# Datensicherheit

Report | Lösungsansätze für KMU

SHARP

Be Original.

# Einleitung

## An den meisten Arbeitsplätzen sind Drucker oder Multifunktionsdrucker (MFPs) ein fester Bestandteil.

Täglich werden sie routinemäßig genutzt und scheinen sich rein äußerlich innerhalb der letzten zehn oder sogar 20 Jahre kaum verändert zu haben. Wie IT-Administratoren jedoch wissen, haben sich MFPs in ihrem Inneren zu hochentwickelten Computersystemen entwickelt, die mit ihrem Unternehmensnetzwerk und dem Internet verbunden sind.

Obwohl in Europa neun von zehn Büroangestellten Drucker oder MFPs nicht als Sicherheitsrisiko einstufen, sind sie für Hacker ebenso ein Ziel wie ein Laptop oder ein PC. Sie müssen mithilfe von Technologie und sicherem Benutzerverhalten geschützt werden.

Als Druckerhersteller steht Sicherheit also im Zentrum unserer Produktentwicklung. Wir möchten, dass unsere Produkte und Dienstleistungen das Arbeitsleben der Menschen erleichtern und produktiver gestalten und gleichzeitig die Datensicherheit gewährleisten.

Wir wollten in Erfahrung bringen, welche Einstellung Büroangestellte in Bezug auf Druckersicherheit haben. Betrachten Personen außerhalb unserer Branche sie als potenzielles Problem oder Risiko?

Dazu haben wir über 5.500 Büroangestellte in kleinen und mittelständischen Unternehmen (KMU) in Europa befragt und festgestellt, dass fast die Hälfte der Befragten nicht wusste, dass es überhaupt möglich ist, einen Drucker zu hacken.

Außerdem ergaben unsere Untersuchungen einen deutlichen Mangel an formalen Schulungen und Beratungen in Bezug auf die Datensicherheit bei Druckern und MFPs. Wir möchten dazu beitragen, diese Wissenslücke durch technische Ratschläge, Whitepapers auf unserer Website und durch diesen Report, der vom „ethischer Hacker“ Jens Müller erstellt wurde, zu schließen.

Dieser Report enthält eine Momentaufnahme des Druckverhaltens von Büros in Europa und einige leicht zu befolgende Sicherheitstipps für die Verantwortlichen für Bürotechnik in KMU. Zudem zeigen wir Ihnen auf, wie Sie mit Sharp Produkten die Sicherheitslücken in Ihrem Unternehmen schließen können.

Die Untersuchung für diesen Report wurde von Censuswide für Sharp durchgeführt. Befragt wurden 5.514 Büroangestellte in Unternehmen mit 10 bis 250 Beschäftigten aus sieben europäischen Ländern: Großbritannien, Deutschland, Frankreich, Italien, den Niederlanden, Schweden und Polen.

Wir hoffen, dass Ihnen diese Informationen nützlich erscheinen und begrüßen Ihre Gedanken oder Erfahrungen zu den größten Hürden, denen Sie beim Schutz Ihrer Daten gegenüberstehen.

Peter Plested,
Director Information Systems
Sharp Electronics Europe

# Ist Ihr Netzwerk sicher?

## Ist Ihnen bewusst, dass es unwahrscheinlich ist, dass kleinere Unternehmen über Druckersicherheitsfunktionen verfügen?

62 % der Beschäftigten in Unternehmen mit weniger als 49 Mitarbeitern geben an, dass jeder von ihnen einen Drucker oder ein MFP verwenden kann. Bei Unternehmen mit 151 bis 250 Beschäftigten sinkt dieser Wert auf 43 %.

Das Risiko, den Druckerzugriff nicht zu kontrollieren, reicht von Malware, die absichtlich oder unbeabsichtigt über den Drucker in das Netzwerk geladen wird, bis zum Verlust vertraulicher Daten, die als Ausdrucke im Drucker-Ausgabefach verbleiben.

### Untersuchungsergebnisse

**10 %**

Lediglich 10 % der Büroangestellten haben festgestellt, dass Drucker oder Multifunktionsprodukte ein Sicherheitsrisiko an ihrem Arbeitsplatz darstellen.

**21 %**

21 % der Büroangestellten gaben an, an ihrem Arbeitsplatz über keinerlei Sicherheitsprozesse für Drucker oder MFPs zu verfügen.

**25 %**

25 % der Büroangestellten sagten, vertrauliche oder persönliche Informationen im Ausgabefach des Druckers gefunden zu haben, die nicht für sie bestimmt waren – was eine Verletzung des Datenschutzes bedeuten kann.

**28 %**

28 % der Büroangestellten haben schon einmal einen Arbeitsplatzdrucker zum Drucken eines persönlichen Dokuments verwendet, das sie außerhalb der Sicherheitsumgebung des Unternehmens erstellt hatten.

**14 %**

14 % haben mit dem Bürodrucker schon mal ein Dokument gedruckt, das heruntergeladen wurde – trotz der Warnung, dass diese Datei ggf. unsicher und das Unternehmensnetzwerk einer potenziellen Bedrohung aussetzt ist.

# Die Einschätzung eines Experten.

## Der „ethische Hacker“ Jens Müller überprüfte die Auswirkungen von Sharps Untersuchungsergebnissen und die potenziellen Risiken für die Datensicherheit der KMU, die von Druckern und MFPs ausgehen.

Sharps Studie ergab, dass neun von zehn europäischen Büroangestellten ihren Drucker oder ihr MFP nicht als ein potenzielles Sicherheitsrisiko für ihr Unternehmen betrachten. Warum sollte jemand den Drucker oder das MFP eines Unternehmens hacken wollen? Wie profitabel wäre das?

Erstens gibt es Drucker überall. Jedes Unternehmen besitzt mindestens einen. Sie sind mit dem Netzwerk verbunden und können von Hackern leicht angegriffen werden, wenn sie nicht sicher sind. Zweitens können Drucker und MFPs wertvolle Informationen enthalten, wodurch die Motivation entsprechend groß ist, sich in einen Drucker zu hacken.

Unternehmen sollten sich fragen, wie wertvoll die Informationen sind, die sie drucken und scannen. In einer Zeit, in der Unternehmen nach der Allgemeinen Datenschutzgrundverordnung (DSGVO) dazu verpflichtet sind, personenbezogene Daten zu schützen, über die sie verfügen, könnten Drucker oder MFPs eine kostspielige Schwachstelle darstellen.

In der Regel gibt es zwei Arten von Hackern. Das sind zum einen Kinder, die Spaß haben wollen und ihre Hacking-Fähigkeiten aus Neugier testen, und zum anderen „finstere Gestalten“, deren Ziel die Unternehmensspionage ist.

Obwohl wir derzeit nicht wissen, wie groß das Problem von Sicherheitsverletzungen durch Drucker und MFPs derzeit ist, wissen wir, dass Zehntausende von Druckern für Hacker verfügbar sind, sodass das potenzielle Problem sehr groß ist. Es wäre ein Fehler zu glauben, dass es sich hierbei lediglich um ein Problem für größere Konzerne handelt, da KMU genauso anfällig sind. Das gilt besonders dann, wenn ihre Arbeit von Interesse für Kriminelle ist, die von einem Diebstahl ihrer Daten oder einer Störung ihres Geschäfts profitieren könnten, wie beispielsweise Zulieferer von staatlichen, wie bspw. sicherheitsrelevanten Organisationen. Wie die Sharp-Studie hervorhebt, ist das insofern problematisch, dass kleinere Unternehmen im Vergleich zu Unternehmensorganisationen, weniger Möglichkeiten besitzen und mit geringeren Ressourcen ausgestattet sind, die Cybersicherheit

in Angriff zu nehmen. Aus diesem Grund ist es wichtig, das Personal zu schulen. KMU müssen ihre Mitarbeiter auf dieselbe Weise über die Sicherheitsrisiken von Druckern und MFPs – und darüber wie sie diese mindern können – informieren, wie über wichtige Sicherheitsbedrohungen wie Phising. Und doch wissen wir, dass 40 % der Büro-angestellten in Europa noch nie eine Schulung oder Beratung zum sicheren Drucken erhalten haben.

### Wo liegen die Risiken?

Drucker und MFPs bieten nicht nur Zugriff auf vertrauliche gedruckte, gescannte und gefaxte Dokumente, es besteht außerdem die Gefahr, dass Drucker missbraucht werden, um in das Netzwerk eines Unternehmens einzudringen oder verteilte Überlastangriffe (DDoS) auszuführen. Das zeigten uns im Jahr 2016 die Bot-Netze von Mirai, die Geräte auf der ganzen Welt – einschließlich Drucker – kompromittierten und den größten DDoS-Angriff in der Geschichte durchführten. Hacker suchen immer nach dem schwächsten Glied und das könnte der Drucker sein.

Wenn der Drucker oder das MFP kein sicheres Kennwort hat, dann ist das ein Problem. Wir wissen außerdem, dass europaweit mehr als die Hälfte (52 %) der Büroangestellten angibt, dass keine Authentifizierung erforderlich ist, um Funktionen ihres Druckers oder MFPs zu nutzen. Ältere Geräte können anfälliger sein, da ihre Sicherheit nicht auf dem neuesten Stand ist, ähnlich wie alte Windows-Geräte häufig Zugang für Viren oder Cyberangriffe ermöglichen. Die Schwachstellen veralteter Software wurden im Mai 2017 durch den großen Cyberangriff mit WannaCry dramatisch hervorgehoben, und diese Risiken gelten ebenso für Drucker.

Wie schützt sich ein KMU vor einer Sicherheitsanfälligkeit durch Drucker oder MFPs? Nun, Verteidigung ist schwieriger als Angriff. Hacker müssen lediglich ***einen*** Weg finden, während der IT-Manager (oder wer auch immer die Verantwortung für die IT in einem Unternehmen übernimmt) über ***jede*** mögliche Schwäche nachdenken muss. Sicherheit bedeutet wiederkehrende Kosten für den Administrator, was wahrscheinlich erklärt, warum dieser Punkt in der Prioritätenliste weit unten steht. Außerdem fällt es schwer, Investitionen in etwas zu priorisieren, das eigentlich funktioniert und seine Kernaufgabe (d.h. Dokumente drucken oder scannen) gut erledigt.

### Es geht nicht nur ums Drucken.

Auch der Scanner kann eine Schwachstelle darstellen, und gescannte Dokumente können leicht zu einem Hacker durchsickern. Unternehmen sollten die Verschlüsselung von PDF-Dokumenten in Betracht ziehen und prüfen, ob ihre vom MFP gesendeten E-Mail-Scans sicher sind.

Der Fokus liegt natürlich besonders stark auf Daten – aber Datensicherheits-Beauftragte dürfen auf keinen Fall die „analoge“ Bedrohung durch Informationen auf Papier übersehen. In der Vergangenheit haben Hacker sensible Informationen im Müll gefunden. Der Zugriff auf den Drucker und eventuell im Ausgabefach des Druckers verbliebene Ausdrucke ist leicht, da sie sich häufig in offenen Bereichen des Büros befinden und abteilungsübergreifend genutzt werden.

Obwohl die Risiken überwältigend erscheinen können, ist es einfacher die Druckersicherheit im Auge zu behalten, als Sie vielleicht annehmen. Es gibt einfache Möglichkeiten, um Risiken zu minimieren, und die meisten erfordern, abgesehen von Ihrer Zeit keine zusätzlichen Investitionen. Lesen Sie dazu auf den folgenden Seiten meine „Tipps zur Druckersicherheit“ für IT-Administratoren oder Verantwortliche für Bürotechnik.

Jens Müller

# Tipps zur Druckersicherheit.

## Diese Tipps beziehen sich auf alle Drucker oder MFPs, die in Ihrem Firmennetzwerk eingebunden sind.

Einige beziehen sich auf Einstellungen, die Sie selbst als Administrator ändern können, andere erfordern möglicherweise, dass Sie sich an das Unternehmen wenden, das Ihren Drucker geliefert hat oder wartet.

### Ändern Sie die Standardkennwörter

Lassen Sie nicht zu, dass Hacker die Kontrolle über Ihren Drucker übernehmen. Richten Sie unmittelbar nach dem Einrichten Ihres Geräts ein sicheres Kennwort für die Webseite des Administrationsbedienfelds ein. Drucker werden üblicherweise mit einem Standardkennwort bereitgestellt, das öffentlich verfügbar und Hackern daher bekannt ist. Aus diesem Grund müssen IT-Administratoren für jeden Drucker in Ihrem Büro ein Kennwort festlegen.

### Benutzerauthentifizierung

Stellen Sie sicher, dass Ihr MFP nur Druckaufträge von autorisiertem Personal akzeptiert. Richten Sie es so ein, dass Benutzer sich authentifizieren ***müssen***, bevor sie Dokumente ausdrucken können. Die Benutzerauthentifizierung kann im Konfigurationsmenü des Druckers aktiviert werden. Die Zugriffsbeschränkung für Whitelist-Nutzer sollte für Ihre Sicherheitsstrategie von zentraler Bedeutung sein, um Angreifer auszuschließen und somit unerwünschte Ausdrucke und komplexere Angriffe zu verhindern.

### Keine Umgehung

Stellen Sie sicher, dass eine andere Möglichkeit zum Drucken besteht. Umgehen Sie hierfür nicht die Zugriffskontrollen, sondern stellen Sie Gästen eine andere Möglichkeit zum Drucken bereit, z. B. WLAN oder eine zweite Netzwerkkarte.

### Deaktivieren Sie nicht benötigte Dienste und Netzwekprotokolle

Führen Sie nur das aus, was Sie wirklich benötigen. Deaktivieren Sie alle anderen Netzwerk- und lokalen Druckdienste, um das Risiko durch Angriffe zu minimieren. Wenn Sie herausgefunden haben, welche Protokolle in Ihrem Setup wirklich verwendet werden, deaktivieren Sie alle anderen nicht benötigten Dienste. Drucken Sie beispielsweise über IPP, muss der Raw-Port-9100-Druckdienst nicht geöffnet bleiben. Drucken Sie lediglich über LAN, muss der Drucker nicht als WiFi/Airprint-Hotspot fungieren.

### Netzwerksicherheit

Das Internet kann ein gefährlicher Ort sein. Stellen Sie sicher, dass Ihre Drucker dem öffentlichen Internet nicht direkt ausgesetzt sind, um unerwünschte Ausdrucke zu verhindern und die Möglichkeiten für komplexere Angriffe einzuschränken. Obwohl es so offensichtlich klingt, gibt es derzeit Zehntausende von Druckern, die direkt über öffentlich weitergeleitete IP-Adressen erreichbar sind. Mithilfe der IP- oder MAC-Adressfilterung können Sie die Sicherheit Ihres internen Netzwerks weiter verbessern.

### Physische Sicherheit

Für nicht autorisierte Benutzer ist der physische Zugriff auf Drucker und Multifunktionsgeräte einfacher als der Zugriff auf Server oder Workstations. Das Starten eines böswilligen Druckauftrags von einem USB-Port kann nur wenige Sekunden dauern. Kontrolle durch Authentifizierung oder die Deaktivierung aller physischen Ports können als Gegenmaßnahme behilflich sein. Hierunter fallen beispielsweise nicht autorisiertes Drucken über USB (Vorderseite), Parallel- oder USB-Kabel (Rückseite), NFC und Bluetooth.

Stellen Sie keine Drucker an öffentlichen Orten auf und stellen Sie sicher, dass die Druckerwartung nur von autorisiertem Personal durchgeführt wird, und schulen Sie Ihre Mitarbeiter darin, sich verdächtigen oder unbekannten Personen zu nähern. Lassen Sie keine vertraulichen Dokumente im Ausgabefach des Druckers liegen. Aktivieren Sie die sichere Druckfreigabe (manchmal auch als „Pull Printing“, „Follow Me Secure Print“ oder „Pick up Protection“ bezeichnet) basierend auf PINs oder ID-Karten, um das Dokument zu genehmigen.

### Firmware-Aktualisierungen

In den letzten zehn Jahren haben sich Drucker von mechanischen Geräten mit Mikrochips zu vollwertigen Computersystemen entwickelt. Aus diesem Grund ist es wichtig, sie wie andere Komponenten in Ihrem IT-System zu behandeln: Stellen Sie stets sicher, dass Sie über die neuesten Sicherheitspatches und Firmware-Updates verfügen. Die neueste Version ist die stabilste und sicherste. Sie garantiert, dass die neuesten Sicherheitsfunktionen und Schutzmechanismen ausgeführt werden. Vereinbaren Sie einen festen, regelmäßigen Termin, um Firmware-Updates durchzuführen – oder tun Sie es immer dann, wenn sie bei Ihrem Service-Dienstleister erhältlich sind.

### Monitoring aktivieren

Was passiert, wenn Sie einen Verstoß oder verdächtige Aktivitäten im Netzwerk Ihrer Organisation festgestellt haben? In Protokolldateien können Informationen darüber enthalten sein, was genau passiert ist. Außerdem können digitale Belege über Angriffe wie böswillige Druckaufträge aufbewahrt werden (Benutzerauthentifizierung aktivieren). IT-Administratoren können E-Mail-Benachrichtigungen aktivieren, um sich über kritische Probleme und Sicherheitsverletzungen zu informieren.

### Sichere Entsorgung

Schmeißen Sie Drucker nicht einfach weg. Vergangene Sicherheitsverletzungen traten auf, weil Hacker sich ausrangierte Drucker und somit Zugriff auf deren Festplatten oder den nichtflüchtigen Speicher (NVRAM) verschafften. Wurde das Gerät in das Netzwerk der Organisation integriert, enthält es möglicherweise vertrauliche Daten. Stellen Sie bei der Außerbetriebnahme sicher, dass Speicher oder Festplatte gelöscht sind. Soll das Gerät an das Unternehmen zurückgegeben werden, bei dem Sie es bezogen haben, stellen Sie mithilfe der End-of-Lease-Funktionen sicher, dass alle vertraulichen Daten überschrieben werden, bevor das Gerät Ihr Unternehmen verlässt.

### Aktivieren Sie die Verschlüsselung

Ihre Daten sind wertvoll. Sind diese nicht verschlüsselt, wird jedes Dokument, das auf einem Netzwerkdrucker gedruckt wird, im Klartext über das Netzwerk übertragen. So kann jeder „in der Mitte“ auf Druckaufträge zugreifen. Um die Verschlüsselung während der Übertragung zu aktivieren, gibt es für IT-Administratoren grundsätzlich zwei Möglichkeiten: Transport Layer Encryption (TLS / SSL) und IPSec. Diese Verschlüsselungsprotokolle verschlüsseln den gesamten Netzwerkverkehr.

Müssen Sie vertrauliche Dateien wie gescannte Dokumente über unsichere Kanäle versenden, verwenden Sie die End-to-End-E-Mail-Verschlüsselung S/MIME, die auf Zertifikaten basiert oder eine PDF-Verschlüsselung mit sicherem Kennwort. Aktivieren Sie die Festplattenverschlüsselung und das sichere Löschen des Druckers, um die sichere Speicherung von Dokumenten auf dem Drucker oder dem MFP zu gewährleisten.

# Fachbegriffe

**Authentifizierung**
Eindeutige Identifikation, in der Regel durch zwei Informationen wie Benutzername und Passwort.

**DoS/DDoS**
Ein Denial of Service (DoS) ist eine Art von störendem Angriff, bei dem der normale Betrieb oder Dienst, der von einem Netzwerk oder Gerät bereitgestellt wird, blockiert oder gestört wird. Ein Distributed Denial of Service (DDoS) ist eine Art von DoS-Angriff, bei dem mehrere (zahlreiche) Angriffssysteme verwendet werden, um den Netzwerkverkehr zu verstärken, wodurch die Zielsysteme oder Netzwerke überflutet und möglicherweise überlastet werden.

**Internet Printing Protocol (IPP)**
Ein Netzwerkdruckprotokoll zur Authentifizierung und Verwaltung von Druckaufträgen. IPP wird von den meisten modernen Druckern und MFPs standardmäßig unterstützt und aktiviert.

**IP-Adressen**
Jedes mit dem lokalen Netzwerk verbundene Gerät muss eine eindeutige Nummer (IP-Adresse) haben, um eine Verbindung mit anderen Geräten herstellen zu können und bietet den Vorteil einer verschlüsselten Druckdatenübertragung. Derzeit gibt es zwei Versionen der IP-Adressierung: IPv4 und eine später aktualisierte Version namens IPv6.

**IP- oder MAC-Adressfilterung**
IP- und MAC-Adressen sind eindeutige nummerische bzw. alphanummerische Kennungen, mit denen Geräte im Internet (IP) oder in einem lokalen Netzwerk (LAN) identifiziert werden. Durch das Filtern wird sichergestellt, dass IP- und MAC-Adressen anhand einer Whitelist überprüft werden, bevor Geräte eine Verbindung zu Ihrem Netzwerk herstellen können.

**IPsec (Internet Protocol Security)**
Eine Reihe von Protokollen zur Sicherung der IP-Kommunikation (Internet Protocol) auf Netzwerkebene. IPsec enthält auch Protokolle für die Einrichtung von Chiffrierschlüsseln.

**MAC-Adressen**
Die Media Access Control-Adresse (MAC-Adresse) eines Geräts ist eine eindeutige Kennung, die einer Netzwerkkarte zugewiesen wird. Das bedeutet, dass ein mit dem Netzwerk verbundenes Gerät anhand seiner MAC-Adresse eindeutig identifiziert werden kann.

**Malware-Angriff**
Schädliche Software (Malware) kann als unerwünschte Software bezeichnet werden, die ohne Ihre Zustimmung auf Ihrem System installiert ist. Sie kann sich an einen legitimen Code anhängen und sich verbreiten. Sie kann in nützlichen Anwendungen lauern oder sich selbst über das Internet replizieren.

**Man-in-the-Middle-Angriff**
Bei einem Man-in-the-Middle-Angriff (MITM) sitzt der Angreifer unbemerkt zwischen zwei Systemen im Netzwerk, die glauben, direkt miteinander verbunden zu sein und privat miteinander zu kommunizieren. Der Angreifer lauscht und kann die Kommunikation zwischen den Parteien auch verändern.

**Netzwerkdienste**
Netzwerkdienste ermöglichen die Kommunikation in einem Netzwerk zwischen den jeweiligen Systemen und Rechnern in einem Netzwerk. Sie werden in der Regel von einem Server bereitgestellt (auf dem ein oder mehrere Dienste ausgeführt werden können), der auf Netzwerkprotokollen basiert. Beispiele hierfür wären DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol) und VoIP (Voice over Internet Protocol).

**Phishingangriff**
Phishing ist das betrügerische Versenden von E-Mails, die angeblich von seriösen Unternehmen stammen, um Personen zur Offenlegung persönlicher Informationen wie Passwörtern und Kreditkartennummern zu veranlassen.

**Ports**
Ports werden von vernetzten Geräten (PCs, Servern, Druckern usw.) zur Kommunikation miteinander verwendet (z. B. eine Workstation, die mit einem Drucker verbunden ist). Unbeaufsichtigte offene Ports und Dienste können als Angriffsvektor verwendet werden, um beispielsweise Malware hochzuladen.

**Protokolle**
Ein Protokoll ist als eine Reihe von Regeln und Formaten definiert, die es Informationssystemen ermöglichen, Informationen auszutauschen. Im Kontext eines Netzwerks wären das zum Beispiel IP und TLS / SSL Protokolle.

**S/MIME (Secure / Multipurpose Internet Mail Extensions)**
Eine Reihe von Spezifikationen zum Sichern von E-Mails. Secure/Multipurpose Internet Mail Extensions (S/MIME) basieren auf dem weit verbreiteten MIME-Standard und beschreiben ein Protokoll zur Erhöhung der Sicherheit durch digitale Signaturen und Verschlüsselung.

**Spoofing-Angriff**
Ein Spoofing-Angriff bedeutet, dass eine böswillige Partei sich in einem Netzwerk als ein anderes Gerät oder ein anderer Benutzer ausgibt, um Angriffe auf Netzwerkhosts zu starten, Daten zu stehlen, Malware zu verbreiten oder Zugriffskontrollen zu umgehen.

**Transport Layer Security (TLS / SSL)**
Eine Technologie, die Daten verschlüsselt, wenn sie zwischen Geräten transportiert oder übertragen werden, um das Abhören zu verhindern. TLS / SSL ist besonders bei Websites üblich, kann aber auch zum Schutz anderer Dienste verwendet werden.

**Whitelist**
Eine Whitelist ist eine exklusive Liste von Personen, Entitäten, Anwendungen oder Prozessen, denen besondere Berechtigungen oder Zugriffsrechte erteilt wurden. Im geschäftlichen Sinne können das beispielsweise die Mitarbeiter einer Organisation und ihre Zugriffsrechte auf das Gebäude, das Netzwerk und ihre Computer sein. In Bezug auf Netzwerk oder Computer kann eine Whitelist Anwendungen und Prozesse definieren, welche die Rechte zum Zugriff auf Datenspeicher in sicheren Bereichen haben.

# Sharps Sicherheitsfunktionen

## Sharps MFPs sind geschützt. Sind Ihre das auch?

Sharp bietet eine Reihe integrierter Sicherheitsfunktionen, um die Informationen und Dokumente von Unternehmen vor einer Vielzahl von Bedrohungen zu schützen. Die neuesten A3-MFP- und A4-MFP -Reihen von Sharp sind die bisher sichersten. Zu diesen Geräten gehören:

**A3-Modelle**

- MX-6071 / MX-5071 / MX-4071/ MX-3571 / MX-3071
- MX-6051 / MX-5051 / MX-4051 / MX-3551 / MX-3051
- MX-4061 / MX-3561 / MX-3061
- MX-2651

**A4-Modelle**

- MX-C304W / MX-C303W
- MX-B456W / MX-B356W

Sharp bietet einen einzigartigen 360-Grad-Sicherheitsansatz, mit dem KMU die Möglichkeit erhalten, ihre Druckrichtlinien zu steuern und zu verwalten und ihre vertraulichen Informationen zu schützen. Und zwar unabhängig davon, ob sie über ihr Netzwerk gedruckt, kopiert, gescannt, gefaxt, oder als Daten über das MFP gespeichert oder freigegeben werden.


Von der Netzwerksicherheit – die alle Unternehmensnetzwerke und alle angeschlossenen Peripheriegeräte abdeckt – über die Ausgabesicherheit zur Kontrolle und Verfolgung des Zugriffs bis hin zur Dokumentensicherheit, die sowohl digitale als auch physische Dokumente schützt: Sharp hat die richtige Lösung für Sie.

Um Ihre Sicherheitsanforderungen detaillierter zu besprechen, kontaktieren Sie uns bitte. Wir beraten Sie auch zu den Themen:

- Netzwerksicherheit
- Ausgabe-Sicherheit
- Dokumentensicherheit
- DSGVO Compliance

Dieser umfassende Sicherheitsansatz gewährleistet, dass Ihre Organisation auch von den neuesten Sicherheitsbestimmungen, einschließlich der Allgemeinen Datenschutzverordnung (DSGVO) profitiert.

Alle modernen Sharp MFPs können bereits ab Werk die Empfehlungen des BSI in Bezug auf Sicherheit für Drucker, Scanner, Faxgeräte und MFPs in Unternehmensnetzwerken erfüllen. Selbst die hohen Anforderungen nach Common Criteria HCD/PP V1.0 sind optional erfüllbar. Kontaktieren Sie hierzu bitte Ihren Sharp Berater.

# Wiederkehrende Fragen an Sharp:

**Warum sollte ich mir Sorgen über die Sicherheit meines Druckers oder meines MFPs machen? Ich habe noch nie von diesem Problem gehört.**
Gerade ein fehlendes Bewusstsein zur Drucker-Sicherheit kann zu Problemen führen. Schlecht verwaltete MFPs und Drucker im Netzwerk sind häufig die Ursache für Datendiebstahl und sehr attraktiv für Hacker, welche besonders auch gegen KMU immer wieder Angriffe versuchen.

**Ich weiss, dass es Sachen gibt, die ich machen kann, oder Dienste angeboten werden, die ich beauftragen kann – aber ich kann mir das nicht leisten!**
Tatsächlich kostet es viel weniger, Sicherheitsmaßnahmen umzusetzen, als die Kosten für einen Datenverstoß oder den Verlust des Unternehmens zu tragen. Viele der Sicherheitsfunktionen von Sharp funktionieren entweder ohne zusätzliche Einstellung ab Werk oder benötigen nur einen minimalen Aufwand für die Einrichtung.

**Warum ist Sharp besser? Jeder spricht über Sicherheit – also kann auch jedes Druckausgabesystem sicher gemacht werden, oder nicht? Warum sollte ich mich also mit Sharp unterhalten?**
Sharp war der erste Hersteller von Multifunktionssystemen (MFP) und Druckern, der auf das Thema Sicherheit im digitalen Imaging eingegangen ist. Sharp hat die erste Common Criteria-Validierung für ein MFP im Jahr 2001 erhalten und wurde als Erster mit einem EAL4-Rating für ein Data Security Kit ausgezeichnet.

Unsere Systeme entsprechen den strengsten Sicherheitsanforderungen, unter anderem dem HCD/PP V1.0-Standard – der modernsten Sicherheitsvalidierung für Regierungs- und Militärorganisationen. Auch hier waren wir Vorreiter.

**Ich denke, dass ich da ganz gut aufgestellt bin. Ich kenne mich in Sachen Drucker-Sicherheit aus. Wir schreddern Unterlagen und haben Kartenlesegeräte. Da bin ich doch schon sicher, oder nicht?**
Dass eine Authentifizierung und somit Sicherheit der Geräte (Drucken, Kopieren, Scannen) implementiert ist, ist bereits eine sehr gute Ausgangslage. Häufig werden aber ‚offene Ports' im Netzwerk übersehen. Hacker nutzen dieses Problem im Internet für ihre Zwecke aus, um so Malware hochzuladen.

Die Spezialisten von Sharp können Ihnen dabei helfen, Zugriffe auf das MFP und die Druckfunktionen ‚ausschließlich' auf unternehmerische Bedürfnisse zu begrenzen und jede Möglichkeit für einen Sicherheitsverstoß des Geräts zu unterbinden.

**Ich habe schon viel Geld für Sicherheit ausgegeben. Funktioniert die Sharp-Lösung mit meinen bestehenden Massnahmen in Sachen IT-Sicherheit?**
Die neuesten MFP-Serien von Sharp sind mit allen notwendigen Netzwerk-Ports, Diensten, Protokollen und Kontrollmöglichkeiten ausgestattet, damit sie in einer sicheren Netzwerk-Umgebung reibungslos funktionieren. Unsere Systeme können auch über eine Active Directory-Konzernrichtlinie gesteuert werden.

**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
Be Original.