Whitepaper

Datenschutz und Informationssicherheit in Druckinfrastrukturen

DEUTSCHER
LANDKREISTAG

Inhaltsverzeichnis

2. Version 11.4.2018

Autoren:

Andreas Scholtz, LL.B.
Dipl.-Ing. (TU) Martin Stolle

in redaktioneller Zusammenarbeit mit

Markus Albert, Stadt Frankfurt
Claudia Engel, Dortmunder Systemhaus
Britta Gerken, Ministerium für Schule und Bildung NRW
Regina Holzheuer, Landratsamt Esslingen
Jens Lange, Stadt Kassel
Maik Poburski, Landkreis Osnabrück
Heino Reinartz, Städteregion Aachen
Heino Sauerbrey, Deutscher Landkreistag

Kontakt:

mc² management consulting GmbH
Ludwig-Rinn-Str. 14 – 16
D-35452 Heuchelheim
Telefon: +49 641 966 2370
E-Mail: info@mc-2.de

1. Einleitung

Drucker, Multifunktionsgeräte, Scanner, Faxgeräte und die dazu gehörigen Softwarekomponenten sind ein Teil der betrieblichen Informationsverarbeitung. Der Fokus von Datenschutz und Informationssicherheit liegt in vielen Organisationen auf den digitalen Daten und der IT-Infrastruktur. Die Vertraulichkeit und rechtliche Bewertung einer Information ist aber unabhängig von ihrem Träger. Papierdokumente mit Informationen müssen genauso wie ihre digitalen Gegenstücke behandelt und geschützt werden.

Ausdrucke und Scans werden als notwendiges Element innerhalb von Verwaltungsvorgängen und geschäftlichen Prozessen verwendet. Damit hat die Verfügbarkeit und Integrität der Dokumenteninfrastruktur eine hohe Priorität. Als Konsequenz sind Geräte und Softwarekomponenten durch Härtung gegen bekannte Angriffs- und Störungsszenarien zu schützen.

Verstöße gegen den Datenschutz und die Informationssicherheit werden unabhängig von der Quelle des Problems geahndet: Abhängig vom Vorfall und den dadurch berührten relevanten Gesetzen sowie Verordnungen, können signifikante Geld- und Freiheitsstrafen verhängt werden. Diesbezüglich sind Verstöße gegen die Datenschutzgrundverordnung oder strafbewährte Verstöße des Geheimnisverrates (Betriebs- und Geschäftsgeheimnisse, Privatgeheimnis) denkbar. Deshalb unterliegen Drucker, Scanner, Fax- und Multifunktionsgeräte der gleichen Sorgfaltspflicht wie alle anderen Elemente der IT-Infrastruktur. Datenschutz und Informationssicherheit sind auch für die Druckinfrastruktur zu gewährleisten.

Dieses Whitepaper ist ein komprimierter Leitfaden zur Erarbeitung von Datenschutz und Informationssicherheit. Die erforderlichen technischen und organisatorischen Maßnahmen sind beschrieben.

Im Sinne einer besseren Lesbarkeit wird entweder die männliche oder weibliche Form von personenbezogenen Hauptwörtern in diesem Dokument genutzt. Dies impliziert keinesfalls eine Benachteiligung des jeweils anderen Geschlechts. Frauen und Männer mögen sich von den Inhalten dieses Dokuments gleichermaßen angesprochen fühlen.

2. Rechtliche Betrachtung

Jede Information hat einen juristischen Kontext (juristischen Tag). Je nach Bedeutung der Information ist dieser größer oder kleiner. Das etwaige rechtliche Risiko einer Information ist unabhängig vom Informationsträger. Es spielt keine Rolle, ob sie in einem Gespräch, digital oder als vergessener Ausdruck in falsche Hände gerät.

Das primäre Risiko von Organisationen entsteht nicht nur durch externe Akteure, sondern auch durch interne Gefahrenquellen. Vertrauliche Informationen und/oder personenbezogene Daten müssen zwingend durch interne Vorsorge geschützt werden. Denn

rechtliche Verstöße - ob vorsätzlich oder fahrlässig – können je nach Schweregrad erheblich geahndet werden. Die Sanktionen reichen von hohen Geldbußen (ggf. sogar in das Privatvermögen) bis zu mehrjährigen Freiheitsstrafen.

Ein außer Betracht lassen von Sicherungsmaßnahmen, welches zu Datenschutzverstößen oder anderen Verletzungen führen kann, geht gleichermaßen zu Lasten der jeweils betroffenen Bürger wie auch der (IT-) Verantwortlichen – gleich ob Vorstand, Geschäftsführung, Behördenleitung, angestellter oder externer IT-Administrator. Die Organisationen sind zu erhöhter Sorgfalt verpflichtet. Es ist somit essentiell, Datenschutz und Informationssicherheit unter anderem im Bereich der Druckinfrastrukturen umfänglich zu diskutieren, durchzusetzen und zu dokumentieren.

Die Modernisierung von Organisationen ist auf zeit- und ortsunabhängige Dienste ausgerichtet. Dabei macht diese Modernisierung nicht vor Druckinfrastrukturen halt. In Hinblick auf diesen Trend ist es entscheidend, dass das Grundrecht auf die Gewährleistung der Vertraulichkeit und der Integrität informationstechnischer Systeme gewahrt bleibt (BVerfG v. 27.02.2008 – 1 BvR 370/07, 1BvR 595/07, BVerfG 120, 274).

Es wird einen Übergang der traditionellen, vielfach papierbasierenden Organisation zu rein digitalen Prozessen geben. Papierverarbeitende Endgeräte erhalten eine wichtige Rolle in der Zwischenperiode. Scanprozesse sind die Schnittstelle zu neuen Systemen für die Verarbeitung und Speicherung von Daten. Die notwendigen Technologien sind in den Organisationen bereits weitestgehend vorhanden.

Die Beschaffungen dafür sind so zu steuern, dass neue Elemente der Infrastruktur sowie zukünftige Prozesse dem Anspruch an die Informationssicherheit und den Datenschutz genügen. Mit durchdachten Beschaffungen lassen sich die Kosten einer Druck- und Dokumenteninfrastruktur signifikant reduzieren und zukünftige Investitionen in Dokumentenprozesse minimieren.

3. Risiken

Die Druck- und Dokumenteninfrastruktur birgt sowohl Datenschutz- als auch geschäftliche Risiken. Eine Bewertung ist über die Analyse der betrieblichen Situation möglich.

Beispiele für Risiken:

- Dokumente mit auch innerbetrieblich vertraulichen Informationen liegen ungeschützt in der Ausgabe von zentralen Druckern und Multifunktionsgeräten. Mitarbeiter bekommen Einblick in personenbezogene Daten von Kolleginnen und Kollegen. Innerhalb der Organisationen kann dies zu Misstrauen unter Mitarbeitern, Mobbing, einem schlechten Arbeitsklima oder Zweifeln am Management führen. Die mögliche rechtliche Folge sind Ermittlungen, ein Bußgeldverfahren und Rechtsstreitigkeiten.
- Das Sendeprotokoll eines Faxgerätes gibt Hinweise zu einer Verhandlung über eine börsenrelevante Firmenübernahme. Es erfolgt eine Untersuchung über Insiderhandel.

- Der Ausfall eines Druckservers in einem Industriebetrieb kann kurzfristig nicht behoben werden. Produktion und Logistik müssen für mehrere Stunden unterbrochen werden. Ein großer Kunde muss als Folge seine eigene Fertigung unterbrechen. Die eigenen Verluste und die Regressforderungen verursachen einen immensen finanziellen Schaden.
- In einem Untersuchungsverfahren zu einem (beispielsweise strafrechtlichen) Konflikt muss zum Schutz eines wichtigen Zeugen dessen Identität geheim gehalten werden. Im Rahmen des Verfahrens werden Papierdokumente genutzt. Der „unsichtbar" aufgedruckte Maschinenidentifikationscode (mitgedruckte Wasserzeichen auf Basis „gelber Punkte") auf den Papieren ermöglicht Rückschlüsse auf den genutzten Drucker, welcher zur Erstellung beweiserheblicher Dokumente diente. Mit genug krimineller Energie könnten theoretisch Rückschlüsse auf den Ersteller der Dokumente gezogen werden. Dieses könnte zu einer Gefährdung eines zu schützenden Zeugen und dessen Familie führen.

4. Organisatorischen Maßnahmen

Der erste Schritt zu einer datenschutzfreundlich gestalteten und technisch gehärteten Druckinfrastruktur ist die Einbeziehung aller Verantwortlichen:

- Die Führungsebene (**Geschäftsführung, Leitung)** der Organisation ist je nach rechtlicher Norm direkt verantwortlich für potentielle Verstöße gegen den Datenschutz. Ermittlungen richten sich direkt an die Führungsebene. In diesem Fall ist die Sorgfalt bei der Schaffung einer gesicherten Druckinfrastruktur nachzuweisen. Mögliche Bußgeld- und Strafverfahren richten sich im ersten Schritt gegen das Management. Bei finanziellen Schäden, zum Beispiel durch Störungen des Betriebsablaufs in gewerblichen Anwendungen, muss sich die Geschäftsführung bei Nichteinhaltung der Sorgfaltspflicht verantworten. Technische Störungen, aber auch Sabotage der Druckinfrastruktur können Fertigung und Logistik eines Betriebes komplett stoppen.
- Die **Datenschutzbeauftragten** müssen, um ihrem Auftrag gerecht zu werden, auch die Abläufe in der Druck- und Dokumenteninfrastruktur betrachten und bewerten. Im Rahmen der periodischen Überprüfung ist auch die Einhaltung der beschlossenen Regeln zu verifizieren und zu dokumentieren.
- Die **IT-Sicherheitsbeauftragten** müssen Druck- und Dokumenteninfrastruktur in ihr Sicherheitskonzept mit einbeziehen. Ohne diese Maßnahme können weder die Informationssicherheit noch der Datenschutz in den betrieblichen Abläufen gewährleistet werden. Das IT-Sicherheitskonzept muss die Endgeräte und die damit verbundene Software einschließen. Das Risiko von Störungen in geschäftskritischen Druckprozessen muss bewertet und dokumentiert werden.

- Die für die Druck- und Dokumenteninfrastruktur verantwortliche **IT-Administration** benötigt klare Vorgaben zu Handhabung und Konfiguration der Endgeräte und damit verbundener Software. Diese müssen dokumentiert und als standardisierter Ablauf umgesetzt werden. Die Berechtigungen für technische Maßnahmen müssen klar geregelt sein.
- Die Beschaffungsstelle initiiert und überwacht die Beschaffung. Dabei sind die Vorgaben von Datenschutz und Informationssicherheit bei der Beschaffung zu berücksichtigten und auf die jeweiligen Umgebungen mit den IT-Administratoren abzustimmen (Privacy by Design, Privacy by Default).
- Alle **Mitarbeiter** müssen mit den Regeln zu Informationssicherheit und Datenschutz vertraut gemacht werden. Dieses schließt den Umgang mit Papierdokumenten von der Erzeugung bis zur Entsorgung ein. Ein Schwerpunkt ist der Schutz von Informationen nach außen – aber auch die Vertraulichkeit innerhalb der Organisation. Eine periodische Auffrischung ist notwendig, um die Sensibilität aufrechtzuerhalten. Die Information von neuen Mitarbeitern ist zu regeln.

5. Checkliste zum Datenschutz

Funktion	Risiko	Empfehlung
Druck von Dokumenten an zentralen Geräten	Gedruckte Dokumente liegen unbeaufsichtigt im Ausgabefach oder auch neben Druckern und Multifunktionsgeräten. Vertrauliche Informationen können in die Hände unbefugter Akteure gelangen: Sie werden von anderen, nicht autorisierten Mitarbeitern oder auch Betriebsfremden gelesen. Mit Methoden wie Kopie, Scan oder Foto z. B. per Smartphone können die Informationen einfach reproduziert und entwendet werden. Der Druck mit vierstelligem Pin-Code aus dem Druckertreiber ist kein zeitgemäßer Schutz vertraulicher Daten: Das Abholen von Dokumenten erfordert zu viel Interaktion mit dem Endgerät. Dieses führt zur Nutzung nur in Ausnahmefällen. Der begrenzte Zahlenraum bietet einen nur eingeschränkten Schutz gegen das Ausprobieren.	Dokumente werden erst gedruckt, wenn der Empfänger sich am Gerät authentifiziert hat (Pull Printing). Dieses kann per Mitarbeiterausweis, einen RFID-Anhänger, über den Windows Login und andere Methoden geschehen. Steht das Gerät nicht zur Verfügung, kann auf ein anderes, mit Pull Print versehenes System ausgewichen werden; ohne den Druck erneut auszulösen. Die Druckaufträge verbleiben bis zum Abruf auf dem Druckserver oder Rechner des Anwenders.
Druck von Dokumenten auf Arbeitsplatzdruckern	Dokumente im Ausgabefach von arbeitsplatznahen Druckern können von nicht berechtigten Personen eingesehen werden.	Wenn ein Gerät im unmittelbaren Zugriff des druckenden Anwenders steht, kann auf eine Sicherung der Druckausgabe verzichtet werden.

Funktion	Risiko	Empfehlung
Druck auf Geräten, welche auf jeder Seite einen nicht direkt sichtbaren Maschinenidentifikationscode (MIC, „Yellow Dots“, „Tracking Dots“, „Hidden Dots“) aufbringen	Der Machine-Identification-Code (MIC) ist eine undokumentierte Funktion, welche ohne Wissen und Wollen des Eigentümers auf jeder Druckseite in verschlüsselter Weise Identifikationsmerkmale des Farbdruckers, den Druckzeitpunkt sowie ggf. weitere Informationen hinzufügt, wodurch ggf. der einzelne Anwender identifiziert werden kann. Dazu werden winzige gelbe Punkte, die nur mit Mikroskop und UV-Licht sichtbar werden, zusätzlich zum beabsichtigten Druckbild in Punktewolken oder -rastern über den gesamten Druckbereich verteilt Die Eigentümer haben keinen Einfluss darauf, welche Informationen durch den MIC weitergegeben werden und sie können diese auch nicht auswerten. Es ist nicht bekannt, welchen Funktionsumfang der MIC darüber hinaus haben könnte und ob sich dieser möglicherweise durch Firmware-Updates oder auf andere Weise ändern bzw. erweitern lässt. Die MIC-Funktion ist Bestandteil der Firmware und nicht abschaltbar. Auf Nachfrage verwiesen Hersteller auf Regierungen, die diese MIC-Funktion wünschen. Welche Regierungen das sind, wurde nicht mitgeteilt. Im Rahmen der Strafverfolgung scheinen die Informationen des MIC Verwendung zu finden Durch die undokumentierte, intransparente und nicht beeinflussbare Eigenschaft weist der MIC wesentliche Eigenschaften einer Schadsoftware auf.	Da der MIC eine undokumentierte Routine darstellt, von welcher nur bekannt ist, dass sie ohne Wissen und Wollen des Eigentümers Informationen verborgen und verschlüsselt weitergibt, sollte in sicherheitskritischen Bereichen der Einsatz von Geräten mit Maschinenidentifikationscode genau auf seine Risiken geprüft werden und ggf. unterbleiben. Darüber hinaus sollte geprüft werden, ob Arbeitnehmervertretungen und Datenschutzbeauftragte auf den Einsatz von Geräten mit MIC hinzuweisen sind. Es wird empfohlen, die Verwendung von MIC als ein Ausschreibungs- bzw. Ausschlusskriterium zu berücksichtigen sowie – falls MIC verwendet wird – detaillierte und verbindliche Auskünfte zu den konkreten Inhalten und Funktionen von den Anbietern einzuholen.

Funktion	Risiko	Empfehlung
Übertragung der Druckdatei über einen Druckserver	Mit der Druckdatei werden Metadaten zum „Druckjob“ übertragen. Es handelt sich u. a. um den Namen des Druckjobs, die User ID des Anwenders und Datum/Uhrzeit. Der Name der Druckdatei ist abhängig von seiner Quelle. Oft handelt es sich um den ursprünglichen Dokumentennamen. Der Name des Druckjobs kann damit eine vertrauliche Information offenbaren z.B. ‚Herbert Schmidt Abmahnung‘. Die Information ist im Druckserver sichtbar und kann mit zusätzlicher Software protokolliert werden. Besonders problematisch ist die Anzeige aller im Server anstehenden Druckaufträge in jedem einzelnen Rechner der Nutzer eines zentralen Gerätes. Wenn nicht unterbunden, kann ein Anwender sich einen Drucker, z.B. der Geschäftsführung, auf seinem Client installieren und so die Druckaufträge anonym verfolgen.	Die Namen der Druckjobs werden in den Druckerwarteschlangen eines Druckservers im Klartext angezeigt. Wenn das Betriebssystem es erlaubt, sollte auf eine anonymisierte Anzeige umgeschaltet werden. In jedem Fall darf nur Mitarbeitern mit besonderer Verpflichtung zur Verschwiegenheit und Externen nach Instruktion sowie der Unterzeichnung einer Geheimhaltungserklärung der Zugang zu Druckservern gewährt werden. Die Konfiguration innerhalb eines Netzwerks ist so gestalten, dass Nutzer eines zentralen Gerätes in der Druckwarteschlange nur ihre eigenen Druckaufträge sehen können.
Übertragung der Druckdatei zum Drucker oder Multifunktionsgerät	Viele Drucker und Multifunktions-geräte protokollieren in ihrer Standardkonfiguration die Metadaten der Druckaufträge inklusive dem Auftragsnamen. Die Protokolle können auf dem Display des Gerätes oder per Zugriff auf den Webserver mit oder ohne Login gelesen werden. Andere Anwender, der interne IT-Support oder auch externe Techniker können Einblick in vertrauliche Informationen bekommen.	Die Protokollierung von Druckaufträgen im Gerät sollte abgeschaltet sein. Die Namen von Druckaufträgen dürfen nicht sichtbar sein.

Funktion	Risiko	Empfehlung
Faxversand von Faxgeräten und Multifunktionsgeräten per analogem Modem	Nach dem Faxversand wird, wenn so konfiguriert, ein Sendebericht als Nachweis des erfolgreichen Versands bzw. eines Sendefehlers gedruckt. Das Protokoll enthält eventuell ein verkleinertes Abbild der ersten Seite des Faxdokumentes. Der Sendebericht wird zeitverzögert gedruckt und liegt bis zur Abholung oder Entsorgung im Ausgabefach des Endgerätes. Nicht autorisierte Personen können aus dem Protokoll vertrauliche Informationen gewinnen.	Eingehende Faxdokumente, Sendeberichte und Faxprotokolle sollen geschützt werden. Somit sollen Faxgeräte und mit analogen Faxmodems ausgerüstete Multifunktionsgeräte in Räumen betrieben werden, welche unberechtigten Mitarbeitern und Betriebsfremden keinen Zutritt ermöglichen. Eine technische Alternative ist der Ersatz von Faxgeräten und Multifunktionsgeräten mit analogem Modem durch den digitalen Versand von Dokumenten per Faxserver und alternativem Scan an den Faxserver direkt von Multifunktionsgeräten. Für den Faxversand soll sich der Mitarbeiter mit dem für den „sicheren Druck“ verwendeten Verfahren authentifizieren. Damit werden Sendeberichte an die Mailadresse des Mitarbeiters oder ein Gruppenpostfach gesendet. Die Protokollierung geschieht, soweit gewünscht, im gesicherten Faxserver.
Faxempfang von Faxgeräten und Multifunktionsgeräten per analogem Modem	Per Fax empfangene Dokumente werden in der Regel sofort ausgedruckt und liegen bis zur Abholung in der Papierausgabe des Endgerätes. Information können von unberechtigten Personen gelesen und reproduziert werden.	
Faxversand und -empfang von Faxgeräten und Multifunktionsgeräten per analogem Modem	Viele Fax- und Multifunktionsgeräte mit analogem Modem protokollieren den Faxverkehr und speichern die Metadaten im Gerät. Per Ausdruck oder Zugriff über die Netzwerkschnittstelle lassen sich sensible Informationen wie Faxnummern, Datum, Uhrzeiten und Seitenzahlen auslesen.	
Versand von Faxdokumenten an den falschen Empfänger	Der Versand von personenbezogenen Daten an die falsche Faxadresse ist eine der häufigsten Ursachen von unbeabsichtigten Datenschutzverstößen. Dieses betrifft insbesondere Organisationen mit hoher Nutzung von Faxgeräten wie Kliniken, Arztpraxen, Labore und Anwaltskanzleien. Ursache ist in der Regel mangelnde Aufmerksamkeit bei der Auswahl der Kurzwahltasten oder der korrekten Faxnummer.	Das mit der Nutzung von Faxgeräten beauftragte Personal muss über die datenschutzrechtlichen Konsequenzen von Unaufmerksamkeit informiert werden. Die Nutzung von geschlossenen Informationssystemen z.B. für den medizinischen Bereich ist dem öffentlichen Faxverkehr vorzuziehen.

Funktion	Risiko	Empfehlung
Scan (allgemein)	Multifunktionsgeräte werden (oftmals) im Rahmen der Digitalisierung zum ersetzenden Scannen verwendet – ohne dass das eingesetzte Kompressionsverfahren geprüft worden ist. Verlustbehaftete Kompressionsverfahren können die Information verändern z.B. ‚Zahlendreher' bei kleiner Schriftgröße.	Schon bei der Anschaffung sollte explizit darauf geachtet werden, dass keine Systeme beschafft werden, die einen verlustbehafteten Kompressionsstandard (insbesondere JBIG2) einsetzen. Sollte dies jedoch bereits erfolgt sein, so sind geeignete Kompressionsstandards festzulegen und umzusetzen.
Scan an Email	Multifunktionsgeräte bieten die Funktion Scan an E-Mail. Papierdokumente können ohne vorsorgliche Maßnahmen auch an externe Empfänger gesendet werden. Die freie Eingabe oder Wahl der Absenderadresse ermöglicht E-Mail-Spoofing. Eine festgelegte Maschinenadresse als Absender ermöglicht den anonymen Versand von Dokumenten.	Für den Mailversand soll sich der Mitarbeiter mit dem für den sicheren Druck verwendeten Verfahren authentifizieren. Damit wird die E-Mail-Adresse des Anwenders fest in das VON: Feld eingetragen. Die Empfängeradresse wird per LDAP aus dem Active-Directory gewählt. Die freie Adresseingabe ist unterbunden. Alternativ oder in Kombination kann der Versand an sich selbst als Funktion zur Verfügung gestellt werden. <VON:> und <AN:> sind fest mit der E-Mail-Adresse des authentifizierten Mitarbeiters vorbelegt.
SMTP Gateway	SMTP (Simple Mail Transfer Protocol) wird in der Regel zum E-Mail Versand von Multifunktionsgeräten an einen Mailserver genutzt. Ist der SMTP Gateway nicht geschützt, können E-Mails auch von anderen Quellen gesendet werden. Risiken sind z.B. Spam-Mails und Identity Spoofing.	Der SMTP Gateway ist durch geeignete Maßnahmen gegen den Empfang von nicht autorisierten Systemen zu schützen. Alternativ oder zusätzlich können im Mailserver Regeln hinterlegt werden, um unerlaubten E-Mail-Verkehr zu unterbinden.
Scan an Ordner	Am Multifunktionsgerät werden Scanpfade definiert, mit welchen direkt z.B. auf Ordner gescannt werden kann. Ein Datenschutzproblem tritt auf, wenn vertrauliche Dokumente durch einen Anwenderfehler auf einen falschen Ordner gescannt werden, für den der Mitarbeiter möglicherweise weder Zugangsberechtigung noch Korrekturmöglichkeit besitzt.	Das Risiko kann durch Scanpfade entsprechend den Nutzerrechten reduziert werden. Eine Alternative ist der Scan an den „Homefolder" (Basisordner) des Mitarbeiters und nachträgliches Verschieben der Scandatei am Rechner. Der Pfad zum „Homefolder" wird nach Authentifizierung des Anwenders am Multifunktionsgerät angeboten.

Funktion	Risiko	Empfehlung
Scan vom Multifunktionsgerät über das Netzwerk z.B. über die Webschnittstelle des Gerätes oder Scansoftware	Originaldokumente werden häufig von Anwendern auf dem Vorlagenglas vergessen. Durch einen über das Netzwerk ausgeführten Scanvorgang lassen sich Dokumente anonym scannen oder kopieren.	Der Scan über die Webschnittstelle des Endgerätes soll unterbunden werden. Die Sicherheit des Scans über das Netz per Software auf Clients ist vor ihrem Einsatz zu untersuchen.
Entsorgung von gedruckten Dokumenten	Gedruckte Dokumente werden häufig in einfachen Abfallbehältern oder Sammelboxen neben Druckern, Multifunktions- und Faxgeräten entsorgt. Damit sind vertrauliche Informationen gefährdet, da diese (wenn auch unwillentlich) der Öffentlichkeit ausgesetzt werden. Die finale Entsorgung geschieht oft über betriebsfremde Dienstleister. Der Datenschutz außerhalb der Organisation ist nicht gewährleistet. Angreifer von außen können über entsorgtes Papier zu wertvollen Informationen über die betriebliche Organisation (z.B. für Social Engineering) und Behörden- bzw. Firmendaten kommen.	Die Entsorgung von gedruckten Dokumenten muss entsprechend einer vorgegebenen und angemessenen (Datenschutz-)Richtlinie geschehen. Ggf. sind Aktenvernichter einer geeigneten Schutzklasse neben den Geräten bereit zu stellen. Die notwendigen Entsorgungseinrichtungen, insbesondere Papiercontainer, sind entsprechend den Erfordernissen der Mitarbeiter zu positionieren. Per Arbeits-/Dienstanweisung ist auf die Notwendigkeit der sicherheits- und datenschutzkonformen Entsorgung hinzuweisen. Die Arbeits-/Dienstanweisung ist schriftlich durch die unterwiesenen Mitarbeiter zu bestätigen und der Vorgang ist der durchführenden Stelle zu dokumentieren.
Entsorgung in häuslichen, mobilen und Telearbeitsplätzen	Wie die in Arbeitsplätzen gedruckten Dokumente entsorgt werden (z.B. in öffentlichen Recyclingcontainern oder im Restmüll), entzieht sich dem direkten Einfluss des Arbeitgebers.	In der betrieblichen Vereinbarung zu häuslichen, mobilen- und Telearbeitsplätzen ist die Entsorgung zu regeln und seitens des Unterwiesenen schriftlich zu bestätigen. Arbeitsplätze außerhalb der Betriebsstätte werden mit einem Aktenvernichter mit geeigneter Schutzklasse ausgerüstet. Besonders vertrauliche Dokumente sind in der Organisation (Unternehmen bzw. Behörde) gem. der (Datenschutz-) Richtlinien zu entsorgen. Alternativ kann der Druck und damit die Entsorgung von Dokumenten untersagt werden.

Funktion	Risiko	Empfehlung
Multifunktionsgeräte mit Anschlussmöglichkeit für USB Sticks, SD Karten und andere mobile Datenträger	Neben dem direkten Druck von Dokumenten und Fotos vom Speichergerät, kann auf den Datenträger gescannt werden. Vertrauliche Informationen können als digitale Kopie entwendet werden.	Anschlüsse für USB Sticks, SD Karten etc. werden per Gerätekonfiguration gesperrt. In Bereichen, in welchen die Funktion Drucken oder Scannen auf USB freigeschaltet ist, sind die Geräte als Standalone-Geräte zu betreiben oder eine strikte Netztrennung durchzuführen.
Viele Multifunktionsgeräte und Drucker enthalten eine Festplatte oder SSD auf denen Druck-, Scan-, Kopier- und andere Nutzdaten gespeichert werden.	Die auf Datenträgern gespeicherten Informationen können ausgelesen und rekonstruiert werden. Diebstahl, Reparatur, Rückgabe oder Verkauf der Geräte nach Ende der Betriebszeit sind mögliche Szenarien für Datenschutzprobleme.	Geräte sind grundsätzlich mit verschlüsselten Festplatten auszurüsten. Ein sicherer Mindeststandard bei der Verschlüsselung ist vorzugeben. Alternativ können Nutzdaten verschlüsselt abgelegt werden. Daten dürfen nur temporär für die aktuell anliegenden Jobs abgelegt werden. Eine Speicherung von Daten z.B. auf geräteinternen Dokumentenservern ist zu unterbinden. Nach Löschung der Nutzdaten z.B. Druckdateien sind die freigegebenen Datensegmente sofort und automatisch mit Zufallswerten zu überschreiben. Bei Entnahme der Festplatte z.B. bei Reparatur, der Rückgabe oder Entsorgung des Gerätes ist die Löschung der Festplatten entsprechend vereinbarter Löschregularien für Festplatten aus betrieblich genutzten PCs und Servern zu handhaben. Der Datenschutz für SSDs ist mit äquivalenten Methoden zu realisieren. Der zu vereinbarende Datenlöschungsprozess ist schriftlich zu dokumentieren und von den einzelnen Parteien schriftlich zu bestätigen. Kann ein Lieferant die sichere unwiederbringliche Löschung der Daten auf ausgemusterten/defekten Festplatten nicht sicherstellen, sollte eine - nach DIN 66399 - nachzuweisende zertifizierte Vernichtung der Festplatten vorgeschrieben werden (Schutzklasse 2, Sicherheitsstufe H5), alternativ die Übergabe der betreffenden Festplatten.

Funktion	Risiko	Empfehlung
Multifunktionsgeräte bieten zum Teil interne Dokumentenserver als Komfortfunktion.	Gespeicherte Dokumente können über das Netz ausgelesen werden. Diebstahl, Reparatur oder Verkauf und Rückgabe der Geräte nach Ende der Betriebszeit können zu Datenschutzproblemen führen.	Dokumentenserver und vergleichbare Funktionen sollen nicht verfügbar oder deaktiviert sein.
Auswertung der von Mitarbeitern individuell gedruckten und kopierten Seiten	Mit der Authentifizierung zur Freischaltung von Funktionen, insbesondere dem sicheren Druck, wird die User ID des Anwenders erfasst. Damit lassen sich die Druck- und Kopiervolumina per Anwender sammeln und verwerten.	Die Sammlung von Daten zur Gerätenutzung ist abzuschalten. Sollen zur innerbetrieblichen Abrechnung Nutzungsdaten ermittelt werden, sind die Volumina der Druck- und Kopieraufträge des Mitarbeiters unmittelbar auf dessen Abteilungsnummer zu buchen und die individuelle Information zu löschen.
Datentransfer über das Netz	„Von“ und „zu“ Druckern und Multifunktionsgeräten gesendete Daten können im Netzwerk abgehört werden.	Wenn die Netzwerkstrecken als angreifbar eingestuft werden und keine Maßnahmen auf Netzwerkebene möglich sind, sollen Druck-, Scan- und Maildaten während des Transfers verschlüsselt werden. Alternativ kann die Strecke verschlüsselt werden.
Remote Konsole	Per Remote Konsole kann das User-Interface von Druckern und Multifunktionsgeräten über das Netz betrachtet werden. Die Funktion ist ein Werkzeug insbesondere für den IT-Support, um Anwender zu unterstützen. Mit der Remote Konsole können auch vertrauliche Eingaben des Anwenders durch den IT-Support gesehen werden.	Wenn sich ein Mitarbeiter über die Remote Konsole auf das Display eines Endgerätes schaltet, muss dieses für den am Multifunktionsgerät oder Drucker stehenden Anwender deutlich erkennbar sein. Wenn verfügbar, soll der Anwender am Gerät seine Zustimmung geben, bevor ein Aufschalten über das Netzwerk möglich wird. Passworte z.B. der „Windows-Login“ dürfen unter keinen Umständen sichtbar sein.

6. Checkliste zur Informationssicherheit

Funktion	Risiko	Empfehlung
Gerätekonfiguration	Drucker und Multifunktionsgeräte werden von Herstellern mit Werkseinstellungen ausgeliefert. Generelle und kundenspezifische Sicherheitsanforderungen müssen konfiguriert werden. Das Aufstellen von Geräten ohne Konfiguration der sicherheitsrelevanten Parameter resultiert in Sicherheitsrisiken.	Die Sicherheitsanforderungen werden in einer klar definierten Gerätekonfiguration umgesetzt. Diese wird bei Erstinstallation, nach Rücksetzen auf Werkseinstellungen und nach Gerätereparaturen angewendet. Die Konfiguration der Geräte kann per Arbeitsanweisung über den Webserver des einzelnen Gerätes manuell erfolgen. Eine automatisierte Konfiguration über eine Gerätemanagement-Software ist zu bevorzugen, da Fehler vermieden und Arbeitszeit gespart werden kann. Es muss sichergestellt sein, dass die Gerätekonfiguration aller Geräte, unabhängig von den administrierenden Personen, identisch ist. Die Standardkonfiguration ist zu dokumentieren.
Gerätepasswort	Mit Zugang zu den Administrationsmenüs der Endgeräte lassen sich sicherheitsrelevante Veränderungen der Konfiguration vornehmen. Daraus ergeben sich mögliche Risiken beim Datenschutz und der Informationssicherheit. Über Jahre verwendete Gerätepassworte oder vom Hersteller voreingestellte Standardpassworte bieten einen nur schwachen Schutzmechanismus.	Alle Geräte werden mit einem Gerätepasswort geschützt und können ohne dessen Kenntnis nicht verändert werden. Das Ausgangspasswort muss geändert werden. Das Gerätepasswort soll den Regeln für starke Kennworte entsprechen und periodisch (z.B. jährlich) erneuert werden.
Netzwerkprotokolle	Endgeräte werden in der Regel mit offenen Netzwerk-Ports ausgeliefert. Systeme können darüber angegriffen werden.	Alle nicht verwendeten Ports sollen deaktiviert werden.
SNMP Community Name	Per „SNMP Get“ Befehl können Informationen und Einstellungen aus der geräteinternen Management Information Base (MIB) gelesen werden. Über „SNMP Set“ können Einstellungen verändert werden.	Der “SNMP Set Community Name“ (Passwort)“ soll geändert werden, um nicht autorisierte Änderungen über das Netz zu verhindern. Der „SNMP Get Community Name“ kann geändert werden.

Funktion	Risiko	Empfehlung
PJL Passwort	Geräteeinstellungen können über Printer Job Language (PJL) Befehle verändert werden. Zusätzlich kann, abhängig vom Gerätehersteller, auf das geräteinterne Dateisystem zugegriffen werden.	Das „Printer Job Language Protokoll“ soll mit einem Passwort versehen werden.
Andere zur Gerätekonfiguration verwendbare Protokolle	Von Herstellern und Endgeräten werden spezifische Protokolle zu Konfiguration von Geräten angeboten, zum Beispiel Download von Konfigurationsdateien oder Webservices.	Nicht benötigte Protokolle sind zu deaktivieren. Sofern IPv6 im Netzwerk nicht eingesetzt wird, ist dieses ebenfalls zu deaktivieren.
Firmware und Softwareänderungen in den Geräten	Das Unterlassen von Firmware-Upgrades und nicht vom Hersteller zertifizierten Softwareerweiterungen können die Sicherheit der Endgeräte möglicherweise herabsetzen.	Geräte sollen abgesichert sein gegen das Einspielen von nicht vom Hersteller herausgegebener Firmware und gegen nicht durch den Hersteller zertifizierte Zusatzsoftware. Sicherheitslücken sind durch proaktive und unverzügliche Bereitstellung insbesondere sicherheitsrelevanter Firmware-/Software-Updates und -Upgrades durch den Hersteller zu schließen. Dieses soll mit dem Lieferanten schriftlich vereinbart sein. Der Prozess für Firmware-Upgrades innerhalb der Organisation soll dokumentiert sein.
Einbindung in das Netz	Drucker und Multifunktionsgeräte sind Server. Damit sind sie analog zu anderen IT-Systemen angreifbar.	Drucker und Multifunktionsgeräte sollen gehärtet werden. Herstellerempfehlungen zum Schutz vor Malware, Viren etc. sind einzuhalten. Nicht genutzte Netzwerkprotokolle sollen abgeschaltet werden.
Anbindung an das öffentliche Internet	Über das Internet oder halböffentliche Intranets verfügbare Drucker und Multifunktionsgeräte sind besonders gefährdet. Die Szenarien reichen vom Hacking bis unautorisiertem Druck.	Drucker und Multifunktionsgeräte sollen nicht über das öffentliche Internet erreichbar sein. Der Zugriff auf Geräte und deren Funktionalitäten in Intranets soll durch geeignete Maßnahmen reglementiert werden. Wo möglich, sind eigene Netzsegmente für Druckerinfrastrukturen zu bilden.

Funktion	Risiko	Empfehlung
Software zur zentralen Geräteverwaltung und Überwachung	Eine zentrale Software zur Geräteadministration und Überwachung spart Arbeitszeit, birgt aber auch ein Risiko, da über die Konfiguration einzelner Geräte bis zur gesamten Flotte Schaden verursacht werden kann.	Die Zugriffsberechtigung auf Software zur Geräteverwaltung soll den Regeln anderer IT-Komponenten entsprechen. Den mit dem Support von Druckern und Multifunktionsgeräten betrauten Personen sollen eingeschränkte Berechtigungen entsprechend ihrer Tätigkeit gegeben werden. Die Struktur der Zugriffsberechtigung sollte schriftlich dokumentiert werden.
Software zur Kommunikation von Gerätedaten an Lieferanten	Gerätedaten zur Versorgung mit Verbrauchsmaterial, Wartungseinsätzen, Seitenzahlen etc. können per Software innerhalb der Firewall automatisiert erfasst und an Lieferanten außerhalb der Firewall versendet werden.	Die Methodik der Datensammlung und des Datentransfers soll vom Anbieter der Lösung schriftlich dargestellt und bestätigt werden, um eine sicherheitstechnische Beurteilung zu ermöglichen. Dieses sollte bereits mit der Antwort auf die Ausschreibung/Beschaffung von Geräten des Herstellers vorliegen.
Überwachung der Sicherheitseinstellungen	Die Sicherheit von Geräten wird durch Reparaturen, Rückstellung auf Werkseinstellungen und bewusste oder unbedachte Eingriffe gefährdet.	Die Sicherheitseinstellungen der Geräte sind zu erhalten. Abweichungen sind zu korrigieren. Dieses kann durch periodisches Aufspielen von Gerätekonfigurationen auf alle Geräte geschehen. Eine Alternative ist der Einsatz von Software zur kontinuierlichen Überwachung und automatischen Korrektur der Sicherheitseinstellungen.
Wartungsarbeiten an den Geräten durch Techniker	Techniker schließen mobile IT-Systeme zu Wartungszwecken an die Geräte an und gefährden so die Sicherheit.	Zu Wartungszwecken dürfen mobile IT-Systeme nur unter der Voraussetzung angeschlossen werden, dass das Betriebssystem mit den aktuellsten Sicherheitsupdates, aktueller Antiviren-Software oder einer entsprechend gesicherten Konfiguration betrieben wird.