Bundesamt
für Sicherheit in der
Informationstechnik

SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte

1. Beschreibung

1.1. Einleitung

Moderne Drucker, Kopierer und Multifunktionsgeräte sind komplexe Geräte, die neben mechanischen Komponenten eigene Betriebssysteme enthalten und Serverdienste und -funktionen bereitstellen. Da die Geräte oft vertrauliche Informationen verarbeiten, müssen sie bzw. die gesamte Druck- und Scan-Infrastruktur geschützt werden.

Als Multifunktionsgeräte werden Geräte bezeichnet, die mehrere papierverarbeitende Funktionen bieten, etwa Drucken, Kopieren, Scannen sowie auch Versenden und Empfangen von Fax-Dokumenten.

Für viele Geschäftsprozesse und Fachaufgaben wird auch heute noch Papier als Informationsträger benutzt. Damit sind Drucker, Kopierer oder Multifunktionsgeräte wichtige Komponenten in der IT-Infrastruktur. Fallen die Geräte aus oder werden verfälschte Dokumente ausgedruckt, kann sich das mitunter auf kritische Prozesse auswirken und zu erheblichen wirtschaftlichen Schäden führen.

1.2. Zielsetzung

Dieser Baustein beschreibt, wie sich Drucker, Kopierer und Multifunktionsgeräte sicher betreiben lassen, sodass weder Informationen über diese Geräte abfließen können noch durch sie die Sicherheit der übrigen internen IT-Infrastruktur beeinträchtigt wird.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.4.1 *Drucker, Kopierer und Multifunktionsgeräte* ist für jeden Drucker, Kopierer oder jedes Multifunktionsgerät im Informationsverbund anzuwenden.

Der Baustein behandelt die Sicherheit von Druckern, Kopierern und Multifunktionsgeräten. Vernetzte oder lokal an IT-Systemen angeschlossene Dokumentenscanner werden nicht explizit berücksichtigt. Die Risiken und Anforderungen lassen sich jedoch aus denen für Multifunktionsgeräte ableiten. Ebenso werden vernetzte Faxgeräte nicht gesondert betrachtet. Die in diesem Baustein aufgeführten Risiken und Anforderungen für die Faxfunktion gelten deshalb auch für diese Art von Geräten. Ergänzend sind die Anforderungen des Bausteins NET.4.3 *Faxgeräte und Faxserver* zu berücksichtigen.

Drucker, Kopierer und Multifunktionsgeräte werden oft an Datennetze angeschlossen. Neben kabelgebundenen Anschlüssen können einige Geräte auch direkt mit einem WLAN verbunden werden. Empfehlungen hierzu sind in den Bausteinen der Teilschicht NET *Netze und Kommunikatio*n zu finden, wie z. B. im Baustein NET.2.2 *WLAN-Nutzung*.

Auf Druckern, Kopierern und Multifunktionsgeräten sind oft vertrauliche Informationen gespeichert, die nach der Außerbetriebnahme auf den Geräten verbleiben. Geleaste Geräte werden häufig, je nach Vertrag, nach einer vorher festgelegten Nutzungsdauer oder -häufigkeit ausgetauscht. Sie werden spätestens nach Ablauf des Leasingvertrags zurückgegeben. Auch Papier und andere Betriebsmittel können vertrauliche Informationen beinhalten. Bevor diese Geräte und Betriebsmittel ausgesondert, getauscht, instandgesetzt oder zurückgegeben werden, müssen alle sensiblen Informationen von ihnen gelöscht werden. Empfehlungen hierzu sind nicht Gegenstand des vorliegenden Bausteins, sondern sind im Baustein CON.6 *Löschen und Vernichten* zu finden.

Bei Druckservern handelt es sich um IT-Systeme mit Druckwarteschlangen, Druckjobverwaltung und möglichen weiteren Funktionen, z. B. Treiberverteilung oder gesichertes Drucken. Für jeden Druckserver müssen die generellen und betriebssystemspezifischen Sicherheitsanforderungen für Server erfüllt werden. Diese werden nicht in diesem Baustein, sondern in den Bausteinen SYS.1.1 *Allgemeiner Server* und den jeweiligen betriebssystemspezifischen Server-Bausteinen beschrieben.

Ein essentieller Schwerpunkt bei der Absicherung von Druckern, Kopierern und Multifunktionsgeräten ist es, die auf den Geräten installierte Software regelmäßig zu aktualisieren und dadurch Softwareschwachstellen zu schließen. Der vorliegende Baustein behandelt diesen Aspekt allerdings nicht. Anforderungen hierzu sind im Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* zu finden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.4.1 *Drucker, Kopierer und Multifunktionsgeräte* von besonderer Bedeutung.

2.1. Unerlaubte Einsicht in ausgedruckte Dokumente

Ausgedruckte Dokumente verbleiben oft für eine längere Zeit im Ausgabefach von zentralen Druckern und Multifunktionsgeräten, weil beispielsweise erst mehrere Dateien ausgedruckt und später alle zusammen abgeholt werden. Auch kann es sein, dass am Client ein falscher Drucker ausgewählt wurde und sich die Dokumente nicht am erwarteten Ort befinden. Da Etagen- oder Abteilungsdrucker von vielen Benutzenden verwendet werden, können so auch unberechtigte Personen schützenswerte Informationen einsehen oder mitnehmen.

Auch liegengebliebene Ausdrucke in den Ausgabefächern dezentraler Arbeitsplatzdrucker, die sich in unmittelbarer Nähe in den Büroräumen befinden, sind ein Risiko. Denn Personen, die Zutritt zu diesen Räumen haben, könnten die Ausdrucke ebenso einsehen oder entnehmen.

Eine weitere Gefahr sind im Ausgabefach befindliche Faxdokumente und ausgedruckte Sendeprotokolle, auf denen neben Faxnummer, Datum, Uhrzeit und Seitenzahl mitunter ein verkleinertes Abbild der ersten Seite zu sehen ist. Da solche Protokolle erst ausgegeben werden, nachdem ein Fax verschickt wurde oder ein Sendefehler aufgetreten ist, könnten sie auch über einen längeren Zeitraum im Gerät liegen bleiben oder gar nicht abgeholt werden. Dadurch befinden sich unter Umständen vertrauliche Informationen unbeaufsichtigt im Ausgabefach und können im schlimmsten Fall gestohlen werden.

Zudem werden nicht abgeholte Dokumente irgendwann entsorgt. Das geschieht oft, indem die Ausdrucke wahllos in nahegelegene Papierkörbe geworfen werden, statt Ausdrucke mit

schützenswerten Informationen sicher zu vernichten. Dadurch können diese Informationen in die öffentliche Müllentsorgung und so in die Hände Dritter gelangen.

Auch viele Telearbeitsplätze werden mit einem eigenen Drucker oder Multifunktionsgerät ausgestattet. Hierdurch können ebenfalls schützenswerte Informationen offengelegt werden.

2.2. Sichtbarkeit von Metadaten

Zusammen mit einem Druckauftrag werden Metadaten gesendet, die in der Regel die Kennung der Benutzenden, Datum, Uhrzeit und den Namen des Druckauftrages enthalten. Diese Daten werden im Bedienfeld und im Webserver vieler Drucker und Multifunktionsgeräte angezeigt. Der Name des Druckauftrages ergibt sich oft aus dem Namen des digitalen Dokumentes. Falls der Drucker über einen integrierten Webserver verfügt, können über einen Browser oft vertrauliche Vorgänge eingesehen werden. Ebenso sind die Metadaten auf den Druckservern im Klartext sichtbar, sofern sie nicht anonymisiert werden. Damit können Dritte an vertrauliche Informationen gelangen. Viele Geräte erlauben es zudem, Druckaufträge abzuspeichern, um sie später nach Authentisierung über eine PIN auszudrucken. Auch in diesem Fall wird der Name aller vorhandenen Dokumente im Bedienfeld eines Ausgabegerätes angezeigt.

Bestimmte Drucker und Kopierer drucken sogenannte „Yellow Dots“ (auch „Machine Identification Code“, „Tracking Dots“, „Secret Dots“) auf das Papier. Diese oft undokumentierten Wasserzeichen können das Datum und die Uhrzeit sowie die Seriennummer des Druckers beinhalten und sind mit dem bloßen Auge kaum zu erkennen. Auf diese Weise kann ein Ausdruck einer Institution oder einer bestimmten Person direkt zugewiesen und so zu der Person zurückverfolgt werden, die den Text verfasst hat. Neben datenschutzrechtlichen Auswirkungen könnten so ungewollt Informationen die Institution verlassen.

Auch Faxprotokolle können bei vielen Multifunktionsgeräten ohne Zugriffsschutz ausgedruckt werden. Selbst wenn nur Telefonnummer, Datum, Uhrzeit und Seitenzahl aufgelistet werden, können damit schon Rückschlüsse auf personenbezogene Daten oder geschäftliche Vorgänge ermöglicht werden.

2.3. Ungenügender Schutz gespeicherter Informationen

Drucker, Kopierer und Multifunktionsgeräte sind oft mit nichtflüchtigen Speichern ausgestattet, auf denen Informationen temporär oder auch längerfristig abgelegt werden. So werden dort z. B. Adressbücher, Dokumente, Fax-Dateien und Druckaufträge abgespeichert. Sind diese Informationen unzureichend geschützt, können Dritte darauf zugreifen und sie auslesen. Unter Umständen können sogar bereits gelöschte Informationen rekonstruiert werden, wenn unsichere Löschmethoden angewendet wurden.

Über Netzprotokolle können Daten im Gerät gespeichert und gelesen werden. Drucker und Multifunktionsgeräte mit Datenträgern sind, wenn diese nicht gesichert werden, oft als nicht autorisierte Fileserver nutzbar. Auf diese Weise können unkontrolliert Informationen dezentral abgespeichert werden, die nicht im Datensicherungskonzept berücksichtigt werden.

2.4. Unverschlüsselte Kommunikation

Druck- und Scandaten werden oft unverschlüsselt über das Netz übertragen. Dadurch können die gesendeten Dokumente mitgelesen werden. Ebenso lassen sich in Druckservern temporär gespeicherte Druckdateien auslesen. Das gilt auch für zentrale Scan- und Dokumentenverarbeitungssysteme.

Weitere Gefahrenquellen sind unverschlüsselte Kommunikationsschnittstellen zur Administration der Geräte. Wird beispielsweise über HTTP, SNMPv2 oder Telnet auf Drucker zugegriffen, werden die Informationen dabei ungeschützt transportiert. Dadurch sind die Zugriffsinformationen inklusive Gerätepasswörter gefährdet.

2.5. Unberechtigter Versand von Informationen

Viele Multifunktionsgeräte können digitalisierte Papierdokumente per E-Mail und Fax verschicken. Ohne besondere Schutzmaßnahmen können dadurch Informationen bewusst oder auch versehentlich an nicht autorisierte Empfänger oder Empfängerinnen gelangen. Benutzende könnten beispielsweise Adressen oder Telefonnummern falsch eingeben. Als Folge werden eventuell schutzbedürftige Daten unbeabsichtigt an falsche Empfänger oder Empfängerinnen gesendet. Außerdem können mithilfe der E-Mail- oder Fax-Funktion vertrauliche Unterlagen schnell nach außen gelangen.

Viele vernetzte Drucker lassen sich so konfigurieren, dass Druckaufträge aus dem Internet per E-Mail empfangen und gescannte Dokumente als E-Mail-Anhang versendet werden können. Dabei lässt sich die freie Eingabe der Absendendenadresse missbrauchen, um E-Mails unter fremden Namen an interne und externe Personen zu versenden.

2.6. Unkontrollierter Datenaustausch über Speicherschnittstellen bei Druckern, Kopierern und Multifunktionsgeräten

Dokumente auf Papier können mithilfe von Multifunktionsgeräten schnell kopiert werden. Durch vorhandene USB- oder SD-Anschlüsse ist es zudem möglich, selbst große Mengen an Papierunterlagen direkt und ohne jegliche Kontrolle zu digitalisieren und auf USB-Sticks oder SD-Karten zu speichern. Auch können über die Speicherschnittstellen hierauf abgelegte Dokumente direkt ausgedruckt werden.

Sind die Drucker, Kopierer und Multifunktionsgeräte an ein Datennetz oder direkt an Clients angeschlossen, können IT-Systeme oft auch direkt auf die an Drucker, Kopierer und Multifunktionsgeräte angeschlossenen Speichermedien zugreifen. Auch wenn die Einbindung von Speichermedien an IT-Systeme selbst technisch verhindert wird, können über diesen Umweg unkontrolliert Informationen über die Speicherschnittstellen kopiert werden.

Auf diese Weise kann zum einen über die Speicherschnittstellen (Schad-)Software über die Multifunktionsgeräte auf den hieran angeschlossen Clients oder in das Datennetz der Institution gelangen. Zum anderen können auch vertrauliche (Papier-)Dokumente unbemerkt digitalisiert und unnachvollziehbar gestohlen werden.

2.7. Ungenügend abgesicherte Netzzugänge von Druckern, Kopierern und Multifunktionsgeräten

Firewalls zwischen LAN und Internet werden häufig so konfiguriert, dass ganze Subnetze auf das Internet zugreifen können. Zudem werden Drucker, Kopierer und Multifunktionsgeräte oft dem gleichen Subnetz zugeordnet wie die Clients. Dadurch können z. B. auch die Netzdrucker auf Informationen im Internet zugreifen. Auch wenn die IT-Systeme der Institution nur über einen Proxy auf das Internet zugreifen, können Drucker, Kopierer und Multifunktionsgeräte diesen ebenfalls nutzen. Wenn die Verbindungen von und zu den Druckern aus dem Internet nicht von der Firewall abgewiesen werden, können unter Umständen schützenswerte Informationen unerwünscht das eigene Datennetz verlassen. Umgekehrt könnte ein netzfähiges Gerät unerwünscht Daten aus dem Internet empfangen und weiter verteilen. Ein Netzdrucker kann dadurch z. B. zu einem Einfallstor für Angriffe aus dem Internet werden.

2.8. Mangelhafter Zugriffsschutz zur Geräteadministration

Vernetzte Drucker, Kopierer und Multifunktionsgeräte können über das Bedienfeld und den eingebauten Webserver verwaltet werden. Bei Auslieferung der Geräte haben diese in der Regel kein oder nur ein Standardpasswort. Wird das Passwort nicht gesetzt oder nicht geändert, kann sehr leicht auf die Geräte zugegriffen werden.

In vielen Institutionen werden zudem einheitliche Passwörter für alle Drucker und Multifunktionsgeräte benutzt, die nur selten geändert werden. Dadurch sind sie oft vielen internen und externen Personen bekannt und unbefugte Dritte können somit einfach auf die Geräte zugreifen.

Weiter lassen sich über Bootmenüs Drucker und Multifunktionsgeräte in den Werkszustand zurücksetzen. Davon betroffen sind auch die Sicherheitseinstellungen. So ist beispielsweise das Gerätepasswort oft nicht mehr vorhanden, nachdem der Drucker oder das Multifunktionsgerät auf die Werkseinstellungen zurückgesetzt wurde. Ungesicherte Bootmenüs erleichtern zwar die Administration, verringern aber gleichzeitig die Sicherheit.

Drucker, Kopierer und Multifunktionsgeräte sind mit zahlreichen Netzprotokollen ausgerüstet. Bei Auslieferung sind meistens alle Protokolle aktiviert. Dadurch könnten Angreifende z. B. auf die Geräteeinstellungen zugreifen und diese so verändern, dass schützenswerte Informationen aus dem Netz abfließen.

Viele Geräte können ihr Bedienfeld über das Netz an den Support übertragen. Damit können jedoch auch vertrauliche Eingaben der Benutzenden am Bedienfeld des Gerätes mitgelesen werden.

In größeren Institutionen gibt es meistens sehr viele Drucker, Kopierer und Multifunktionsgeräte. Um diese noch effizient verwalten und überwachen zu können, wird oft eine Gerätemanagementsoftware eingesetzt. Viele Institutionen schützen diese Software jedoch nicht ausreichend vor unberechtigten Zugriffen, da sie als weniger kritisches System wahrgenommen wird. Dadurch können einzelne oder auch alle Geräte unbeabsichtigt oder bewusst verändert werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.4.1 *Drucker, Kopierer und Multifunktionsgeräte* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Informationssicherheitsbeauftragte (ISB)

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.4.1.A1 Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten (B)

Bevor Drucker, Kopierer und Multifunktionsgeräte beschafft werden, MUSS der sichere Einsatz geplant werden. Dabei SOLLTEN folgende Kriterien berücksichtigt werden:

- Unterstützung sicherer Protokolle zur Datenübertragung und Administration,
- Verschlüsselung der abgespeicherten Informationen,
- Authentisierung der Benutzenden direkt am Gerät,

- Nutzung physischer Schutzmechanismen, wie Ösen zum Diebstahlschutz oder Geräteschlösser,
- Existenz eines zuverlässigen und leistungsfähigen automatischen Seiteneinzugs der Scaneinheit,
- Unterstützung geeigneter Datenformate,
- Bei Bedarf Unterstützung von Patch- sowie Barcodes zur Dokumententrennung und Übergabe von Metainformationen,
- Existenz einer Funktion zum sicheren Löschen des Speichers sowie
- Verfügbarkeit von regelmäßigen Updates und Wartungsverträgen.

Es MUSS festgelegt werden, wo die Geräte aufgestellt werden dürfen. Außerdem MUSS festgelegt sein, wer auf die Drucker, Kopierer und Multifunktionsgeräte zugreifen darf. Die Ergebnisse SOLLTEN in einem Basiskonzept dokumentiert werden.

SYS.4.1.A2 Geeignete Aufstellung und Zugriff auf Drucker, Kopierer und Multifunktionsgeräte (B)

Der IT-Betrieb MUSS Drucker, Kopierer und Multifunktionsgeräte so aufstellen und absichern, dass nur befugte Personen die Geräte verwenden und auf verarbeitete Informationen zugreifen können. Außerdem MUSS sichergestellt sein, dass nur berechtigte Personen die Geräte administrieren, warten und reparieren können. Mit Dienstleistenden (z. B. für die Wartung) MÜSSEN schriftliche Vertraulichkeitsvereinbarungen getroffen werden.

Drucker, Kopierer und Multifunktionsgeräte MÜSSEN mit Gerätepasswörtern versehen sein, um so den Zugriff auf Webserver und Bedienfeld für die Administration zu sperren. Diese MÜSSEN die Vorgaben des Identitäts- und Berechtigungsmanagements der Institution erfüllen.

SYS.4.1.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.4.1.A12 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.4.1.A13 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.4.1.A22 Ordnungsgemäße Entsorgung ausgedruckter Dokumente (B)

Nicht benötigte, aber ausgedruckte Dokumente mit vertraulichen Informationen MÜSSEN in geeigneter Weise vernichtet werden. Sind Heimarbeitsplätze mit Druckern, Kopierern oder Multifunktionsgeräten ausgestattet, SOLLTE gewährleistet werden, dass die ausgedruckten Informationen auch direkt vor Ort geeignet vernichtet werden können, wenn sie nicht mehr benötigt werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.4.1.A4 Erstellung einer Sicherheitsrichtlinie für den Einsatz von Druckern, Kopierern und Multifunktionsgeräten (S)

Die Institution SOLLTE eine Sicherheitsrichtlinie für Drucker, Kopierer und Multifunktionsgeräte entwickeln. Darin SOLLTE geregelt werden, welche Anforderungen und Vorgaben an die Informationssicherheit der Geräte gestellt und wie diese erfüllt werden sollen. Es SOLLTE auch

festgelegt werden, welche Funktionen von welchen Benutzenden unter welchen Bedingungen administriert beziehungsweise genutzt werden dürfen.

SYS.4.1.A5 Erstellung von Nutzungsrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten (S) [Informationssicherheitsbeauftragte (ISB)]

Für die Institution SOLLTE der oder die ISB eine Nutzungsrichtlinie erstellen, auf der alle Sicherheitsvorgaben zum Umgang mit den Geräten übersichtlich und verständlich zusammengefasst sind. Die Nutzungsrichtlinie SOLLTE allen Benutzenden bekannt sein.

SYS.4.1.A6 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.4.1.A7 Beschränkung der administrativen Fernzugriffe auf Drucker, Kopierer und Multifunktionsgeräte (S)

Der IT-Betrieb SOLLTE sicherstellen, dass der administrative Fernzugriff auf Drucker, Kopierer und Multifunktionsgeräte nur einer klar definierten Gruppe des Administrations- und Servicepersonals ermöglicht wird. Das SOLLTE auch dann gewährleistet sein, wenn die Institution eine zentrale Geräteverwaltungssoftware einsetzt.

Es SOLLTE festgelegt werden, ob die Anzeige des Bedienfelds über ein Datennetz eingesehen werden darf. Wenn dies gewünscht ist, SOLLTE es nur an den IT-Betrieb übertragen werden können. Auch SOLLTE dies mit den betroffenen Benutzenden abgestimmt sein.

SYS.4.1.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.4.1.A9 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.4.1.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.4.1.A11 Einschränkung der Anbindung von Druckern, Kopierern und Multifunktionsgeräten (S)

Der IT-Betrieb SOLLTE sicherstellen, dass netzfähige Drucker, Kopierer und Multifunktionsgeräte nicht aus Fremdnetzen erreichbar sind. Wenn Multifunktionsgeräte an das Telefonnetz angeschlossen werden, SOLLTE sichergestellt werden, dass keine unkontrollierten Datenverbindungen zwischen dem Datennetz der Institution und dem Telefonnetz aufgebaut werden können. Netzdrucker und Multifunktionsgeräte SOLLTEN in einem eigenen Netzsegment, das von den Clients und Servern der Institution getrennt ist, betrieben werden.

SYS.4.1.A15 Verschlüsselung von Informationen bei Druckern, Kopierern und Multifunktionsgeräten (S)

Wenn möglich, SOLLTEN alle auf geräteinternen, nichtflüchtigen Speichermedien abgelegten Informationen verschlüsselt werden. Auch Druckaufträge SOLLTEN möglichst verschlüsselt übertragen werden.

SYS.4.1.A17 Schutz von Nutz- und Metadaten (S)

Nutz- und Metadaten wie Druckaufträge und Scandateien SOLLTEN 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 nicht für Unberechtigte sichtbar sind. Es SOLLTE von der Institution geregelt werden, wie mit Metadaten versehene Ausdrucke an Dritte weitergegeben werden.

SYS.4.1.A18 Konfiguration von Druckern, Kopierern und Multifunktionsgeräten (S)

Alle Drucker und Multifunktionsgeräte SOLLTEN nur vom IT-Betrieb konfiguriert werden können. Nicht benötigte Gerätefunktionen SOLLTEN abgeschaltet werden. Insbesondere SOLLTEN alle nicht benötigten Daten- und Netzschnittstellen von Druckern, Kopierern und Multifunktionsgeräten deaktiviert 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, SOLLTEN vom IT-Betrieb durch verschlüsselte ersetzt oder abgeschaltet werden. Das SOLLTE insbesondere für Protokolle umgesetzt werden, mit denen sich die Gerätekonfiguration verändern lässt, z. B. SNMP, Telnet und PJL.

SYS.4.1.A19 ENTFALLEN (S)

Diese Anforderung ist entfallen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.4.1.A14 Authentisierung und Autorisierung bei Druckern, Kopierern und Multifunktionsgeräten (H)

Nur berechtigte Personen SOLLTEN auf die ausgedruckten oder kopierten Dokumente zugreifen können. Es SOLLTEN möglichst nur zentrale Drucker, Kopierer und Multifunktionsgeräte eingesetzt werden, bei denen sich die Benutzenden am Gerät authentisieren, bevor der Druckauftrag startet („Secure-Print“). Nachdem sich die Benutzenden authentisiert haben, SOLLTEN ausschließlich nur die eigenen Druckaufträge sichtbar sein. Nur die für die jeweiligen Benutzenden notwendigen Funktionen SOLLTEN freigeschaltet werden.

SYS.4.1.A16 Verringerung von Ausfallzeiten bei Druckern, Kopierern und Multifunktionsgeräten (H)

Um die Ausfallzeiten von Druckern, Kopierern und Multifunktionsgeräten so gering wie möglich zu halten, SOLLTEN unter anderem

- Ersatzgeräte bereitstehen,
- in Wartungsverträgen auf eine angemessene Reaktionszeit geachtet werden,
- eine Liste mit Fachhandlungen geführt werden, um schnell Ersatzgeräte oder -teile beschaffen zu können und
- falls erforderlich, häufig benötigte Ersatzteile gelagert werden.

SYS.4.1.A20 Erweiterter Schutz von Informationen bei Druckern, Kopierern und Multifunktionsgeräten (H)

Es 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 Benutzenden 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 den E-Mail-Adressen der authentisierten Benutzenden versendet werden können. Auch SOLLTEN Dokumente nur an interne E-Mail-Adressen verschickt werden können.

Eingehende Fax-Dokumente sowie Sendeberichte SOLLTEN nur autorisierten Personen zugänglich sein.

SYS.4.1.A21 Erweiterte Absicherung von Druckern, Kopierern und Multifunktionsgeräten (H)

Der IT-Betrieb SOLLTE die Sicherheitseinstellungen von Druckern, Kopierern und Multifunktionsgeräten regelmäßig kontrollieren und, falls notwendig, 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 auf Druckern und Multifunktionsgeräten installiert werden kann, die nicht von den jeweiligen Herstellenden verifiziert und freigegeben wurde.

4. Weiterführende Informationen

4.1. Wissenswertes

Die Allianz für Cybersicherheit (ACS) gibt in den BSI-Empfehlungen „Drucker und Multifunktionsgeräte im Netzwerk BSI-CS 015" sowie „Sichere Passwörter in Embedded Devices (BSI-CS 069)" Hinweise zu den genannten Themen. Auch in dem Whitepaper „Datenschutz und IT-Sicherheit in Druckinfrastrukturen" der ACS-Partnerfirma mc² management consulting GmbH sind vertiefende Informationen zu Druckern, Kopierern und Multifunktionsgeräten zu finden.

Das National Institute of Standards and Technology (NIST) beschreibt in seiner Special Publication 800-53 „Security and Privacy Controls for Federal Information Systems and Organizations", insbesondere in dem Kapitel „PE-5 Access control for output devices", Anforderungen an Ausgabegeräte wie Drucker, Kopierer und Multifunktionsgeräte.

Das IEEE Standard Schutzprofil für Multifunktionsgeräte im IEEE Std 2600TM-2008 Operational Environment B, "IEEE Std 2600.2TM-2009" wurde von dem IEEE Computer Society, Information Assurance (C/IA) Committee als Basis für die Erstellung von Sicherheitsvorgaben entwickelt, um eine Zertifizierung eines IT-Produkts, des Evaluierungsgegenstands (EVG) durchzuführen.