüsselte Protokolle wie HTTPS und SNMPv3 verwaltet werden. Sämtliche Protokolle, mit denen unverschlüsselt auf Drucker und Multifunktionsgeräte zugegriffen werden kann, sollte vom IT-Betrieb durch verschlüsselte ersetzt oder abgeschaltet werden. Insbesondere sollten unverschlüsselte und daher unsichere Protokolle ersetzt werden, mit denen sich die Gerätekonfiguration verändern lässt, z. B. SNMP, Telnet und PJL (Printer Job Language). Falls SNMPv3 verwendet wird, dann sollte der voreingestellte SNMP Set Community Name geändert werden.

SYS.4.1.M19 Entfallen (S)

Die zugehörige Anforderung ist entfallen.

SYS.4.1.M20 Erweiterter Schutz von Informationen bei Druckern und Multifunktionsgeräten (H)

Druckdateien mit vertraulichen Informationen sollten nur verschlüsselt übertragen werden. Auch sollten auf dem Druckserver die Namen der Druckaufträge nur anonymisiert angezeigt werden.

Alle Schnittstellen für externe Speichermedien sollten gesperrt werden.

Weiterhin sollten geräteinterne Adressbücher deaktiviert und den Benutzern alternative Adressierungsverfahren (z. B. Adresssuche per LDAP) angeboten werden.

Bei Druckern und Multifunktionsgeräten mit E-Mail-Funktion sollte sichergestellt sein, dass E-Mails ausschließlich mit der E-Mail-Adresse eines authentisierten Benutzers versendet werden können. Auch sollten Dokumente nur an interne E-Mail-Adressen verschickt werden können.

Eingehende Fax-Dokumente sowie Sendeberichte sollten nur autorisierten Benutzern zugänglich sein.

SYS.4.1.M21 Erweiterte Absicherung von Druckern und Multifunktionsgeräten (H)

Die Sicherheitseinstellungen von Druckern, Kopierern und Multifunktionsgeräten sind regelmäßig zu kontrollieren und, falls notwendig, zu korrigieren. Wenn ein automatisiertes Kontroll- und Korrektursystem verfügbar ist, sollte es genutzt werden.

Zudem sollte eingeschränkt werden, dass die Geräte über das Bootmenü auf die Werkseinstellungen zurückgestellt werden können. Es sollte sichergestellt sein, dass keine Firmware oder Zusatzsoftware in Druckern und Multifunktionsgeräten installiert werden kann, die nicht vom jeweiligen Hersteller verifiziert und freigegeben wurde.

SYS.4.1.M22 Ordnungsgemäße Entsorgung ausgedruckter Dokumente (B)

Nicht benötigte, aber ausgedruckte Dokumente mit Informationen, die für die Institution kritisch sein könnten, müssen in geeigneter Weise vernichtet werden, z. B. in geeigneten Papiercontainern. Sind Heimarbeitsplätze mit Druckern, Kopierern oder Multifunktionsgeräten ausgestattet, sollte gewährleistet werden, dass die ausgedruckten Informationen auch direkt vor Ort geeignet vernichtet werden können.

In der Institution müssen die dafür benötigten Entsorgungseinrichtungen vorhanden sein, z. B. Aktenvernichter. Wird schutzbedürftiges Material erst gesammelt und dann entsorgt, so ist die Sammlung unter Verschluss zu halten und vor unberechtigtem Zugriff zu schützen.

3. Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind.

Verwaltung von Druckern

Im Folgenden werden typische Drucksysteme sowie deren Bestandteile und Kommunikationsbeziehungen vorgestellt. Drucksysteme bestehen in der Regel aus Client- und Server-seitigen Software-Komponenten.

Drucksysteme

In den seltensten Fällen sendet eine Anwendung den Druckauftrag direkt an einen Drucker, sondern zwischen der Anwendung und dem Drucker wird ein Drucksystem betrieben. Hierbei ist es oft erforderlich, dass diese Drucksysteme netzfähig sind und mehrere Clients auf einen Drucker zugreifen können. Auch bei einer ausschließlich lokalen Installation wird ein Drucksystem benötigt. Hierbei sendet der Client intern den Druckauftrag an den Druckserver.

Ein Drucksystem kann unter anderem folgende Aufgaben erfüllen:

- Annahme des Druckauftrags von der Anwendung,
- Verwaltung der Druckaufträge in einer Warteliste (Spooling),
- Ergänzung um zusätzliche Informationen, wie Trennseiten, Papierformat oder andere Eigenschaften,
- Umwandlung in ein dem Drucker verständliches Datenformat, wie PostScript oder PCL,
- Verwaltung von logischen und physischen Druckern,
- Benutzerverwaltung und

- Protokollierung.

Unterschiedliche Betriebssysteme favorisieren unterschiedliche Drucksysteme. Besonders bei heterogenen IT-Landschaften ist es entscheidend, dass die Drucksysteme miteinander kompatibel sind. Viele Systeme bieten Schnittstellen zu anderen Drucksystemen. Dadurch kann beispielsweise ein Unix-System auf einen Drucker zugreifen, der von einem Windows-System verwaltet wird.

Abhängig vom Betriebssystem sind folgende Drucksysteme weit verbreitet:

- Berkeley Printing System,
- Common Unix Printing System (CUPS) und
- Druckerfreigaben auf der Basis von SMB unter Windows.

Bei heterogenen Netzlandschaften ist möglichst ein Drucksystem auszuwählen, das von allen Betriebssystemen unterstützt wird. Als Alternative kann es zweckmäßig sein, mehrere verschiedene Drucksysteme einzusetzen, die unter Umständen untereinander kommunizieren können. Die Entscheidung über die zu nutzenden Drucksysteme ist zu begründen und zu dokumentieren.

Bestandteile

Der Druckauftrag, der von einer Anwendung erstellt wurde und an einen Drucker ausgegeben werden soll, muss mehrere Zwischenschritte durchlaufen. Für diese Schritte sind jeweils einzelne Komponenten zuständig, die im folgenden vorgestellt werden.

- **Druckclient**
  Bei einem Druckclient handelt es sich um eine Softwarekomponente, die auf dem Arbeitsplatz-PC installiert ist. In der Regel empfängt der Druckclient eine entsprechende Anweisung von einer Anwendung und sendet den Druckauftrag an den Druckserver weiter.
  Mit der Auswahl eines Druckernamens kann in vielen Fällen der Zieldrucker ausgewählt werden. Eine Ausnahme ist der Ausdruck in Druckerpools, bei denen für jeden Druckauftrag ein anderer Drucker vom Druckserver bestimmt werden kann.
  Häufig können weitere Funktionen, wie Duplexdruck und Heften, durch den Druckclient festgelegt werden. Hierfür sendet der Druckclient die Druckdaten an den Druckserver. Wie der Drucker angesteuert werden kann und welche Formate er beherrscht, wird in der Regel bei der Installation des Druckers dem Drucksystem bekannt gemacht.

- **Druckserver**
  Der Druckserver empfängt die Druckaufträge der Clients und verwaltet sie. Die Aufträge werden in eine Warteliste eingefügt und anschließend an den Drucker übertragen. Je nach Konfiguration wird bei mehreren Druckaufträgen das zuerst empfangene Dokument als erstes an den Drucker weitergeleitet oder durch eine entsprechende Priorität bevorzugt behandelt. In einigen Fällen lassen sich auch spezielle Zeiträume festlegen, in denen Druckaufträge ausgeführt werden.
  Das Dokument wird meistens direkt auf dem Druckserver für den Ausdruck aufbereitet. Dafür benötigt das Drucksystem die gerätespezifischen Druckerinformationen und Filter. Beispiele für die spezifizierten Parameter sind Papierformate, Rasterauflösungen, Schriftarten, Duplex, Heften, Lochen und Farbdruck. Anhand dieser Spezifikation kann die Druckanweisung, die an den Drucker übermittelt wird, generiert werden.
  Der Druckserver bereitet den Druckauftrag auf. Dazu konvertiert er ihn in ein Datenformat, das vom jeweiligen Drucker unterstützt wird. Ist das Eingangsformat beispielsweise PostScript, muss das Dokument in ein für diesen Drucker verständliches Ausgangsformat konvertiert werden, wenn der Drucker nicht PostScript-fähig ist. Beispiele für Ausgangsformate sind PDF, PCL und PostScript.

- **Drucker**
  Der Drucker empfängt das vorbereitete Dokument vom Druckserver und gibt es aus. Es kann zwischen logischen und physischen Druckern unterschieden werden. Logische Drucker werden auf Druckservern eingerichtet. Die Druckausgabe erfolgt über einen physischen Drucker. Folgende Anschlussarten werden in der Praxis für **physische Drucker** eingesetzt:

  - Lokale Drucker: Diese Drucker verfügen in der Regel über eine USB-Schnittstelle und werden direkt an ein IT-System, z. B. einen Arbeitsplatz-PC, angeschlossen.
  - Netzdrucker: Der physische Drucker wird von den einzelnen IT-Systemen über ein Netz angesprochen.
  - Druckserver mit lokalen Druckern: Der Druckserver wird von den einzelnen IT-Systemen über ein Netz angesprochen. An den Druckserver werden die physischen Drucker lokal angeschlossen. Dabei kann der Druckserver in Form einer Appliance oder als klassischer Server realisiert sein. Bei diesem Ansatz muss der Druckserver häufig zwischen Netz und den lokalen Anschlüssen der physischen Drucker konvertieren, beispielsweise als USB-Ethernet-Bridge.

- **Logische Drucker** auf Druckservern können innerhalb des Drucksystems unterschiedliche Aufgaben haben. Die folgenden Szenarien sind in der Praxis häufig anzutreffen:
  - Mehrere physische Drucker werden über einen logischen Drucker angesprochen. Neben dem Vorteil einer höheren Druckleistung (es kann parallel gedruckt werden), kann ohne größeren Konfigurationsaufwand auf einen anderen Drucker zugegriffen werden, wenn einer ausfällt. Es wird empfohlen, nur Geräte mit ähnlichen Eigenschaften in einer Klasse zusammenzufassen.
  - Ein physischer Drucker wird von mehreren logischen Druckern, die jeweils auf unterschiedlichen Druckservern installiert sind, angesprochen. Das bietet sich an, wenn mehrere Druckserver eingesetzt werden. Fällt ein Druckserver aus, kann einfach auf einen anderen Druckserver gewechselt werden, sodass der Druckbetrieb ohne größeren Konfigurationsaufwand fortgesetzt werden kann.
  - Des Weiteren können logische Drucker verwendet werden, um einem physischen Drucker mit mehreren verschiedenen Einstellungen jeweils einen eigenen Druckernamen zuzuordnen. Beispielsweise können für einen physischen Drucker zwei logische Drucker definiert werden: einer für Simplex- und einer für Duplex-Druck. Alle logischen Drucker sind zu dokumentieren.

Kommunikationsbeziehungen

Zwischen den einzelnen Komponenten eines Drucksystems entstehen unterschiedliche Kommunikationsverbindungen.

- **Kommunikation zwischen Druckclient und Druckserver**

  Die Kommunikationsverbindung kann zwischen einem Druckclient und dem Druckserver sowie zwischen verschiedenen Druckservern aufgebaut werden. Je nach Szenario werden die Druckinformationen über ein Netz oder lokal ausgetauscht. Je nach Drucksystem können folgende Protokolle eingesetzt werden:
  - HTTP (Hypertext Transfer Protocol),
  - IPP (Internet Printing Protocol),
  - LPR/LPD (Line Printer Remote / Line Printer Daemon),
  - SMB (Server Message Block) und
  - Appletalk beziehungsweise Bonjour.

  Abhängig von den eingesetzten Druckern und vom gewählten Drucksystem sind geeignete Protokolle auszuwählen. Innerhalb eines Netzes sollten möglichst wenig unterschiedliche Druck-Protokolle eingesetzt werden. Die Entscheidung ist zu dokumentieren.

  Auch für die Verwaltung müssen bei einigen Drucksystemen Informationen ausgetauscht werden. Die Clients müssen beispielsweise regelmäßig über die verfügbaren Drucker und deren Status informiert werden. Dabei können, je nach Drucksystem, folgende Strategien verfolgt werden:

- Broadcasting: In regelmäßigen Abständen sendet der Server unaufgefordert eine Nachricht an alle Clients in der Broadcast-Domäne.
- Polling: Der Druckclient fragt die Informationen vom Server ab.

  Broadcasting vereinfacht die Administration, ist aber mit weiteren Problemen verbunden. Befinden sich die Clients und Server in verschiedenen Broadcast-Domänen, erreichen die Pakete nicht alle Clients. In der Praxis können auch Probleme auftreten, wenn der Druckserver mehrere Netzschnittstellen hat und die Broadcast-Pakete an die falschen Schnittstellen sendet. Für die Konfiguration ist ein Verfahren auszuwählen und zu dokumentieren.

- **Kommunikation zwischen Druckserver und Drucker**

  Für die Kommunikation mit den Druckern werden ebenfalls entsprechende Protokolle benötigt. Diese hängen von den Druckerspezifikationen und von der Anschlussart ab. Beispielsweise gibt es Protokolle für

  - die Kommunikation über die parallele Schnittstelle,
  - den Anschluss über USB,
  - den Betrieb über die serielle Schnittstelle und
  - die netzbasierte Kommunikation mit den Druckern, beispielsweise über das HP JetDirect Protokoll oder über IPP (Internet Printing Protocol).

  Einige Druckersysteme ermöglichen auch die Konfiguration der Drucker über den Druckserver. Neben proprietären Protokollen wird hier oft das Simple Network Management Protocol (SNMP) eingesetzt.

  Es müssen Protokolle ausgewählt werden, die für die Anforderungen der Institution und für die einzusetzenden Komponenten geeignet sind. Die Entscheidungen sind zu dokumentieren.

Design der Druckerlandschaft

Neben der Auswahl des Drucksystems spielt die Anordnung der einzelnen Bestandteile, wie Clients, Server und Drucker, eine wichtige Rolle. Grob können folgende Ansätze für die Druckerarchitektur unterschieden werden:

- **Lokale Drucker**: Die Anwendung, die den Druckauftrag generiert, der Druckclient, der den Druckserver anfragt, sowie der Druckserver, der den Drucker ansteuert, werden gemeinsam auf einem IT-System, z. B. einem Arbeitsplatz-PC, betrieben. Der Drucker ist über die USB-, parallele oder serielle Schnittstelle an das IT-System angeschlossen.
- **IT-System**, z. B. Arbeitsplatz-PC, **mit Netz-Drucker**: Auf einem oder mehreren IT-Systemen befinden sich neben der generierenden Anwendung auch der Druckclient und der Druckserver. Die Druckserver der einzelnen IT-Systeme senden die Druckaufträge an einen netzfähigen Drucker.
- **Zentraler Druckserver**: Auf den IT-Systemen sind nur die Druckclients installiert. Diese nehmen den Druckauftrag an und leiten ihn über ein Netz an einen zentralen Druckserver weiter.
  Auf diesem Druckserver werden die Druckaufträge verwaltet. Der Druckserver sendet die Aufträge an lokale oder netzbasierte Drucker weiter, wo sie ausgegeben werden.
- **Kombinationen**: Es sind zahlreiche Kombinationen aus den oben genannten Anordnungen möglich. Ein Beispiel ist der Anschluss eines lokalen Druckers direkt an das IT-System für kleinere Druckaufträge und der parallele Betrieb eines zentralen Druckservers für umfangreiche Ausdrucke.

Die getroffenen Entscheidungen zum Aufbau der Druckerlandschaft sind zu dokumentieren.

Über **Dokumentenscanner** können analoge Informationen digitalisiert werden, beispielsweise um ein Papierdokument auf IT-Systeme zu kopieren und es dort zu archivieren oder weiter zu bearbeiten. Statt an jedem Arbeitsplatz-PC einen lokalen Scanner zu installieren, ist es meist wirtschaftlicher, einen oder mehrere zentrale Scanner zur Verfügung zu stellen. Um geeignete Sicherheitsmaßnahmen auszuwählen, muss zwischen Scan-PCs und netzfähigen Dokumentenscannern unterschieden werden.

Ein Scan-PC ist ein Standard-PC, der oft an ein LAN angebunden ist und an den ein lokaler Scanner angeschlossen ist. Scan-PCs werden häufig in ähnlichen Räumlichkeiten wie Netzdrucker betrieben und können von diversen Mitarbeitern benutzt werden. Außerdem ist auf Scan-PCs üblicherweise Software installiert, mit der die eingescannten Informationen nachbearbeitet werden können, also beispielsweise OCR (Optical Character Recognition)- oder Bildbearbeitungsprogramme.

Netzfähige Dokumentenscanner (*Büroscanner*) sind Kompaktgeräte, an denen Papierdokumente und Ähnliches ohne größeren Aufwand eingelesen und zur weiteren Bearbeitung über ein LAN an den Benutzer übertragen werden können, beispielsweise per E-Mail. Diese Funktion ist häufig auch in Faxgeräten integriert. Der Funktionsumfang von netzfähigen Dokumentenscannern ist meist deutlich geringer als bei Scan-PCs.

Scan-PC

Wird ein Standard-PC zum Scannen verwendet, so sind die Empfehlungen aus den Baustein SYS.2.1. *Allgemeiner Client* und den zutreffenden betriebssystemspezifischen Client-Bausteinen des IT-Grundschutz-Kompendiums umzusetzen.

Scan-PCs können im Produktivnetz, in einem Testnetz oder auch als Stand-Alone-System ohne einen Netzanschluss betrieben werden. Sie sollten so konfiguriert sein, dass sich die Benutzer authentisieren müssen. Die eingescannten Daten können über das Netz oder über transportable Datenträger zu den Arbeitsplatz-PCs übertragen werden.

Die analogen Scan-Vorlagen sollten nicht unbeaufsichtigt beim Gerät verbleiben. Auch die digitalen Scan-Ergebnisse sollten nach der Übertragung auf das gewünschte Zielsystem, zum Beispiel auf den Arbeitsplatz-PC des jeweiligen Benutzers, aus allen allgemein zugreifbaren Verzeichnissen gelöscht werden.

Netzfähige Dokumentenscanner

Mit diesen Geräten können auch ohne einen angeschlossenen PC Dokumente gescannt werden. Dabei werden die Dokumente in Bild-Dateien mit gängigen Dateiformaten umgewandelt.

Zur weiteren Bearbeitung müssen die Geräte die eingescannten Dokumente an andere IT-Systeme im Netz versenden. Folgende Übertragungs- und Speicherverfahren werden in der Regel unterstützt:

- **Ablage auf Netzlaufwerke:**

  Die eingescannten Dokumente werden direkt mittels eines Netzprotokolls zum Dateitransfer auf einen Datei-Server übertragen. Unterstützt werden in der Regel NFS- und SMB-Freigaben oder die Übertragung mittels FTP. Grundsätzlich sollte sichergestellt werden, dass der Personenkreis, der Zugriff auf die Zielverzeichnisse mit den eingescannten Daten hat, so klein wie möglich ist. Bei erhöhtem Schutzbedarf ist es eventuell erforderlich, dass nur der Benutzer, der die Informationen eingescannt hat, auch auf die Scan-Ergebnisse zugreifen kann. Nicht alle Scanner ermöglichen es, die erzeugten Dateien in benutzerspezifischen Bereichen der Server zu speichern. Wenn hierfür nur ein allgemein zugreifbares Verzeichnis gewählt werden kann, müssen die Dokumente so schnell wie möglich aus diesen öffentlichen Verzeichnissen gelöscht werden. Die Benutzer müssen entsprechend angewiesen werden. Zusätzlich sollten diese Verzeichnisse einmal täglich automatisch gelöscht werden. Der Zeitpunkt sollte den Benutzern bekannt gegeben werden und ist so zu wählen, dass zu diesen Zeiten keine Benutzer mit den Scannern arbeiten.

- **Scan-to-Mail:**

  Hierbei hat der Benutzer beim Scannen die Möglichkeit, eine E-Mail-Adresse oder eine Benutzer-Kennung, der eine E-Mail-Adresse zugeordnet ist, anzugeben. An diese E-Mail-Adresse wird die erzeugte Datei über einen voreingestellten SMTP-Server übermittelt. Da auf diese Weise vertrauliche Informationen anonym das Netz verlassen könnten, sollte darauf geachtet werden, dass keine externen E-Mail-Adressen eingegeben werden können. Besser ist es, auch den SMTP-Server so zu konfigurieren, dass von den netzfähigen Dokumentenscannern keine E-Mails an externe E-Mail-Adressen versendet werden können.

- **Scan-to-Print**:

Hier wird das Dokument direkt an einen Drucker gesendet, also die Scanner-Drucker-Kombination als digitaler Kopierer eingesetzt. Sind beide Geräte räumlich voneinander getrennt, besteht die Gefahr, dass während des Scannens die Dokumente unbefugt vom Drucker entfernt werden. Daher sollten die Systeme in diesem Fall möglichst so konfiguriert werden, dass der Ausdruck erst erfolgt, wenn alle Seiten des jeweiligen Dokuments vollständig eingescannt sind. Anderenfalls vergeht zwischen dem Scannen der ersten Seite und dem Abholen am Drucker unter Umständen zu viel Zeit.

- **Scan-to-Fax**:

  Das Verfahren Scan-to-Fax erlaubt es, eingescannte Dokumente direkt per Fax zu versenden. Hierfür wird beim Scannen eine Fax-Nummer angegeben. Das erzeugte Dokument wird dann entweder über ein integriertes Modem versendet, oder der Scanner baut über das LAN eine Verbindung zu einem Faxservers auf.

  Beim Einsatz von Scannern, die über eingebaute Fax- oder Modem-Schnittstellen verfügen, müssen besondere Sicherheitsvorkehrungen getroffen werden, damit über diese Schnittstellen keine unerwünschten Kommunikationsverbindungen mit externen Netzen aufgebaut werden.

  Wenn möglich, sollte ein zentraler Faxserver als Schnittstelle zwischen Scanner und Telefonnetz agieren. In diesem Fall sind insbesondere die Maßnahmen-Empfehlungen, die im Baustein NET.4.3 *Faxgeräte und Faxserver* aufgeführt sind, anzuwenden.

Wenn die eingesetzten Komponenten dies unterstützen, sollten die Kommunikationsverbindungen möglichst verschlüsselt werden, um zu erschweren, dass Angreifer die übertragenen Informationen abhören.

Nach dem Scannen dürfen keine Restinformationen auf dem System verbleiben. Die Dokumentenspeicher des Geräts sollten möglichst automatisch gelöscht werden, wenn der Scan-Vorgang abgeschlossen ist. Ist das nicht realisierbar, müssen die Benutzer darauf hingewiesen werden, dass sie die Dokumentenspeicher des Geräts nach der Benutzung manuell löschen müssen, damit nachfolgende Benutzer die eingescannten Informationen nicht einsehen können. Entsprechende Sicherheitsvorkehrungen müssen auch für sonstige Speicherbereiche getroffen werden, die im Rahmen des Scan-Vorgangs verwendet werden, beispielsweise für die dabei benutzten Netzlaufwerke.

3.2 Quellenverweise

Für diese Umsetzungshinweise sind keine Quellenverweise vorhanden.