



Security Guide

Sichern Sie Ihr Unternehmen, schützen Sie Ihre Daten

SHARP
Be Original.

Sofort wirksamer Schutz.

Denn wussten Sie, dass ungeschützte Drucker eine offene Hintertür für die Gefährdung oder den Diebstahl Ihrer wertvollen Daten darstellen können?

Drucker sind an den meisten Arbeitsplätzen ein fester Bestandteil. Sie werden jeden Tag routinemäßig benutzt und haben sich äußerlich in den letzten zwanzig Jahren kaum verändert. Wie IT-Administratoren jedoch wissen, haben sich Multifunktionsdrucker (MFPs) und Drucker zu hochentwickelten Computersystemen entwickelt, die mit Ihrem Unternehmensnetzwerk und dem Internet verbunden sind.

Während das Thema Datensicherheit bei den meisten Unternehmen ganz oben auf der Tagesordnung steht, werden ihre Druckgeräte leider oft übersehen. Tatsächlich verfügt ein Drittel der europäischen kleinen und mittleren Unternehmen (KMU) nicht über IT-Sicherheitsmaßnahmen für Drucker*. Das macht sie zu einem Hauptziel für Hacker und andere böswillige Akteure, zumal die Entwicklung hin zu hybriden Arbeitsplätzen noch zusätzliche Schwachstellen eröffnet hat. Ungesicherte Drucker bieten oft ein einfaches Einfallstor in Ihr Unternehmen und ermöglichen den Zugriff auf in den Druck- und Scanaufträgen enthaltene sensible Informationen und möglicherweise sogar auf Ihr gesamtes IT-Netzwerk.

Die Bedrohung ist sehr real – und sich bietende Lücken werden ausgenutzt. Fast ein Fünftel (19%) der europäischen KMU waren schon einmal von einem Sicherheitsverstoß in einem Drucker betroffen*. Darüber hinaus kann ein Datenverlust, insbesondere wenn diese in die falschen Hände geraten, einen enormen und langfristigen Imageschaden verursachen.

Jedes Unternehmen, egal wie groß oder klein, muss sicherstellen, dass seine Dokumentenproduktionsumgebung durch Technologie und sicheres Benutzerverhalten geschützt ist – genauso wie jeder Geschäftslaptop oder PC. Deshalb steht das Thema Sicherheit im Mittelpunkt aller Produktentwicklungen von Sharp. Wir wollen gewährleisten, dass unsere Produkte und Dienstleistungen das Arbeitsleben der Menschen einfacher und produktiver machen und gleichzeitig die Daten sicher halten.

Die Risiken verstehen

Moderne Unternehmen verarbeiten eine Vielzahl von Informationen, haben aber oft keinen wirklichen Überblick darüber, wie diese erstellt, gespeichert, weitergegeben und abgerufen werden. Dies führt unweigerlich zu potenziellen Sicherheits- und Compliance-Risiken, wozu auch Datenschutzverletzungen, ungesicherte Dateien, menschliche Fehler und unbefugter Zugriff auf Informationen gehören können.

* Quelle: Die Studie wurde von Censuswide zwischen dem 1. und dem 13. Februar 2023 durchgeführt. Insgesamt haben 5.770 IT-Entscheidungsträger und für den IT-Einkauf in KMU verantwortliche Personen aus 11 Ländern (Deutschland, Österreich, Schweiz (DACH) sowie Belgien, Frankreich, Italien, Niederlande, Polen, Spanien, Schweden und Großbritannien) die Studienfragen beantwortet, davon 1.543 Personen in der DACH-Region.



Um wirklich effektiv zu sein, muss Ihre Informationssicherheit Ihre Drucker und Unternehmensinformationen vor allen Formen des Zugriffs und der Nutzung durch Unbefugte sowie der Offenlegung, Änderung oder Zerstörung schützen. Diese sind:

Physische Bedrohungen

Alle physischen Handlungen und Ereignisse, die zu einem schwerwiegenden Verlust oder einer Beschädigung von Informationen oder Systemen führen könnten, seien sie interner (z. B. durch eine instabile Stromversorgung) oder externer (etwa durch Blitzeinschlag) Natur oder von Menschen verursacht (z. B. durch einen verärgerten Angestellten oder aufgrund von sensiblen Dokumenten, die unbeaufsichtigt im Ausgabefach liegen).

Netzwerkbedrohungen

Jede Aktivität, die einen unbefugten Zugang zu Ihrem Netzwerk ermöglicht, in der Regel um durch Viren und Malware auf Daten zuzugreifen oder diese zu gefährden, um durch Phishing-Kampagnen vertrauliche Informationen zu stehlen oder um mithilfe von Denial-of-Service (DoS) Angriffen oder Ransomware Zugang zum System zu erlangen.

Gesetzliche Verpflichtungen

Der Schutz aller sensiblen Daten, die ein Unternehmen besitzt (wie z. B. Mitarbeiterdaten, Kundeninformationen und Kontodaten), gemäß der geltenden staatlichen oder branchenspezifischen Vorschriften (wie z. B. der DSGVO) – unabhängig von ihrem jeweiligen Speicherort.

Sicher sein und dabei produktiv bleiben.

In der heutigen, ständig vernetzten Welt werden die Bedrohungen immer komplexer. Die Sicherungsmaßnahmen für Multifunktionsdrucker sollten dies auch sein – ohne die Produktivität zu beeinträchtigen.

Der gesamte Schutz, den Sie brauchen

Sharp ist sich bewusst, dass der Schutz Ihrer Unternehmens- und Nutzerdaten für Ihren Erfolg – und Ihr Überleben – entscheidend ist. Wir wissen aber auch, dass zu strenge oder ineffizient umgesetzte Sicherheitsmaßnahmen ernsthafte Auswirkungen auf die Produktivität haben können.

Unsere Drucker und Multifunktionssysteme verfügen über eine Reihe fortschrittlicher SIEM-Funktionen (Security Information and Event Management), die entwickelt wurden, um Ihre Informationen und Dokumente vor einer Vielzahl von physischen und Cyber-Sicherheitsbedrohungen, einschließlich der langwierigsten und hartnäckigsten Angriffe, zu schützen. Sie helfen Ihnen auch bei der Einhaltung immer strengerer gesetzlicher und behördlicher Anforderungen, wie z. B. der Datenschutz-Grundverordnung (DSGVO).

Wir geben Ihnen die Werkzeuge an die Hand, mit denen Sie Ihre Drucksicherheitsrichtlinien kontrollieren und verwalten und sicher auf Ihre vertraulichen Informationen zugreifen können, unabhängig davon, wie sie erfasst, gespeichert, gedruckt oder über Ihr Netzwerk weitergegeben werden:

- **Automatische Verschlüsselung** aller Dokumente, die auf dem Gerät gespeichert sind oder von ihm per E-Mail verschickt werden
- **Selbsteilungstechnologie** zur sicheren Wiederherstellung eines Endgeräts im Falle eines Angriffs
- **Blinkende LED** als Erinnerung, dass Dokumente nicht in der Ausgabe des Originalinzugs liegengelassen werden
- **Whitelisting** von Anwendungen und Firmware, die mit dem Gerät kommunizieren können
- **SSL/TLS Zertifikatsvalidierung** zur Überprüfung der Sicherheit von mit Ihrem Endgerät kommunizierenden Servern von Drittanbietern
- **Audit Trail** und Job Log-Funktionen zur Bereitstellung einer umfassenden Übersicht über sämtliche Nutzeraktivitäten
- **Anti-Malware-Überwachung** mittels Bitdefender zur Wahrung der Sicherheit Ihrer Daten und Endgeräte sowie des gesamten Netzwerks (optional)



Für noch mehr Sicherheit

Unsere neuesten „Future Workplace“-MFPs verfügen über BIOS-basierte Sicherheitsfunktionen, die den Start des Geräts sofort verhindern, wenn Fehler festgestellt werden. Außerdem werden Sicherheitsupdates automatisch aus der Cloud bereitgestellt, sodass der Schutz vor Cyberangriffen immer auf dem aktuellsten Stand ist. Zudem bieten diese MFPs noch mehr Sicherheit durch Anti-Malware-Software mit Bitdefender.*

Um jede unbefugte Nutzung zu verhindern, enthalten unsere neuesten MFPs auch vorinstallierte Root-Zertifikate. Außerdem überwachen sie automatisch Zugriffsversuche und gewähren nur den Anwendungen und Betriebssystemen Zugriff, die auf einer genehmigten Whitelist stehen. Alle anderen externen Anwendungen werden sofort blockiert, protokolliert und gemeldet. Die Zugriffserkennung (Intrusion Detection) bietet die nächste Stufe des Schutzes und schützt Ihr MFP* vor verdächtigen Netzwerkzugriffsversuchen. Denn auch Informationen, die zwischen einem MFP und einer anderen Anwendung oder einem E-Mail-System ausgetauscht werden, können abgefangen oder kompromittiert werden.

Zukunftsorientiertes Sicherheitsmanagement

Für eine sichere und stabile IT-Infrastruktur sind regelmäßige Wartungen und zeitnahes Einspielen von Updates für alle Systeme notwendig. Denn nicht oder zu spät gepatchte IT-Systeme können durch veraltete Software und Betriebssysteme erhebliche

Sicherheitslücken aufweisen und einen instabilen Betrieb zur Folge haben. Firmware-Updates sollten also so zeitnah wie möglich verteilt werden.

Die neuen Arbeitsplatz-MFPs sind hochgradig belastbar und zukunftssicher durch ihre Firmware-Update-Funktion. Die Systeme erkennen eigenständig die Verfügbarkeit einer neuen Version, laden diese sicher herunter und installieren die Firmware ohne aufwendigen Technikereinsatz just in time.

Und irgendwann kommt der Zeitpunkt, an dem der Multifunktionsdrucker für immer vom Netz geht. Eine letzte, absolut essenzielle Sicherheitsregel gilt es auch dann noch zu beachten: Speicher/Festplatte, benutzerorientierte Daten, Adressbücher und IT-Einstellungen sollten zwingend unwiderruflich gelöscht werden. So gehen Sie auf jeden Fall auf Nummer sicher.

*optional; nicht für alle Modelle verfügbar.

Umfassender Schutz.

Ihre auf einem Gerät vorhandenen Sicherheitsmaßnahmen sollte einen vollständigen Schutz an allen wichtigen Schwachstellen und Angriffspunkten bieten.

Während PCs, Laptops und Server immer besser gegen Angriffe abgesichert sind, ist es inzwischen unerlässlich geworden, auch andere vernetzte Geräte, wie Drucker oder Multifunktionssysteme, gegen Zugriffe von außen zu schützen. Aus diesem Grund haben wir eine detaillierte Übersicht der Sicherheitsfunktionen unserer **MFPs und Drucker** auf den folgenden Seiten für Sie zusammengefasst.

Modellübersicht für Folgeseiten				
BP-22C25 BP-C131WD BP-C131PW	MX-CxxxF/P MX-BxxxF/W/P/PW	BP-30C25	MX-M1206 MX-M1056 MX-8081 MX-7081	BP-90Cxx BP-70/60/50/55Cxx BP-70/50Mxx BP-B547WD/B537WR BP-C5xxWD/WR
Modellbezeichnungen				
A3-MFPs				
BP-22C25*		BP-30C25	MX-M1206/MX-M1056 MX-8081/MX-7081	BP-90C80/BP-90C70 BP-70M90/BP-70M75 BP-70C65/BP-70C55 BP-70C45/BP-70C36/BP-70C31 BP-60C45/BP-60C36/BP-60C31 BP-50C65/BP-50C55 BP-50C45/BP-50C36/BP-50C31/BP-50C26 BP-55C26 BP-70M65/BP-70M55 BP-70M45/BP-70M36/BP-70M31 BP-50M65/BP-50M55 BP-50M45/BP-50M36/BP-50M31/BP-50M26
A4-MFPs				
BP-C131WD	MX-C528F/MX-C428F MX-C358F MX-B557F MX-B468F/MX-B427W			BP-B547WD/BP-B537WR BP-C542WD/BP-C533WD/BP-C533WR
A4-Drucker				
BP-C131PW	MX-C428P MX-B557P MX-B468P/MX-B427PW			

* Verfügbar ab Frühjahr 2025

Data Security	BP-22C25 BP-C131WD BP-C131PW	MX-CxxxP/ MX-BxxxP/ W/P/PW	BP-30C25		MX-M1206 MX-M1056 MX-8081 MX-7081	BP-90Cxx BP-70/60/50/55Cxx BP-70/50Mxx BP-B547WD/B537WR BP-C5xxWD/WR		
	Standard-Sicherheitsfunktionen	Standard-Sicherheitsfunktionen*	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit
Trusted Platform Module (TPM)	⊗	+	⊗	✓	⊗	✓	✓	✓
Datenüberschreibungsmethode (HDD)	⊗	✓ NIST*1 DoD 5220.22-M	⊗	⊗	✓ 0-FF Zufallszahl DoD 5220.22-M	✓ 0-FF Zufallszahl DoD 5220.22-M	⊗	⊗
Datenüberschreibungsmethode (Flash, SSD)	✓ AES 256bit CBC	✓ eMMC	✓	✓	⊗	⊗	✓	✓
Datenüberschreibung nach Auftragsabschluss	✓	✓ Einzel- oder Mehrfachdurchlauf gemäß NIST*1	✓	✓	✓ bis zu 10x	✓ bis zu 10x	✓	✓
Datenüberschreibung nach Aufforderung	⊗	✓	⊗	✓	⊗	✓	⊗	✓
Löschung des gesamten Speichers	⊗	✓	⊗	✓	⊗	✓	⊗	✓
Löschung aller Daten in der Auftragsstatusliste unter „abgeschlossen“	⊗	✓	⊗	✓	⊗	✓	⊗	✓
Löschung der Dokumentenablagedaten	⊗	✓	⊗	✓	⊗	✓	⊗	✓
Löschung von Adressbuch/registrierten Daten	⊗	✓	⊗	✓	⊗	✓	⊗	✓
Automatische Datenlöschung nach Auftrag	⊗	✓	⊗	✓	⊗	✓	⊗	✓
Auto-Clear-Funktion beim Einschalten	⊗	⊗	⊗	✓	⊗	✓	⊗	✓
End-of-Lease-Funktion (Löschung des gesamten Speichers und Erstellung einer Bestätigung)	✓	✓	✓ Sicherheitslöschung	✓ Sicherheitslöschung	✓ Wertüberschreibung mit „0“	✓ Wertüberschreibung mit Zufallszahl	✓ Sicherheitslöschung	✓ Sicherheitslöschung
Datenschlüsselung (AES 256 Bit)	✓ AES 256bit	✓ ECB-Modus*2	✓ ECB-Modus*2	✓ EBC-Modus*3	✓ ECB-Modus*2	✓ EBC-Modus*3	✓ EBC-Modus*3	✓ EBC-Modus*3
Verschlüsseltes PDF	✓ nur bei Druck über IPP (AirPrint)	✓	✓	✓	✓	✓	✓	✓
Löschung der Dokumentenablage (Schnellablage, Stapeldruck, Speicherung/Backup von Dokumentenablagedaten)	⊗	✓	✓	✓	✓	✓	✓	✓
Zeitgesteuerte Löschung von Dokumentenablagedaten	⊗	⊗	✓	✓	✓	✓	✓	✓
Betriebssperre bei Fehleingabe des Ablagepassworts	⊗	✓ Nutzer-Lockout	⊗	✓	⊗	✓	⊗	✓
Whitelisting von Anwendungen	✓	⊗	✓	✓	✓	✓	✓	✓
Schutz vor Firmware-Angriffen & Selbstwiederherstellung	⊗	⊗	✓	✓	✓	✓	✓	✓

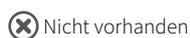
Legende



Standard



Optional



Nicht vorhanden

* MX-B427W und MX-B427PW unterstützen nicht alle Funktionen. MX-C428P, MX-B468P und MX-B557P unterstützen keine MFP-bezogenen Sicherheitsfunktionen für Scans und Fax. Bitte informieren Sie sich in dem entsprechenden Datenblatt oder im Web.

** National Institute of Standards and Technology *2 Electronic Code Book Mode *3 Cipher Block Chaining Mode

Netzwerk- und Kommunikations-sicherheit	BP-22C25 BP-C131WD BP-C131PW	MX-CxxxF/P MX-BxxxF/ W/P/PW	BP-30C25		MX-M1206 MX-M1056 MX-8081 MX-7081	BP-90Cxx BP-70/60/50/55Cxx BP-70/50Mxx BP-B547WD/B537WR BP-C5xxWD/WR		
	Standard-Sicherheits-funktionen	Standard-Sicherheits-funktionen*	Standard-Sicherheits-funktionen	mit installiertem Data Security Kit	Standard-Sicherheits-funktionen	mit installiertem Data Security Kit	Standard-Sicherheits-funktionen	mit installiertem Data Security Kit
Schutz der Netzwerkkommunikation: HTTPS, IPsec & TLS	✓	✓	✓	✓	✓	✓	✓	✓
Schutz der Netzwerkkommunikation: Wireless LAN	✓	✓	✓	✓	✓	✓	✓	✓
Kerberos	✗	✓	✓	✓	✓	✓	✓	✓
S/MIME Verschlüsselung	✗	✓	✓	je nach Einstellung ✓	✓	✓	✓	je nach Einstellung ✓
IP-Adressen-Filter	✓	✓	✓	✓	✓	✓	✓	✓
MAC-Adressen-Filter	✓	✗	✓	✓	✓	✓	✓	✓
Port-Management (Öffnung und Schließung von Ports)	✓	✓	✓	✓	✓	✓	✓	✓
SNMPv3 Unterstützung – SHA1, AES 128 Bit	✓	✓	✓	✓	✓	✓	✓	✓
Vorinstallierte Endgerätezertifikate	✓	✓	✓	✓	✓	✓	✓	✓
Cross-Site Request Forgery (CSRF) Messung	✓	✗	✓	✓	✓	✓	✓	✓
Denial of Service (DoS)	✗	✗	✓	✓	✗ nur MX-xx81	✗ nur MX-xx81	✓	✓
IEEE802.1X™ Authentifizierung	✓	✓	✓	✓	✓	✓	✓	✓
IPP over SSL	✓	✓	✓	✓	✓	✓	✓	✓
Wireless LAN	✓	✓	✓	✓	✓	✓	✓	✓
E-Mail-Warnung/Status	✗	✓	✓	✓	✓	✓	✓	✓
Remote-Betrieb	✓	✓	✓	✓	✓	✓	✓	✓
Öffentlicher Ordner/NAS, Cloud-Verbindung, Export von Auftragsprotokollen/Syslog/Audit Protokollen, Speichersicherung, Klone von Geräten	✗	✓	✓	✓	✓	✓	✓	✓
Active Directory Integration	✗	✓	✓	✓	✓	✓	✓	✓
TLS Verschlüsselung	✓	✓	✓	✓	✓	✓	✓	✓
Sicherheitsrichtlinien-Management	✓	✓	✓	✓	✓	✓	✓	✓

Legende



Standard



Optional



Nicht vorhanden

* MX-B427W und MX-B427PW unterstützen nicht alle Funktionen. MX-C428P, MX-B468P und MX-B557P unterstützen keine MFP-bezogenen Sicherheitsfunktionen für Scans und Fax. Bitte informieren Sie sich in dem entsprechenden Datenblatt oder im Web.

Authentifizierung und Zugriffskontrolle	BP-22C25 BP-C131WD BP-C131PW	MX-CxxxF/P MX-BxxxF/ W/P/PW	BP-30C25		MX-M1206 MX-M1056 MX-8081 MX-7081	BP-90Cxx BP-70/60/50/55Cxx BP-70/50Mxx BP-B547WD/B537WR BP-C5xxWD/WR		
	Standard-Sicherheitsfunktionen	Standard-Sicherheitsfunktionen*	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit
Nutzerauthentifizierung (Lokal/LDAP/Active Directory/Kerberos)	✓	✓	✓	✓	✓	✓	✓	✓
LDAP-SSL / Secure	✓	✓ außer BP-B427W und BP-B427PW	✓	✓	✓	✓	✓	✓
ID-Karten-Authentifizierung	✓	✓	✓	✓	✓	✓	✓	✓
NTLMv2-Authentifizierung bei LDAP	✓	✓	✓	✓	✓	✓	✓	✓
NTLMv2-Authentifizierung bei SMB	✓	✓	✓	✓	✓	✓	✓	✓
Druckrichtlinien-Authentifizierung	✓	✓	✓	✓	✓	✓	✓	✓
Active Directory Integration (MFP wird in AD-Domain aufgenommen)	✗	✓	✓	✓	✓	✓	✓	✓
Active Directory Integration Single Sign-On (Ordner, E-Mail, Home-Verzeichnis)	✗	✓	✓	✓	✓	✓	✓	✓
Passwortgeschützter Admin-Zugriff auf Geräte-Homepage	✓	✓	✓	✓	✓	✓	✓	✓
Admin/Nutzer-Passwort-Richtlinie	✗	✓	✗	✗	✗	✗	✓	✓
Schutz des Admin-Passworts (bei Anmeldung über FTP)	✓	✓	✓	✓	✓	✓	✓	✓
User-Lockout	✓	✓	✓	✓	✓	✓	✓	✓
Passwortlänge und -anforderungen	Nutzer: 0-255/ Admin 5-255	Keine spezifischen Bedingung, aber max. Länge = 128, beliebige Sonder- zeichen werden akzeptiert	Nutzer 0-255 Admin 5-255	Nutzer/Admin N-255 (N: 5 bis 32; Admin spezifizierbar) Zeichen: 52 Buch- staben, 10 Zahlen, 10 spezifische Symbole	Nutzer 0-255 Admin 5-255	Nutzer/Admin N-255 (N: 5 bis 32; Admin spezifizierbar) Zeichen: 52 Buch- staben, 10 Zahlen, 10 spezifische Symbole	Nutzer 0-255 Admin 5-255	Nutzer/Admin N-255 (N: 5 bis 32; Admin spezifizierbar) Zeichen: 52 Buch- staben, 10 Zahlen, 10 spezifische Symbole

Drucksicherheit	BP-22C25 BP-C131WD BP-C131PW	MX-CxxxF/P MX-BxxxF/ W/P/PW	BP-30C25		MX-M1206 MX-M1056 MX-8081 MX-7081	BP-90Cxx BP-70/60/50/55Cxx BP-70/50Mxx BP-B547WD/B537WR BP-C5xxWD/WR		
	Standard-Sicherheitsfunktionen	Standard-Sicherheitsfunktionen*	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit
Authentifizierung von Druckaufträgen	✓	✓	✓	✓	✓	✓	✓	✓
Druckfreigabe mit PIN/Passwort	✓	✓	✓	✓	✓	✓	✓	✓
Serverlose Druckfreigabe	✗	✗	✓	✓	✓	✓	✓	✓
USB-Drucken (wenn erlaubt)	✓	✓	✓	✓	✓	✓	✓	✓
Deaktivierung des Listendrucks	✗	✓	✗	✓	✗	✓	✗	✓
Deaktivierung der Dokumentenablage	✗	✗	✗	✓	✗	✓	✗	✓
Deaktivierung von Druckaufträgen, die keine Druckhalteaufträge sind	✓	✓	✓	✓	✓	✓	✓	✓
Deaktivierung der Anzeige der Liste abgeschlossener Druckaufträge	✗	✗	✗	✓	✗	✓	✓	✓
Druck des Dokumentenkontrollmusters	✗	✗	✗	✓	✗	✓	✗	✓
Auftragsstopp bei Erkennung eines Dokumentenkontrollmusters	✗	✗	✗	✓	✗	✓	✗	✓
Aufrechterhaltung von Druckaufträgen	✓	✓	✓	✓	✓	✓	✓	✓

* MX-B427W und MX-B427PW unterstützen nicht alle Funktionen. MX-C428P, MX-B468P und MX-B557P unterstützen keine MFP-bezogenen Sicherheitsfunktionen für Scans und Fax. Bitte informieren Sie sich in dem entsprechenden Datenblatt oder im Web.

Scan-Funktionen und Sharp OSA® Anwendungen	BP-22C25 BP-C131WD BP-C131PW		MX-CxxxF/P MX-BxxxF/ W/P/PW		BP-30C25		MX-M1206 MX-M1056 MX-8081 MX-7081		BP-90Cxx BP-70/60/50/55Cxx BP-70/50Mxx BP-B547WD/B537WR BP-C5xxWD/WR	
	Standard-Sicherheitsfunktionen	Standard-Sicherheitsfunktionen*	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit		
Direkte Domain-Eingabe	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Sharp OSA: ACM & EAM externe Anwendung	✗	✗	✓	✓	✓	✓	✓	✓	✓	
Scannen in gemeinsame Ordner	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Scannen auf USB	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Scannen an E-Mail	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Scannen auf FTP	✗	✓	✓	✓	✓	✓	✓	✓	✓	
Scannen an E-Mails für Ziele, für die keine S/MIME-Verschlüsselung verfügbar ist	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Scannen auf SMB	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Scannen auf einen USB-Speicher	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Scannen über einen Remote-PC	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Sharpdesk Mobile	✓	✗	✓	✓	✓	✓	✓	✓	✓	
Dokumentenablage – Schnelzugriffordner	✗	✓	✓	✓	✓	✓	✓	✓	✓	
Dokumentenablage – Daten-Backup/-export	✗	✓	✓	✓	✓	✓	✓	✓	✓	

Mobile und Cloud-Funktionen	BP-22C25 BP-C131WD BP-C131PW		MX-CxxxF/P MX-BxxxF/ W/P/PW		BP-30C25		MX-M1206 MX-M1056 MX-8081 MX-7081		BP-90Cxx BP-70/60/50/55Cxx BP-70/50Mxx BP-B547WD/B537WR BP-C5xxWD/WR	
	Standard-Sicherheitsfunktionen	Standard-Sicherheitsfunktionen*	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit		
Cloud Connect (OneDrive, SharePoint Online, Google Drive™, Dropbox, Box)	✗	✓ ¹	✓	✓	✓	✓	✓	✓	✓	
MS Teams Connector (Microsoft Teams)	✗	✗	✗	✗	✗	✗	✓	✓	✓	
Email Connect (Exchange Server, Gmail™)	✗	✗	✓	✓	✓	✓	✓	✓	✓	
Mobiles Drucken (AirPrint, Android™)	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Mobiles Drucken (Sharpdesk® Mobile, Sharp Print Service Plugin)	✓	✗	✓	✓	✓	✓	✓	✓	✓	

Legende



Standard



Optional



Nicht vorhanden

* MX-B427W und MX-B427PW unterstützen nicht alle Funktionen. MX-C428P, MX-B468P und MX-B557P unterstützen keine MFP-bezogenen Sicherheitsfunktionen für Scans und Fax. Bitte informieren Sie sich in dem entsprechenden Datenblatt oder im Web.

** Nicht alle Connectoren sind verfügbar.

Audit Trail und andere Sicherheitsmaßnahmen	BP-22C25 BP-C131WD BP-C131PW	MX-CxxxF/P MX-BxxxF/ W/P/PW	BP-30C25		MX-M1206 MX-M1056 MX-8081 MX-7081	BP-90Cxx BP-70/60/50/55Cxx BP-70/50Mxx BP-B547WD/B537WR BP-C5xxWD/WR		
	Standard-Sicherheitsfunktionen	Standard-Sicherheitsfunktionen*	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit
Auftragsprotokoll und Nutzungsnachweis	⊗	✓	✓	✓	✓	✓	✓	✓
Änderungsnachverfolgung durch Admin (SIEM und Syslog Integration)	✓	✓	✓	✓	✓	✓	✓	✓
Digital signierte Firmware	✓	✓	✓	✓	✓	✓	✓	✓

Faxsicherheit Fax-Option ggf. erforderlich	BP-C131WD BP-C131PW	MX-CxxxF/P MX-BxxxF/ W/P/PW	BP-30C25		MX-8081 MX-7081	BP-70/60/50/55Cxx BP-70/50Mxx BP-B547WD/B537WR BP-C5xxWD/WR		
	Standard-Sicherheitsfunktionen	Standard-Sicherheitsfunktionen*	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit
Trennung von Fax und Netzwerk	✓	✓	✓	✓	✓	✓	✓	✓
Vertrauliches Fax	⊗	⊗	✓	✓	✓	✓	✓	✓
Junk-Filter	⊗	✓	✓	✓	✓	✓	✓	✓

Sicherheitsmanagement	BP-22C25 BP-C131WD BP-C131PW	MX-CxxxF/P MX-BxxxF/ W/P/PW	BP-30C25		MX-M1206 MX-M1056 MX-8081 MX-7081	BP-90Cxx BP-70/60/50/55Cxx BP-70/50Mxx BP-B547WD/B537WR BP-C5xxWD/WR		
	Standard-Sicherheitsfunktionen	Standard-Sicherheitsfunktionen*	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit	Standard-Sicherheitsfunktionen	mit installiertem Data Security Kit
Sharp Smart Security Service	✓	✓		✓	✓		✓	
Überwachung der Gerätesicherheit über SRDM	⊗	⊗		✓	✓		✓	
Viruserkennung dank Bitdefender	⊗	⊗		⊗	⊗		+	

Legende



Standard



Optional



Nicht vorhanden

* MX-B427W und MX-B427PW unterstützen nicht alle Funktionen. MX-C428P, MX-B468P und MX-B557P unterstützen keine MFP-bezogenen Sicherheitsfunktionen für Scans und Fax. Bitte informieren Sie sich in dem entsprechenden Datenblatt oder im Web.

Fachbegriffe | Glossar

Active Directory (AD)

Eine Datenbank und eine Reihe von Diensten, die Nutzer mit denjenigen Netzwerkressourcen verbinden, die sie für ihre Arbeit benötigen. Die Datenbank (oder das Verzeichnis (Directory)) enthält wichtige Informationen über die gesamte Umgebung, z. B. welche Nutzer und Computer es gibt und wer was tun darf. Insbesondere wird darüber in der Regel durch die Überprüfung einer eingegebenen Nutzer-ID und eines Kennworts sichergestellt, dass jede Person auch tatsächlich diejenige ist, die sie zu sein vorgibt (Authentifizierung), und sie nur auf die für sie freigegebenen Daten Zugriff hat (Autorisierung).

BIOS

In der Computertechnik ist das BIOS eine Firmware, die Laufzeitdienste für Betriebssysteme und Programme bereitstellt und die Initialisierung der Hardware während des Bootvorgangs durchführt.

Bitdefender Antivirus

Bitdefender ist eine preisgekrönte Anti-Malware-Engine, die den Benutzer vor einer ganzen Reihe von Cyberbedrohungen schützt. Sie ergänzt die nativen Sicherheitsfunktionen der Multifunktionssysteme und schützt vor bekannten und unbekanntem Malware-Bedrohungen wie Viren, Trojanern, Würmern, Ransomware, Spyware und persistenten Bedrohungen.

Data Security Kit

Das Sharp Data Security Kit hebt die Gerätesicherheit auf ein höheres Niveau mit Funktionen wie dem manuellen Überschreiben von Daten, dem automatischen Überschreiben von Daten beim Einschalten, dem Druck und der Erkennung von versteckten Mustern sowie vielem mehr. Damit ist es möglich, regulatorische Anforderungen zu erfüllen oder spezifische Bedrohungen zu entschärfen. Darüber hinaus sind ausgewählte MFP-Modelle mit einem TPM-Chip (siehe auch Seite 14) ausgestattet, der den unerwünschten Zugriff auf Datenspeicherbereiche, zu denen auch Festplattenlaufwerk (HDD) und Solid-State-Laufwerk (SSD) gehören, verhindert.

Denial of Service/Distributed Denial of Service (DoS/DDoS)

DoS ist eine Art von Störungsangriff, bei dem der normale Betrieb oder Dienst eines Netzwerks oder Geräts blockiert oder gestört wird. DDoS bezeichnet einen DoS-Angriff, bei dem mehrere (zahlreiche) angreifende Systeme eingesetzt werden, um den Netzwerkverkehr zu verstärken, wodurch die Zielsysteme oder -netze überflutet und möglicherweise überschwemmt werden.

End-of-Lease-Funktion

Wenn ein Multifunktionsdrucker ausgemustert wird, ist es wichtig, dass die im Gerät gespeicherten Daten entfernt oder in ein unlesbares Format gebracht werden. Sharp MFPs bieten standardmäßige End-of-Lease-Funktionen, um sicherzustellen, dass alle vertraulichen Daten überschrieben werden, bevor das Modell die Einrichtung oder die Kundenumgebung verlässt. Einmal gestartet, werden die Daten bis zu 10 Mal überschrieben. Wenn ein Sharp Data Security Kit installiert oder die Standard-MFP-Sicherheitsfunktion aktiviert ist, werden die Daten mit Zufallszahlen überschrieben.

IEEE802.1x

Ein Netzwerkauthentifizierungsprotokoll, das Ports für den Netzwerkzugang öffnet, wenn eine Organisation die Identität eines Nutzers authentifiziert und ihm den Zugang zum Netzwerk gestattet. Die Identität des Nutzers wird auf der Grundlage von Anmeldeinformationen oder eines Zertifikats festgestellt.

Internet Printing Protocol (IPP)

Ein Netzwerkdruckprotokoll, das die Authentifizierung und die Verwaltung von Druckauftragswarteschlangen ermöglicht. IPP wird von den meisten modernen Druckern und Multifunktionssystemen unterstützt und ist standardmäßig aktiviert.

Internet Protocol (IP) Adresse

Jedes Gerät, das mit dem Internet verbunden ist, muss eine eindeutige Nummer (IP-Adresse) haben, um mit anderen Geräten in Verbindung treten zu können. Derzeit gibt es zwei Versionen der IP-Adressierung: IPv4 und eine spätere aktualisierte Version namens IPv6.

Filterung von IP- oder MAC-Adressen

IP- und MAC-Adressen sind eindeutige Nummern, die zur Identifizierung von Geräten im Internet (IP) oder in einem lokalen Netzwerk (MAC) verwendet werden. Die Filterung stellt sicher, dass IP- und MAC-Adressen mit einer „Whitelist“ (siehe auch Seite 14) abgeglichen werden, bevor Geräte eine Verbindung zu Ihrem Netzwerk herstellen können.

Internet Protocol Security (IPSec)

Eine Reihe von Protokollen zur Sicherung der IP-Kommunikation auf der Netzwerkebene. IPSec umfasst auch Protokolle für die kryptografische Schlüsselherstellung.

Media Access Control (MAC) Adresse

Die MAC-Adresse eines Geräts ist eine eindeutige Kennung, die einem Network Interface Controller (NIC) zugewiesen wird. Das bedeutet, dass ein an das Netzwerk angeschlossenes Gerät anhand seiner MAC-Adresse eindeutig identifiziert werden kann.

Malware-Angriff

Bösartige Software (Malware) kann als unerwünschte Software bezeichnet werden, die ohne Ihre Zustimmung auf Ihrem System installiert wird. Sie kann sich an einen legitimen Code anhängen und sich verbreiten; sie kann sich aber auch in nützlichen Anwendungen verstecken oder sich über das Internet replizieren.

Man-in-the-Middle (MITM) Angriff

Bei einem MITM-Angriff setzt sich der Angreifer heimlich zwischen zwei Parteien, die glauben, dass sie direkt miteinander verbunden sind und privat miteinander kommunizieren. Der Angreifer „lauscht“ und kann auch die Kommunikation zwischen den Parteien verändern.

Netzwerkdienste

Netzwerkdienste erleichtern den Betrieb eines Netzwerks. Sie werden in der Regel von einem Server (auf dem ein oder mehrere Dienste laufen können) auf der Grundlage von Netzprotokollen bereitgestellt. Einige Beispiele sind Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) oder Voice over Internet Protocol (VoIP).

Phishing-Angriff

Phishing ist eine betrügerische Praxis, bei der E-Mails verschickt werden, die vorgeben, von seriösen Unternehmen zu stammen, um Einzelpersonen dazu zu bringen, persönliche Daten wie Passwörter und Kreditkartennummern preiszugeben.

Ports

Ports werden von vernetzten Geräten (PCs, Servern, Druckern, usw.) für die Kommunikation untereinander verwendet (z. B. ein Arbeitsplatzrechner, der sich mit einem Drucker verbindet). Unbewachte offene Ports und Dienste können von Angreifern genutzt werden, um z. B. Malware hochzuladen.

Protocols (Protokolle)

Ein Protokoll ist definiert als eine Reihe von Regeln und Formaten, die es Informationssystemen ermöglichen, Informationen auszutauschen. In einem Netzwerkkontext gibt es zum Beispiel die Protokolle IP und TLS/SSL.

Single Sign-On (SSO, Einmalanmeldung)

Ausgewählte Sharp MFPs bieten Optionen für Single Sign-On, um die Bedienung zu vereinfachen und gleichzeitig den Nutzerzugriff auf den Multifunktionsdrucker und das Netzwerk zu validieren. Wenn ein MFP einer Domain beiträgt, baut das MFP vertrauenswürdige Verbindungen zu Netzwerkressourcen auf. IT-Administratoren können sichere, auf Token basierende Kerberos SSO für Netzwerk- und Privatorbiter sowie Microsoft® Exchange Server bereitstellen. Für den Online-Speicherdienst Google Drive™, den Webmail-Dienst Gmail™ und ausgewählte Cloud-Dienste wird ein OAuth-Token zur Einrichtung von SSO verwendet.

Secure/Multipurpose Internet Mail Extensions (S/MIME)

Eine Reihe von Spezifikationen für die Sicherung von E-Mails. S/MIME basiert auf dem weit verbreiteten MIME-Standard und beschreibt ein Protokoll zur Erhöhung der Sicherheit durch digitale Signaturen und Verschlüsselung.

Spoofing-Angriff

Bei einem Spoofing-Angriff gibt sich eine Partei als ein anderes Gerät oder ein anderer Nutzer in einem Netzwerk aus, um Angriffe auf Netzwerkhosts zu starten, Daten zu stehlen, Malware zu verbreiten oder Zugangskontrollen zu umgehen.

Transport Layer Security/Secure Sockets Layer (TLS/SSL)

Eine Technologie, die Daten verschlüsselt, wenn sie zwischen zwei Geräten transportiert oder übertragen werden, um ein Abhören bzw. einen Fremdzugriff zu verhindern. TLS/SSL wird häufig für Websites verwendet, kann aber auch zum Schutz anderer Dienste eingesetzt werden.

Trusted Platform Module (TPM)

Ein Computerchip nach Industriestandard, der die Kryptoprozessortechnologie nutzt, um Hardware wie Festplattenlaufwerke und Solid State-Laufwerke in MFPs und Druckern zu schützen. Wenn ein Sharp Multifunktionsdrucker mit einem Datensicherheitskit oder TPM installiert wird, initiiert der TPM-Chip einen kryptografischen Schlüssel, auf den die Software nicht zugreifen kann. Ein passender kryptografischer Schlüssel wird während des Bootvorgangs kodiert. Wenn die beiden Schlüssel nicht übereinstimmen, wird der Zugriff auf das Gerät verweigert.

Whitelist

Eine Whitelist ist eine Liste von ausgewählten Personen, Einrichtungen, Anwendungen oder Prozessen, denen besondere Berechtigungen oder Zugriffsrechte erteilt werden. Im geschäftlichen Sinne könnte es sich dabei beispielsweise um die Mitarbeitenden einer Organisation und ihre Rechte für den Zugriff auf das Gebäude, das Netzwerk und ihre Computer handeln. In einem Netzwerk oder Computer kann eine Whitelist Anwendungen und Prozesse definieren, die das Recht haben, auf Datenspeicher in sicheren Bereichen zuzugreifen.



Sicher? Sicher. Sharp.

Jedes Unternehmen ist einzigartig und steht vor besonderen Herausforderungen. Daher sollten auch Ihre Sicherheitssysteme optimal auf Sie angepasst sein. Der Sicherung der Druckinfrastruktur kommt heute eine zentrale Bedeutung zu, allerdings sollte auch ein einfacher Zugang zum Drucken für die Produktivität des Unternehmens sichergestellt sein. Um diese beiden Pole bestmöglich zu verbinden, bieten wir eine Analyse der Drucklandschaft sowie Trainings durch unsere Spezialisten an.

Vor diesem Hintergrund hat Sharp auch den Smart Security Service eingeführt – ein innovatives Leistungsangebot, das Sicherheit „as a Service“ definiert. Dabei handelt es sich um einen maßgeschneiderten Profiling-Dienst, der entwickelt wurde, um zu gewährleisten, dass Ihre Sharp MFPs sofort sicher sind und über fortschrittliche, sorgfältig auf Ihre Bedürfnisse zugeschnittene Sicherheitsfunktionen verfügen, sodass Ihre geschäftliche Agilität und Produktivität nicht beeinträchtigt wird.

Zunächst gehen wir mit Ihnen die aktuellen und potenziellen Datenbedrohungen in Hinblick auf MFPs durch, damit wir eine geeignete Drucksicherheitsrichtlinie für Sie festlegen können. Unsere Sicherheitsexperten entwickeln dann eine individuelle

Sicherheitskonfiguration für Ihre MFPs, die genau auf die Anforderungen Ihres Unternehmens zugeschnitten ist, indem sie alle relevanten Sicherheitseinstellungen aus über 200 Voreinstellungen aktivieren.

Das führt dazu, dass wir das bestmögliche Maß an Drucksicherheit bieten, ohne die Flexibilität einzuschränken, die Sie und Ihre Angestellten im Arbeitsalltag benötigen. Es bedeutet auch, dass wir Ihre neuen MFPs so einfach und sicher wie möglich vorkonfigurieren, liefern, installieren und integrieren. So können Sie sich vom ersten gedruckten Blatt an darauf verlassen, dass Ihre Systeme und Informationen so sicher wie aktuell möglich sind.

**SHARP BUSINESS SYSTEMS
DEUTSCHLAND GMBH**

Industriestraße 180, D-50999 Köln
Tel.: +49 2236 323 100
www.sharp.de

**Sharp Electronics Europe GmbH
Zweigniederlassung Österreich**

Handelskai 342, A-1020 Wien
Tel.: +43 1 727 19-0
www.sharp.at

SHARP ELECTRONICS (SCHWEIZ) AG

Moosstrasse 2a, CH-8803 Rüschlikon
Tel.: +41 44 846 61 11
www.sharp.ch

Sharp Europe | DACH

Sharp Europe ermöglicht es KMU und großen Unternehmen und Organisationen in ganz Europa, ihre Leistung zu steigern und sich durch eine Reihe von Business-Technologie-Produkten und -Dienstleistungen an den Arbeitsplatz der Zukunft anzupassen. Mit Hauptsitz in London, bedient Sharp in Europa Kunden aus dem privaten und öffentlichen Sektor, dem Bildungswesen und der Regierung. Sharp bietet ein Portfolio, das von Desktop-Druckern über Multifunktionsdrucker, interaktive Monitore und Displays, bis hin zu IT-Dienstleistungen reicht.

Als Teil der Sharp Corporation und mit der Unterstützung von Foxconn, investiert Sharp Europe in neue Technologiebereiche, die das Potenzial haben, die Welt zu verändern, und geht damit in der Branche mit gutem Beispiel voran. Seit der Gründung im Jahre 1912 sorgt das Unternehmen kontinuierlich für Innovationen in zahlreichen Produktkategorien.

In der DACH-Region ist Sharp Teil der Sharp Europe und somit auch Teil der Sharp Corporation. Mit weltweit mehr als 46.000 Mitarbeitenden ist Sharp der Experte für Innovationen im Bereich Business-to-Business und Consumer.

Stand: 06/24, Update: 1/25 | M30 Security-Guide-V01-25

Hinweise: Design und technische Daten können ohne vorherige Ankündigung geändert werden. Alle Informationen waren zum Zeitpunkt der Drucklegung korrekt. Sharp, Synappx und alle damit verbundenen Marken sind Marken oder eingetragene Marken der Sharp Corporation und/oder ihrer angeschlossenen Unternehmen. Microsoft, Microsoft Teams, OneDrive und SharePoint sind Marken der Microsoft-Unternehmensgruppe. Android und Google sind Warenzeichen von Google LLC. AirPrint ist eine in den USA und anderen Ländern und Regionen eingetragene Marke von Apple Inc. Alle anderen Firmennamen, Produktnamen und Logos sind Marken oder eingetragene Marken der jeweiligen Eigentümer. ©Sharp Corporation. Alle Marken werden anerkannt. E&O.

SHARP
Be Original.