dsb
datenschutzbeauftragte
des kantons zürich

Merkblatt

Drucker, Kopierer und Multifunktionsgeräte

1 Einleitung

Dieses Merkblatt richtet sich an öffentliche Organe, die Drucker, Kopierer und/oder Multifunktionsgeräte einsetzen.

Auf Druckern, Kopierern und Multifunktionsgeräten werden alle Arten von Informationen verarbeitet, auch Personendaten und besondere Personendaten wie Arbeitszeugnisse, Personaldokumente, Verfügungen oder Verträge. Diese Daten werden einerseits an die Geräte übertragen und können somit potenziell abgefangen werden, andererseits werden sie von vielen Geräten zwischengespeichert und können somit ausgelesen oder auf ein weiteres Medium übertragen werden.

Öffentliche Organe müssen gemäss § 7 IDG Informationen durch angemessene organisatorische und technische Massnahmen schützen. Sie müssen dafür sorgen, dass Informationen nicht unrechtmässig zur Kenntnis gelangen.

Das Merkblatt zeigt organisatorische und technische Massnahmen auf, mit denen die Datenschutzrisiken vermindert oder ausgeschlossen werden können.

Datenschutzbeauftragte des Kantons Zürich
Postfach, 8090 Zürich, +41 43 259 39 99
datenschutz@dsb.zh.ch, datenschutz.ch, twitter: @dsb_zh

2 Risiken

Im Folgenden wird aufgezeigt, welche Risiken beim Einsatz von Druckern, Kopierern oder Multifunktionsgeräten entstehen können und was die entsprechenden Ursachen sind.

Risiko	Beschreibung / Ursachen
Dokumente können durch Unbefugte mitgenommen werden Daten können ausgelesen werden Gerätespeicher oder Gerät kann mitgenommen werden	Gerät ist in öffentlich zugänglichen Räumen platziert Gerät bzw. Gerätespeicher ist nicht vor logischem und physischem Zugriff gesichert Versehentliches Drucken bei Arbeiten ausser Haus
(Personen-) Daten können geschützte Umgebung verlassen	Ausbau bzw. Löschung Gerätespeicher ist nicht geregelt Austauschprozess Gerät ist nicht geregelt Zugriffsmöglichkeiten für Fernwartung sind nicht ausreichend definiert Versand von Output nach extern ist möglich
Daten können abgefangen werden	Unverschlüsselter Datenverkehr von Benutzerin oder Benutzer zum Gerät
Daten können ausgelesen werden	Daten sind unverschlüsselt gespeichert Zugriff auf Gerät ist nicht gesichert Daten werden unnötig lange gespeichert Fehlendes Datenmanagement
Druckaufträge können von Unbefugten ausgeführt bzw. ausgedruckte Dokumente mitgenommen werden	Ausdruck erfolgt ohne Authentifizierung
Gerät kann als Einfallstor für Cyberangriffe dienen	Gerät hat direkte Verbindung zum Internet und ist nicht vom internen Netzwerk abgetrennt Gerät ist über öffentliches WLAN zugänglich
Drucker, Kopierer oder Multifunktionsgeräte stehen nicht zur Verfügung (Ausfall, fehlen-der Ersatz)	Wartungs- oder Lieferantenverträge sind unzureichend Ungenügende Dokumentation für Wiederherstellung Keine Reserven für Geräte und Verbrauchsmaterial

3 Checkliste: Organisatorische und technische Massnahmen

Der Datenschutz bei der Arbeit mit Druckern, Kopierern und Multifunktionsgeräten kann durch verschiedene organisatorische und technische Massnahmen sichergestellt werden. Die organisatorischen Massnahmen können durch den Kunden respektive die Benutzerinnen und Benutzer der Geräte sichergestellt werden. Die technischen Massnahmen sind in der Regel durch den Lieferanten umzusetzen.

3.1 Organisatorische Massnahmen

Beschaffung von Geräten

- Vor der Beschaffung von Geräten ist festzulegen, für welche Einsatzzwecke und durch welche Personen die Geräte hauptsächlich benutzt werden sollen. Sollen beispielsweise viele vertrauliche Dokumente gedruckt oder kopiert werden und dies hauptsächlich durch eine Person, so ist ein lokaler Drucker vorteilhaft.
- Der Einsatz von Netzwerkgeräten ist analog der Anbindung von Clients zu planen. Dazu gehören Festlegungen über die Konfiguration, Berechtigungen usw. (siehe Ziffer 3.2).

Platzierung von Geräten

- Drucker sind so aufzustellen, dass nur Berechtigte Zugang haben. Zu vermeiden sind Standorte, wo sich Externe unbegleitet aufhalten können.
- Falls Geräte in öffentlich zugänglichen Räumen aufgestellt werden müssen (beispielsweise in Schulen oder Schalterräumen), ist darauf zu achten, dass die Geräte als Ganzes gegen Diebstahl gesichert sind und der Datenspeicher des Gerätes nicht mit einfachen Mitteln ausgebaut werden kann (beispielsweise durch ein Schloss an der Wartungsöffnung gesichert). Zusätzlich sind entsprechende Geräteeinstellungen vorzunehmen (keine permanente Speicherung von Daten, Ausdruck nur nach Login, siehe Ziffer 3.2).
- Anstelle eines offenen Papierkorbs ist in der Nähe von gemeinsam genutzten Multifunktionsgeräten ein Schredder oder eine Reisswolf-Box zu platzieren, so dass Fehldrucke oder liegen gelassene Dokumente vernichtet werden können.

Schulung

- Die Benutzerinnen und Benutzer von Druckern, Kopierern und Multifunktionsgeräten sind für die datenschutzrechtlichen Risiken zu sensibilisieren und für den Umgang mit diesen Geräten zu schulen.
- Den Mitarbeitenden sind Richtlinien, Anleitungen und ähnliches zum Umgang mit Druckern, Kopierern und Multifunktionsgeräten abzugeben.

Wartung / Austausch

- Die Wartung und der allfällige Austausch müssen so geregelt sein, dass vor Abtransport eines Geräts alle Daten unwiederbringlich gelöscht werden oder der Gerätespeicher ausgebaut wird. Für den letzteren Fall ist zu regeln, was mit dem Speicher geschieht.
- Es ist eine Ansprechperson für die Liefer-/Wartungsfirma zu definieren, welche die ordnungsgemässe Abwicklung von Lieferung, Inbetriebnahme, Instruktion, Wartung und Austausch sicherstellt.
- Bei Lieferung ist ein Geräteabnahmeprotokoll zu verlangen und durchzuarbeiten, um sicherzustellen, dass sicherheitsrelevante Einstellungen nach Vorgabe konfiguriert sind.

Berechtigungen

- Es ist zu definieren, ob gewisse Funktionen der Geräte auf ausgewählte Benutzerinnen und Benutzer eingeschränkt werden müssen, vor allem Administrationsfunktionen (definierte Vorgaben von Einstellungen und Berechtigungen).

Verfügbarkeit

- Falls die Geräte eine hohe Verfügbarkeit aufweisen müssen, sind Massnahmen für die Überbrückung von Ausfällen vorzusehen.
- Dokumentation und/oder Speicherung von Konfigurationen, um Ersatzgeräte schnell einrichten zu können
- Allenfalls Vorhalten von Reservegeräten (Cold Standby) für Drucker, Kopierer, Multifunktionsgeräte und Druckserver
- Angemessene Reserven für Verbrauchsmaterialien sowie Überwachung der Bestände
- Einheitliche Gerätebeschaffung, so dass Geräte, Gerätekomponenten und Verbrauchsmaterialien untereinander ausgetauscht werden können
- Abschliessen von Wartungs- oder Lieferverträgen mit an die Anforderungen angepassten Reaktionszeiten

Vertragliche Regelungen

- Regelung von datenschutzrechtlichen Aspekten und Geheimhaltungspflichten in Verträgen mit Lieferanten und Wartungsfirmen
- Regelung von sicherheitsrelevanten Einstellungen und Massnahmen für Lieferung, Wartung und Austausch von Druckern, Kopierern und Multifunktionsgeräten (beispielsweise Löschung von Daten oder Ausbau von Speichermedien)
- Definition und Umsetzung der sicherheitsrelevanten Einstellungen

3.2 Technische Massnahmen

Die folgenden technischen Massnahmen sind bei Druckern, Kopierern oder Multifunktionsgeräten umzusetzen:

- Einsatz eines Druckservers, um die zentrale Protokollierung und Verwaltung sowie einen besseren Schutz vor Angriffen zu ermöglichen
- Einrichten von Passwörtern für Bedienfeld (Konsole) sowie für ein allfälliges Web-GUI für die Wartung. Vordefinierte Initialpasswörter sind zu ändern.
- Verschlüsselung der Kommunikation von und zu den Geräten mit IPSec- oder IPP-Protokoll sowie TLS/SSL
- Sperren von nicht benötigten Ports und Protokollen auf den Geräten, um unerwünschte Verbindungen zu verhindern
- Sperrung der E-Mail-Funktion, falls nicht benötigt
- Verwendung von vordefinierten Zieleingaben, beispielsweise aus internem Adressbuch, statt manueller Zieleingabe (Mail-to, Scan-to)
- Löschen der Daten aus dem Speicher nach Ausdruck/Kopie (wenn möglich automatisch), Verwenden von Funktionen zum unwiederbringlichen Löschen von Daten
- Verschlüsseln der Festplatten beziehungsweise Gerätespeicher
- Aktivieren der Authentifizierung der Benutzerinnen und Benutzer an den Geräten mit Passwort/PIN, Chipkarte oder ähnlichem, so dass ein Ausdruck erst nach Login erfolgt, insbesondere bei öffentlich zugänglichen Druckern
- Automatischer Log-Off des Benutzers nach einer definierten Inaktivitätszeit
- Sperre eines Benutzers nach einer bestimmten Anzahl fehlerhafter Anmeldeversuche
- Definition/Einschränkung von externen Zugriffen für Administratoren
- Definition/Einschränkung der Zugriffe (und Zugriffszeiten) für die Fernadministration der Geräte
- Beim Einsatz von netzfähigen Komponenten Mechanismen zum Schutz vor Angriffen aus dem Netzwerk einrichten, wie Verwenden von IEEE 802.1X oder ähnlichen Verfahren zur netztechnischen Zugangskontrolle, damit Geräte nicht unberechtigt an das Netzwerk angeschlossen werden können
- Wo vorhanden, Verwendung der internen Firewall zur Steuerung von Zugriffen, beispielsweise nur von festgelegten IP-Bereichen aus

- Verwenden von separaten Netzwerkzonen für Drucker, Kopierer und Multifunktionsgeräte
- Verhindern von Netzwerkverbindungen vom Druckserver zu anderen IT-Systemen ausser zu den voreingestellten Druckern
- Sicherstellen, dass Drucker, Kopierer und Multifunktionsgeräte bei Sicherheitsprüfungen berücksichtigt werden

4 Quellenverzeichnis und weiterführende Links

Bundesamt für Sicherheit in der Informationstechnik (BSI), Deutschland:
Baustein SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte gemäss neuem IT-Grundschutz-Kompendium
Darin insbesondere:

- SYS.4.1A1 Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten
- SYS.4.1A4 Erstellung eines Sicherheitskonzepts für den Einsatz von Druckern, Kopierern und Multifunktionsgeräten
- SYS.4.1.A2 Geeignete Aufstellung und Zugriff auf Drucker, Kopierer und Multifunktionsgeräte
- SYS.4.1.A5 Erstellung von Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten
- SYS.4.1.A16 Notfallvorsorge bei Druckern, Kopierern und Multifunktionsgeräten
- SYS.4.1.A7 Beschränkung der administrativen Fernzugriffe auf Drucker, Kopierer und Multifunktionsgeräte
- SYS.4.1.A15 Verschlüsselung von Informationen bei Drucker, Kopierer und Multifunktionsgeräten
- SYS.4.1.A17 Schutz von Nutz- und Metadaten
- SYS.4.1.A20 Erweiterter Schutz von Informationen bei Drucker, Kopierer und Multifunktionsgeräten
- SYS.4.1.A11 Einschränkung der Anbindung von Druckern, Kopierern und Multifunktionsgeräten
- SYS.4.1.A14 Authentisierung und Autorisierung bei Druckern, Kopierern und Multifunktionsgeräten
- SYS.4.1.A12 Ordnungsgemässe Entsorgung von Geräten und schützenswerten Betriebsmitteln

Allianz für Cybersicherheit (ACS) / Bundesamt für Sicherheit in der Informationstechnik (BSI), Deutschland:

- Drucker und Multifunktionsgeräte im Netzwerk

V 1.2 / November 2019