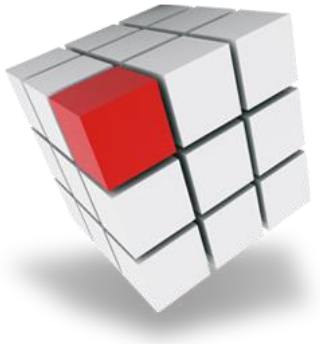
Whitepaper

Datenschutz und IT Sicherheit in Druckinfrastrukturen

mc² management consulting GmbH
Ludwig-Rinn-Str. 14 - 16
D-35452 Heuchelheim
Telefon: +49 641 966 2360
E-Mail: info@mc-2.de



Inhaltsverzeichnis

1. Einleitung

Drucker, Multifunktionsgeräte, Scanner, Faxgeräte und die dazu gehörigen Softwarekomponenten sind ein Teil der betrieblichen Informationsverarbeitung. Der Fokus von Datenschutz und IT Sicherheit liegt meist auf digitalen Daten und der IT-Infrastruktur. Die Vertraulichkeit und rechtliche Bewertung einer Information ist aber unabhängig von ihrem Träger. Papierdokumente mit Informationen müssen äquivalent ihren digitalen Gegenstücken behandelt und geschützt werden. Die Mehrzahl aller Organisationen verwendet Ausdrucke und Scans für Verwaltungsvorgänge und geschäftliche Prozesse. Damit hat die Verfügbarkeit und Integrität der Dokumenteninfrastruktur eine hohe Priorität. Geräte und Softwarekomponenten sind durch Härtung gegen bekannte Angriffs- und Störungsszenarien zu schützen.

Verstöße gegen den Datenschutz und die IT Sicherheit werden unabhängig von der Quelle des Problems geahndet. Deshalb unterliegen Drucker, Scanner, Fax- und Multifunktionsgeräte der gleichen Sorgfaltspflicht wie alle anderen Elemente der IT-Infrastruktur. Abhängig vom Vorfall und den dadurch berührten relevanten Gesetzen sowie Verordnungen, können signifikante Geld- und Freiheitsstrafen verhängt werden. Datenschutz und IT Sicherheit sind auch für die Druckinfrastruktur zu gewährleisten.

Dieses Whitepaper ist ein kondensierter Leitfaden zur Erarbeitung von Datenschutz und IT Sicherheit. Der gesamte Lifecycle von der Installation über den Betrieb bis zur Entsorgung der Endgeräte ist zu betrachten. Abhängig von betrieblicher Organisation, spezifischen Obliegenheiten und vorhandener IT-Infrastruktur ergeben sich zusätzliche Anforderungen. Ein Sicherheitskonzept ist zu erstellen. Damit werden Lücken vermieden und im Schadensfall kann die erforderliche Sorgfalt nachgewiesen werden.

Die Anpassung der Sicherheit an die Erfordernisse der Gesetzeslage soll ganzheitlich unter Einbeziehung aller relevanten Beteiligten in der Organisation erfolgen. Dazu gehören unter anderem Geschäftsführungen, Datenschutzbeauftragte, IT-Sicherheitsbeauftragte, IT-Management sowie Mitarbeitervertretungen. Die schriftlich abgefasste Sicherheitsrichtlinie vereint die Mindestanforderungen und spezifische Anforderungen der Organisation.

Zum Erhalt von Datenschutz und IT-Sicherheit ist die erarbeitete Sicherheitsrichtlinie zu überprüfen und gegebenenfalls an sich ändernde Anforderungen (Stichwort: Rechtslage, neue Bedrohungsszenarien) anzupassen. Der Status der Sicherheit der Druckinfrastruktur muss periodisch überprüft werden.

Die technischen Maßnahmen sind durch Aufklärung und Verpflichtung der Mitarbeiter zu begleiten. Neue Mitarbeiter sind ebenso zu unterweisen wie langjährig Beschäftigte.

Die folgende Checkliste zu Datenschutz und IT-Sicherheit gibt einen weitgehenden aber nicht notwendigerweise vollständigen Überblick der Risiken und Lösungsansätze.

2. Checkliste zum Datenschutz

Funktion	Risiko	Empfehlung
Mitarbeiter	Das Risiko von vertraulichen Informationen auf dem Papier wird von vielen Mitarbeitern nicht wahrgenommen. Die Folge ist eine erhebliche Gefährdung des betrieblichen Datenschutzes.	Die Mitarbeiter der Organisation sind über die Sicherung von gedruckten Informationen auf Papier aufzuklären. Grundregeln sollen an alle, auch langjährige Mitarbeiter kommuniziert werden. Neue Mitarbeiter sind zu informieren. Eine periodische Auffrischung zum Thema Datenschutz ist empfehlenswert. Die Durchführung der Unterweisung sollte schriftlich dokumentiert und von den Unterwiesenen gegengezeichnet werden.
Druck von Dokumenten an zentralen Geräten	Gedruckte Dokumente liegen unbeaufsichtigt im Ausgabefach oder auch neben Druckern und Multifunktionsgeräten. Vertrauliche Informationen können in die Hände irregulärer 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.	Dokumente werden erst gedruckt, wenn der Empfänger sich am Gerät authentifiziert hat. Dieses kann über einen vorhanden Mitarbeiterausweis, über den Windows Login und andere Methoden geschehen.
Druck von Dokumenten auf Arbeitsplatzdruckern	Dokumente im Ausgabefach von arbeitsplatznahen Druckern können von nicht berechtigten Personen eingesehen werden.	Wenn ein Gerät im Sichtkontakt des druckenden Anwenders steht, kann auf eine Sicherung der Druckausgabe verzichtet werden.
Übertragung der Druckdatei über einen Druckserver	Mit der Druckdatei werden Metadaten zum „Druckjob“ übertragen. Es handelt sich u. a. um den Namen des Druckauftrages, 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. Dieser Name selbst kann damit eine vertrauliche Information offenbaren. Die Information ist im Druckserver sichtbar und kann mit zusätzlicher Software protokolliert werden.	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.

Funktion	Risiko	Empfehlung
Übertragung der Druckdatei zum Drucker oder Multifunktionsgerät	Viele Drucker und Multifunktionsgeräte protokollieren in ihrer Standardkonfiguration die Metadaten der Druckaufträge inklusive dem Jobnamen. 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.	Jegliche Protokollierung von Druckaufträgen im Gerät muss abgeschaltet sein.
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.	

Funktion	Risiko	Empfehlung
Scan an Email	Multifunktionsgeräte bieten die Funktion Scan an Email. Papierdokumente können ohne vorsorgliche Maßnahmen auch an externe Empfänger gesendet werden.	Für den Mailversand soll sich der Mitarbeiter mit dem für den sicheren Druck verwendeten Verfahren authentifizieren. Damit wird die Email Adresse des Anwenders fest in das VON: Feld eingetragen. Die Empfängeradresse wird per LDAP aus der 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 Emailadresse des authentifizierten Mitarbeiters vorbelegt.
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, zu dem der Mitarbeiter möglicherweise weder eine Zugangsberechtigung noch Korrekturmöglichkeit besitzt.	Das Risiko kann durch Scanpfade entsprechend den Nutzerrechten reduziert werden. Eine Alternative ist der Scan an den „Homefolder“ des Mitarbeiters und nachträgliches Verschieben der Scandatei am Rechner. Der Pfad zum „Homefolder“ wird nach Authentifizierung des Anwenders am Multifunktionsgerät angeboten.
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.	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 die betriebliche Organisation (Social-Engineering) und Behörden- bzw. Firmendaten kommen.	Die Entsorgung von gedruckten Dokumenten muss entsprechend vorgegebener Datenschutzrichtlinien geschehen. 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.

Funktion	Risiko	Empfehlung
Aktenvernichtung in Heimarbeitsplätzen	Die in Heimarbeitsplätzen gedruckten und in öffentlichen Recyclingcontainern oder im Restmüll entsorgten Dokumente können von nicht befugten Personen eingesehen werden.	Heimarbeitsplätze werden mit einem adäquaten Aktenvernichter ausgerüstet. Besonders vertrauliche Dokumente sind in der Organisation (Unternehmen bzw. Behörde) nach Datenschutzrichtlinien zu entsorgen. In der betrieblichen Vereinbarung zu Heimarbeitsplätzen ist dieses zu regeln und seitens des Unterwiesenen schriftlich zu bestätigen.
Multifunktionsgeräte mit Anschlussmöglichkeit für USB Sticks, SD Karten und anderen mobilen Datenträgern	Neben dem direkten Druck von Dokumenten und Fotos vom Speichergerät, kann auf den Datenträger gescannt werden. Vertrauliche Informationen können per digitaler Kopie entwendet werden.	Anschlüsse für USB Sticks, SD Karten etc. werden per Gerätekonfiguration gesperrt.
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. Alternativ können Nutzdaten verschlüsselt abgelegt werden. Daten dürfen nur temporär für die aktuell anliegenden Aufträge abgelegt werden. 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 beteiligten Parteien schriftlich zu bestätigen.
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 sein.

Funktion	Risiko	Empfehlung
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 Akkumulation 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.
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, soll dieses für den am Multifunktionsgerät oder Drucker stehenden Anwender erkennbar sein. Passworte z.B. der „Windows-Login“ dürfen unter keinen Umständen sichtbar sein.

3. Checkliste zur IT-Sicherheit

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 Geräte-management-Software ist zu bevorzugen, da Fehler vermieden und Arbeitszeit gespart werden kann.
Gerätepasswort	Mit Zugang zu den Administrationsmenüs der Endgeräte lassen sich sicherheitsrelevante Veränderungen der Konfiguration vornehmen. Daraus ergeben sich mögliche Risiken beim Datenschutz und der IT-Sicherheit. 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 Geräte-passwort soll den Regeln für starke Kennworte entsprechen und periodisch (z.B. jährlich) erneuert werden.
Kommunikation mit dem geräteinternen Webserver	Die administrative Kommunikation zum Gerät kann abgehört werden.	Für die Kommunikation mit dem integrierten Webserver soll https: erzwungen werden. Die notwendigen Zertifikate werden auf den Geräten hinterlegt.
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.
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 geschützt werden

Funktion	Risiko	Empfehlung
Firmware und Softwareänderungen in den Geräten	Mit Firmwareupgrades als auch nicht vom Hersteller zertifizierten Softwareerweiterungen wird die Sicherheit der Endgeräte möglicherweise herabgesetzt.	Geräte sollen abgesichert sein gegen das Einspielen von nicht vom Hersteller herausgegebener Firmware und gegen nicht vom Hersteller zertifizierter Zusatzsoftware. Für Firmwareupgrades und das Installieren von zusätzlichen Softwarekomponenten soll eine Regelung mit Genehmigungsprozess erstellt werden. Dieser Prozess muss schriftlich dokumentiert werden.
Einbindung in das Netz	Drucker und Multifunktionsgeräte sind Server im Netz. Damit sind sie analog anderer IT-Systemen angreifbar	Drucker und Multifunktionsgeräte sollen gehärtet werden: • Herstellerempfehlungen zum Schutz vor Malware, Viren etc. sind einzuhalten • Nicht genutzte Netzwerkprotokolle sollen abgeschaltet werden
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.
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 gering kontrollierten Intranets soll durch geeignete Maßnahmen reglementiert werden.
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.

Funktion	Risiko	Empfehlung
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.
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. Diese Methodik ist zu bevorzugen.