DIE BSI CHECKLISTE
FÜR CANON imageRUNNER ADVANCE

SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte

Canon

See the bigger picture

VON GRUND AUF SICHER

Der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) beleuchtet inzwischen seit vielen Jahren die Themen und Entwicklungen in der Informationssicherheit und leitet daraus praktikable Sicherheitsempfehlungen ab.

Das IT-Grundschutz-Kompendium enthält IT-Grundschutz-Bausteine, die Unternehmen und Institutionen – die in Zeiten der Digitalisierung ihre Prozesse und Projekte nach dem Stand der Technik absichern wollen – zu Rate ziehen und verwenden können.

Die beigefügte Übersicht stellt eine Hilfestellung dar, sobald Canon imageRUNNER ADVANCE Systeme und Lösungen zum Einsatz kommen und die IT-Sicherheit nach BSI-Empfehlung realisiert werden soll. Überall, wo die Hard- und Software von Canon etwas zur IT-Sicherheit beiträgt, finden Sie die relevanten Informationen mit der jeweiligen Abschnittskennzeichnung (ID) aus der BSI Checkliste SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte . Kundenseitige Maßnahmen und individuelle Voraussetzungen werden in der Übersicht nicht berücksichtigt. Zusätzlich stellt das BSI weitere Checklisten zur Maßnahmenplanung auf seiner Webseite zur Verfügung (Link auf der Rückseite).

	ID	ANFORDERUNGEN	ERFÜLLT	BEMERKUNGEN
Basis-Anforderung	SYS.4.1.A1	Unterstützung sicherer Protokolle zur Datenübertragung und Administration.	✓	TLS 1.2/1.3; SMB 3.0/3.1/3.1.1 (ab Firmwareplattform 3.15); iPSec, IEEE802.1x, WPA3, SFTP, SNMPv3
		Verschlüsselung der abgespeicherten Informationen.	✓	AES 256 Bit Verschlüsselung, kritische Daten (Login, Zertifikate, Datenzuordnungstabellen) werden zudem mit TPM-Modulen und zusätzlichen Canon Encryption-Chips geschützt
		Authentisierung der Benutzenden direkt am Gerät.	✓	PIN, Passwort, optional Karten oder mobile Authentifizierung oder Kombinationen von verschiedener Authentifizierungsmöglichkeiten
		Existenz eines zuverlässigen und leistungsfähigen automatischen Seiteneinzugs der Scaneinheit.	✓	Originaleinzüge für das gleichzeitige Einscannen von Vorder- und Rückseite (1Pass DADF) verfügen über eine Ultraschall-Doppeleinzugskontrolle und gewährleisten so einen vollständigen Scanvorgang ohne fehlende Inhalte
		Unterstützung geeigneter Datenformate.	✓	TIFF, JPEG, PDF (eingeschränkte Farben, komprimiert, durchsuchbar, Richtlinie anwenden, Optimieren für Web, PDF A/1-b, Trace & Smooth, verschlüsselt, Gerätesignatur, Benutzersignatur), XPS (komprimiert, durchsuchbar, Gerätesignatur, Benutzersignatur), Office Open XML (PowerPoint, Word)
		Existenz einer Funktion zum sicheren Löschen des Speichers	✓	Vollständige Initialisierung (am Nutzungsende) mit auf den jeweiligen Speicher HDD/SSD angepassten Verfahren
		Verfügbarkeit von regelmäßigen Updates und Wartungsverträgen.	✓	Softwareupdates und Serviceverträge via CDS (Canon Content Delivery System)
	SYS.4.1.A2	Drucker, Kopierer und Multifunktionsgeräte MÜSSEN mit Gerätepasswörtern versehen sein, um so den Zugriff auf Webserver und Bedienfeld für die Administration zu sperren.	✓	Komplexe Passwortverfahren, getrennte Passwörter, AMS (Access Management System), ab FW 3.15: Möglichkeit der Zwei-Faktor-Authentifizierung für Administratoren (und Nutzer) nicht nur direkt am System, sondern auch an der Webschnittstelle des iR-ADV DX
		Drucker, Kopierer und Multifunktionsgeräte MÜSSEN die Vorgaben des Identitäts- und Berechtigungsmanagements der Institution erfüllen.	✓	AMS (Access Management System) in Kombination mit entsprechenden Authentifizierungsmethoden (von PIN bis Kartenleser oder mobile Authentifizierung)
Standard-Anforderung	SYS.4.1.A4	Es SOLLTE auch festgelegt werden, welche Funktionen von welchen Benutzenden unter welchen Bedingungen administriert beziehungsweise genutzt werden dürfen.	✓	Das AMS ermöglicht personen- oder rollenbezogene Freigaben
	SYS.4.1.A7	Das SOLLTE auch dann gewährleistet sein, wenn die Institution eine zentrale Geräteverwaltungssoftware einsetzt.	✓	iW EMC – IW Enterprise Management Console
	SYS.4.1.A11	Der IT-Betrieb SOLLTE sicherstellen, dass netzfähige Drucker, Kopierer und Multifunktionsgeräte nicht aus Fremdnetzen erreichbar sind.	✓	Sicherheitsrichtlinien, Portkontrolle
		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.	✓	Trennung der Faxleitung vom LAN (ggf. W-LAN)
	SYS.4.1.A15	Wenn möglich, SOLLTEN alle auf geräteinternen, nichtflüchtigen Speichermedien abgelegten Informationen verschlüsselt werden.	✓	HDD: Durch den Administrator deaktivierbare AES 256 Bit Verschlüsselung, hardwarebasierte HDD-Passwortsperre zusätzlich zur Verschlüsselung (bei Entfernung aus dem MFP – z.B. Diebstahl) SSD: Permanente, nicht deaktivierbare AES 256 Bit Verschlüsselung, hardwarebasierte SSD-Passwortsperre zusätzlich zur Verschlüsselung (bei Entfernung aus dem MFP – z.B. Diebstahl)
		Auch Druckaufträge SOLLTEN möglichst verschlüsselt übertragen werden.	✓	siehe Protokolle zur Datenübertragung, bei nicht ans Netzwerk angeschlossene Systeme kann eine Verschlüsselung bis AES 256 Bit zugeschaltet werden

	ID	INHALT	ERFÜLLT	BEMERKUNGEN
Standard-Anforderung	SYS.4.1.A17	Nutz- und Metadaten wie Druckaufträge und Scandateien SOLLTEN nur so kurz wie möglich auf den Geräten gespeichert werden.	✓	HDD: direkte Löschung nach Auftragsende – z.B. durch 3faches Überschreiben gem. DoD-Standard SSD: Automatische Löschung im Rahmen der automatischen Speicherverwaltung (Garbage Collection) und des sog. „Wear Levelling“
		Dateiserver in den Geräten und Funktionen wie „Scan in den Gerätespeicher" SOLLTEN vom IT-Betrieb abgeschaltet werden.	✓	Systemkonfiguration
		Die dafür benötigten Protokolle und Funktionen SOLLTEN, soweit möglich, gesperrt werden.	✓	Systemkonfiguration
		Generell SOLLTE vom IT-Betrieb sichergestellt werden, dass alle Metadaten nicht für Unberechtigte sichtbar sind.	✓	Systemkonfiguration
	SYS.4.1.A18	Nicht benötigte Gerätefunktionen SOLLTEN abgeschaltet werden.	✓	Systemkonfiguration
		Insbesondere SOLLTEN alle nicht benötigten Daten- und Netzschnittstellen von Druckern, Kopierern und Multifunktionsgeräten deaktiviert werden.	✓	Portmanagement im Rahmen des Setzens und Managens von Sicherheitsrichtlinien
		Die Geräte SOLLTEN ausschließlich über verschlüsselte Protokolle wie HTTPS und SNMPv3 verwaltet werden.	✓	Siehe Protokolle ID: SYS 4.1.A1
		Sämtliche Protokolle, mit denen unverschlüsselt auf Drucker und Multifunktionsgeräte zugegriffen werden kann, SOLLTEN vom IT-Betrieb durch verschlüsselte ersetzt oder abgeschaltet werden.	✓	Siehe Protokolle ID: SYS 4.1.A1
		Das SOLLTE insbesondere für Protokolle umgesetzt werden, mit denen sich die Gerätekonfiguration verändern lässt, z. B. SNMP, Telnet und PJL.	✓	Siehe Protokolle ID: SYS 4.1.A1
Anforderung bei erhöhtem Schutzbedarf	SYS.4.1.A14	Nur berechtigte Personen SOLLTEN auf die ausgedruckten oder kopierten Dokumente zugreifen können.	✓	Diverse Secureprint-Funktionalitäten
		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“).	✓	Diverse Secureprint-Funktionalitäten plus diverse Authentifizierungsfunktionalitäten auch für nicht netzwerkangebundene Systeme.
		Nachdem sich die Benutzenden authentisiert haben, SOLLTEN ausschließlich nur die eigenen Druckaufträge sichtbar sein.	✓	Es wird nur die individuelle Nutzer-Druckwarteschlange angezeigt
		Nur die für die jeweiligen Benutzenden notwendigen Funktionen SOLLTEN freigeschaltet werden.	✓	AMS Konfiguration
	SYS.4.1.A16	Ausfallzeiten von Druckern, Kopierern und Multifunktionsgeräten SOLLTEN möglichst gering sein	✓	siehe Keypoint Intelligence / BLI Auszeichnung „Most relieable A3 Line Up“ 2022 – 2024
		in Wartungsverträgen SOLLTE auf eine angemessene Reaktionszeit geachtet werden	✓	Optional stehen verschiedene SLAs (Service Level Agreements) mit unterschiedlichen Reaktionszeiten zur Verfügung
	SYS.4.1.A20	Es SOLLTEN auf dem Druckserver die Namen der Druckaufträge nur anonymisiert angezeigt werden.	✓	Konfiguration
		Alle Schnittstellen für externe Speichermedien SOLLTEN gesperrt werden.	✓	USB-Port kann gesperrt werden, USB-Port ist vom LAN (ggf. W-LAN) getrennt
		Weiterhin SOLLTEN geräteinterne Adressbücher deaktiviert und den Benutzenden alternative Adressierungsverfahren (z. B. Adresssuche per LDAP) angeboten werden.	✓	Diverse Möglichkeiten der Restriktion von Adressbuch-Zugriffen, Adressmanagement
		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.	✓	Konfiguration via AMS/LDAP
		Auch SOLLTEN Dokumente nur an interne E-Mail-Adressen verschickt werden können.	✓	Konfiguration und Adressmanagement
		Eingehende Fax-Dokumente sowie Sendeberichte SOLLTEN nur autorisierten Personen zugänglich sein.	✓	Secure Faxmailbox, Faxweiterleitung, Unterdrückung des Faxausdruckes
	SYS.4.1.A21	Der IT-Betrieb SOLLTE die Sicherheitseinstellungen von Druckern, Kopierern und Multifunktionsgeräten regelmäßig kontrollieren und, falls notwendig, korrigieren.	✓	Möglich via iW EMC, Setzen und Managen von Sicherheitsrichtlinien (auch automatisches Zurückschreiben)
		Wenn ein automatisiertes Kontroll- und Korrektursystem verfügbar ist, SOLLTE es genutzt werden.	✓	Möglich via iW EMC, Setzen und Managen von Sicherheitsrichtlinien
		Zudem SOLLTE eingeschränkt werden, dass die Geräte über das Bootmenü auf die Werkseinstellungen zurückgestellt werden können.	✓	Passwortmanagement, Zugriffsverwaltung, Admin-Rechte
		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.	✓	Überprüfung und Schutz durch „Sicherer Systemstart“ und im laufenden Betrieb durch Trellix/McAfee Embeded Control (Whitelisting, Run Time Intrusion Detection). Systeme des Modelljahrgangs 2023 verfügen über eine resiliente Firmware, die sich im Falle einer Manipulation selbst „heilt“.

Zuverlässigkeit: Keypoint Intelligence testete über einen **Zeitraum von fünf Jahren** 23 Canon A3 MFPs. Bei **4,45 Millionen produzierten Seiten** gab es **lediglich sechs Fehleinzüge.**

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.

Derzeit finden insbesondere zwei Evaluierungsstandards Anwendung, um die Sicherheits- und Vertraulichkeitsziele zu prüfen:

Bei Systemen mit HDD: „IEEE Std 2600.2TM-2009“ bei der die Prüftiefe durch eine EAL-Einstufung (meist EAL 2+) dokumentiert wird.

Bei Systemen mit SSD:

„Protection Profile for Hardcopy Devices 1.0, 2015“ – hierbei erfolgt keine EAL-Einstufung der Prüftiefe. Bei Erfüllung der Vorgaben erhalten die getesteten Systeme die Common Criteria (ISO 15408) Zertifizierung unabhängig vom Evaluierungsstandard.

Die Common Criteria Zertifizierung erfolgt unabhängig von dem verwendeten Evaluierungsstandard.

Alle iR-ADV sind/werden Common Criteria (ISO 15408) zertifiziert und entsprechen mindestens dem US-Kryptostandard FIPS140-2.

Systeme des Modelljahrgangs 2023 mit Firmwareplattform 3.15 werden dem neuen US-Kryptostandard FIPS140-3 entsprechen und verfügen über eine resiliente Firmware, die sich im Falle einer Manipulation selbst „heilt“.

Canon Deutschland GmbH
Europark Fichtenhain A10
47807 Krefeld
Tel. +49 2151 3450

Finden Sie weiterführende Informationen (Edition 2023) und die Checklisten zum IT-Grundschutz-Kompendium (Edition 2023) als Planungsgrundlage auf: **www.bsi.bund.de**