SHARP

Sicherheitslösungen

Die Sharp Security Suite

Leistungsstarker Schutz für wertvolle Informationen

Sicherheitsrisiken im Alltag erkennen

In der heutigen Bürowelt sind Multifunktionssysteme schnell, vielseitig und benutzerfreundlich. An jedem Tag und zu jeder Stunde werden vielerlei Dokumente kopiert, gedruckt, gescannt und per Telefax gesendet, einschließlich äußerst vertraulicher Unterlagen. Unglücklicherweise können ungesicherte MFPs dabei ein erhebliches Sicherheitsrisiko darstellen.

Denn auf ihren Festplatten werden Kopien tausender, oftmals hochsensibler Dokumente gespeichert, wodurch Multifunktionssysteme im Netzwerk zur Zielscheibe interner wie externer Hacker werden können. Und was die Sache noch bedrohlicher macht, ist, dass die hoch entwickelten Funktionen es den Hackern kinderleicht machen, die sensiblen Daten des Unternehmens von außerhalb zu kopieren bzw. weiterzuleiten.

Vertrauliche Berichte, persönliche Daten, Kundendaten, Abschlussberichte, Mitarbeiterinformationen: diese Daten müssen allesamt gegen eine ganze Bandbreite möglicher Schwachstellen gesichert werden.

Übliche Schwachstellen

Zu den häufigsten Schwachstellen, die ein ungeschütztes Multifunktionsprodukt aufweist, zählen:

- Produktivitätsverluste
- Nichterfüllung gesetzlicher Vorschriften
- Zugriffsausfall
- Gestohlene Informationen
- Gerichtsverfahren
- Unberechtigte Zugriffe

Interne Bedrohungen

Sobald ein Dokument erstellt wurde, wird es anfällig für Verlust bzw. Diebstahl. So könnte es z. B. von der internen Festplatte des MFP kopiert werden, oder an einen Dritten gefaxt werden. Oder auch nur aus dem Ausgabefach genommen werden – vielleicht sogar nur versehentlich. Und natürlich sind im Netzwerk eingebundene MFPs praktische Werkzeuge, wenn es darum geht, Druckausgaben von vertraulichen Informationen zu erzeugen.

Vielschichtige Sicherheits-lösungen

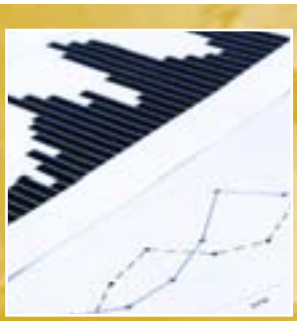
Externe Bedrohungen

Gespeicherte Dokumente und Scan- sowie Druckdaten können in unterschiedlichen Netzwerken und in virtuellen privaten Netzwerken (VPN) und im Internet abgefangen werden. Hacker können MFPs sogar dazu nutzen, um Computer-Viren auszusetzen oder um Denial-of-Service-Attacken (DOS) zu starten. Faxleitungen und LAN-Anschlüsse können ebenfalls das potenzielle Risiko erhöhen, dass Daten durch Dritte, die irgendwo auf der Welt ansässig sind, abgefangen werden.

Vielschichtige Sicherheitslösungen mit der Sharp Security Suite

Die Sharp Security Suite schützt sowohl vor gängigen Schadensanfälligkeiten als auch vor internen und externen Bedrohungen. Im Folgenden werden die Sharp Sicherheitskonzepte in den fünf Schlüsselbereichen erläutert:

1. **Datensicherheit**
2. **Dokumentensicherheit**
3. **Netzwerksicherheit**
4. **Zugriffskontrolle**
5. **Aktivitätsprotokolle**



Data Security Kit

Datensicherheit

Ein ungeschütztes MFP stellt in zweifacher Weise ein Sicherheitsrisiko für Ihre Daten dar: zum einen sind da die Informationen auf der internen Festplatte, zum anderen sind es die Funktionen, mit denen Dokumente kinderleicht kopiert, gefaxt oder per E-Mail an Dritte weitergeleitet werden können. Die Sharp Security Suite schiebt beiden Sicherheitsrisiken einen Riegel vor.

Data Security Kit

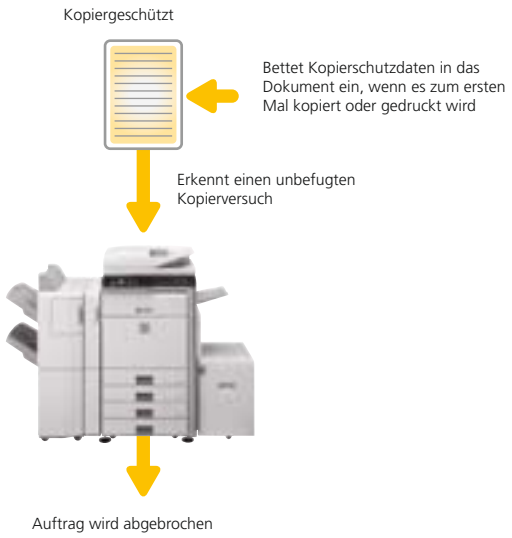
Das optional erhältliche Data Security Kit, welches branchenweit die erste zertifizierte Common-Criteria-Lösung seiner Art war, macht es praktisch unmöglich, Daten von der internen Festplatte abzufangen oder wiederherzustellen. Der Advanced Encryption Standard Algorithmus (AES) wird auf alle Daten angewandt, während diese auf Festplatte, RAM oder Flash-Speicher geschrieben werden.

Das Data Security Kit eliminiert auch verbliebene Daten, indem diese bis zu sieben Mal mit einer Serie zufälliger Werte überschrieben werden. Für zusätzlichen Komfort kann das Data Security Kit so konfiguriert werden, dass Daten auf drei unterschiedliche Arten überschrieben werden:

- automatisch, wenn das Druck-Ausgabegerät eingeschaltet wird,
- automatisch, nach jedem Drucken/Kopieren/Faxen/Scannen,
- von Hand, je nach Bedarf.

Dokumentenkontrolle

Die Dokumentenkontrolle*1 funktioniert, indem das Sharp-MFP, welches mit dem Data Security Kit*2 ausgestattet ist, den Dokumenten ein kaum sichtbares Datenmuster hinzufügt. Versucht jemand nun, eines dieser so gekennzeichneten Dokumente zu kopieren oder zu scannen, wird der Auftrag abgewiesen, oder eine leere Seite ausgeworfen und ein E-Mail-Report an den Administrator geleitet.



*1 Optionales Data Security Kit erforderlich.

*2 Fordern Sie bitte eine Liste kompatibler MFPs von Ihrem Sharp-Partner an.

Auf einen Blick

- *Verschlüsselt die Daten, während diese auf Festplatte, RAM oder Flash-Speicher geschrieben werden*
- *Beseitigt verbliebene Daten mit hoher Zuverlässigkeit, und verhindert so, dass diese entdeckt werden*
- *Verhindert unbefugtes Scannen bzw. Kopieren von Dokumenten*

Common-Criteria-Validierung

Encrypted PDF

Common Criteria

Common Criteria ist ein internationales Auswertungsprogramm für Normen, welches zur Validierung von Hersteller-Datensicherheitsstandards auf Basis von Normen wie ISO 15408 (einer auf Basis der Common Criteria entwickelten Auswertungsnorm für Sicherheitsprodukte und -systeme) eingeführt wurde.

Die Vertrauenswürdigkeitsstufen (Evaluation Assurance Levels – EAL) der Common-Criteria-Auswertungen bewegen sich zwischen EAL 1 und 7, wobei EAL 1 bis 4 am relevantesten für kommerzielle Sicherheitsprodukte sind.

Die weltweit zuerst geprüften MFPs mit der höchsten Qualitätsbewertung

Sharp war weltweit der erste MFP-Hersteller, dem es gelang, die Common-Criteria-Zertifizierung zu erlangen, und war darüber hinaus die erste Firma, die eine EAL4-Wertung für ein Data Security Kit (AR-FR5) erhielt. Bis heute wird Sharp in der Industrie zu Recht als einer der wichtigsten Vorreiter in Sachen Datensicherheit betrachtet.

Heute zählen global agierende Unternehmen und Regierungsbehörden auf Sharp, wenn es darum geht, vertrauliche Daten vor unberechtigtem Zugriff zu schützen.

Dokumentensicherheit

Jedes Dokument, welches zunächst gescannt und dann als E-Mail-Anhang versendet wird, ist potenziell in Gefahr, versehentlich oder absichtlich abgefangen zu werden – von nicht dazu befugten Dritten. Deshalb ist es sinnvoll, sensible Dokumente vor dem Versand zu verschlüsseln.

Als Grundlage für die verschlüsselte PDF-Dateien-Funktion* verwendet Sharp die auch für Scan-to-E-Mail, -FTP, -Desktop, -HDD und -USB geeignete RSA-Technologie, mit der Dateien vor dem Versand verschlüsselt werden. Der Benutzer wird, sobald er ein Dokument scannen will, aufgefordert, ein Passwort einzugeben, so dass der Empfänger die Datei nur dann ansehen kann, wenn er oder sie das entsprechende Passwort kennt.

Eine weitere Sicherheitsebene bietet das Secure Sockets Layer (SSL), welches alle Informationen im Datenstrom, alle Dokumente in der Druck-Warteschlange und auch alle Informationen, die zwischen MFP und Administrator per Web-Schnittstelle ausgetauscht werden, verschlüsselt.

* Fordern Sie bitte eine Liste kompatibler MFPs von Ihrem Sharp-Partner an.

MX-FRX5 Version M.10
MX-FRX6 Version M.10
MX-FRX9 Version M.10
MX-FRX10 Version C.10
MX-FRX11 Version C.10
MX-FRX13 Version C.10

Weitere Data Security Kits befinden sich derzeit in der Zertifizierung.

Common Criteria Validated

MFP Data Security Kit

Auf einen Blick

- *Schützt eingescannte Dokumente vor dem Zugriff Dritter*
- *Verhindert unbefugtes Öffnen oder Drucken vertraulicher Dokumente*
- *Verschlüsselt alle Informationen im Datenstrom*

Sichere Firewall

Netzwerksicherheit

MFPs von Sharp haben eine intelligente Netzwerk-Schnittstelle, die eine sichere Firewall für jedes Multifunktionsprodukt bietet und vor unberechtigtem Zugriff auf Konfigurations- und Netzwerkeinstellungen schützt.

Der Zugriff kann auf drei Ebenen kontrolliert werden:

- IP Adressenfilter – schränkt den Zugriff auf eine bestimmte Anzahl von Adressen ein,
- MAC Adressenfilter – schränkt den Zugriff auf bestimmte PCs unabhängig von der IP-Adresse ein,
- TCP/IP-Servicesperre, die bestimmte Kommunikationsprotokolle sperrt und Administratoren erlaubt, ungeschützte Ports zu schließen und die eingebettete Homepage des Geräts zu deaktivieren.

Die Kommunikation zum und vom MFP kann man auch durch das Secure Sockets Layer (SSL) schützen, welches für sichere Datenübertragung über das Netzwerk sorgt, und viele Druck-Ausgabegeräte unterstützen schon jetzt SMB, IPv6, IPSec und SNMPv3. Darüber hinaus unterstützen viele der neuen MFPs von Sharp auch IEEE802.1X, welches einen hohen Sicherheitsstandard bietet, indem es Geräten, die keine Befugnis haben, den Zugriff auf die Daten verweigert.

Faxsicherheit

Die Kompromittierung der Netzwerksicherheit durch eine offene Faxleitung, mit der ein entschlossener Hacker sich den Zugriff auf eine ungesichertes Netzwerk-Schnittstelle sichert, wird oft als reales Szenario für ein Sicherheitsrisiko dargestellt. Die gute Nachricht in diesem Zusammenhang ist, dass die Architektur der MFPs von Sharp vergleichbare Sicherheitslücken in Geräten anderer Hersteller ausschließt, so dass es für einen Hacker keine Möglichkeit gibt, sich per Dial-up einen Zugriff auf interne Systeme zu verschaffen.

Unsere MFPs* sind so gebaut, dass der Fax-Modem-Controller physisch von den anderen Controllern getrennt ist, zudem haben wir darüber hinaus dafür gesorgt, dass er keinen externen Code verarbeiten kann. Aber dieses Faxsystem läuft nicht nur unabhängig von allen anderen Funktionen – es reagiert nur auf spezielle Faxübertragungsprotokolle, und bricht alle anderen automatisch ab.

* Fordern Sie bitte eine aktuelle Liste bei Ihrem Sharp-Partner an.

Auf einen Blick

- *Schützt das Netzwerk mit einer sicheren Firewall*
- *Bietet Zugriff nur für Geräte mit eindeutiger, bekannter Kennung*
- *Beseitigt das Risiko, welches gewöhnlich in offenen Faxleitungen gesehen wird*

Zugriffs-
kontrolle

Job Log

Zugriffskontrolle

Die Begrenzung der MFP-Zugriffe auf bekannte Benutzer ist ein wichtiger Schritt bei der Sicherung Ihrer vertraulichen Informationen. Die Sharp Security Suite bietet erstklassige Sicherheit, da es sowohl vor unberechtigten Zugriffen direkt an der Maschine als auch aus dem Netzwerk schützt.

Direkt am MFP wird der Zugriff überprüft, indem der Benutzer ein eindeutiges alphanumerisches Passwort vor jeder Tätigkeit eingeben muss. Der Zugriff aus dem Netzwerk wird auf registrierte Benutzer mit gültigen Netzwerkkonten beschränkt, die durch eine Kombination aus Benutzername/Passwort oder numerischem PIN bestehen, welches vom LDAP- oder Active Directory Server validiert wird. Alle Zugangsdaten des Benutzers werden mit einer bewährten Kombination von Verschlüsselungstechniken (Kerberos, SSL und Digest-MD5) übertragen, um ein Abfangen dieser Daten zu erschweren.

Darüber hinaus können Scan-to-E-Mail- und Scan-to-Fax-Funktionen auf vorher festgelegte Adressen eingeschränkt werden, damit Dokumente gar nicht erst an unbefugte Empfänger verschickt werden können.

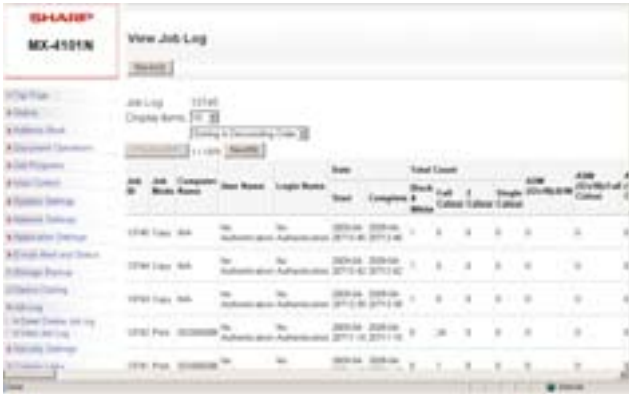
Auf einen Blick

- *Schützt vor unbefugtem Zugriff am Gerät und durch das Netzwerk*
- *Verhindert Bedienung durch unbekannte oder unbefugte Benutzer*
- *Verhindert, dass gescannte Dokumente per E-Mail verschickt werden*

Aktivitätsprotokolle

Der letzte Step hin zu einer umfassenden Sicherheit für Ihre MFPs besteht darin, die Benutzung des Geräts zu protokollieren.

Dabei kann man entweder die vom Sharp-MFP gelieferten Job-Log-Daten nutzen, oder man verwendet die Protokollierungs-Software eines anderen Anbieters, mit der man eine revisionssichere Protokollierung erzeugt. Dann lassen sich die Tätigkeiten der Benutzer mit Details der verwendeten Funktionen festhalten. Zusätzlich kann man bei Scan-to-E-Mail-Dokumenten das Gerät so einstellen, dass die E-Mail-Adresse des Benutzer automatisch in ein Formularfeld eingefügt wird, und – falls notwendig – kann darüber hinaus eine Blindkopie an den Netzwerk-Administrator geschickt werden.



Auf einen Blick

- *Erstellt eine detaillierte Auflistung darüber, wer das MFP wann benutzt hat*
- *Protokolliert jede Benutzung einschließlich Kopieren, Scannen und E-Mail-Versand*
- *Protokolliert Details wie Dateinamen und E-Mail-Bestimmungsorte bei unbekannter Adresse*

Sicherheitslösungen

Sharp Electronics (Europe) GmbH
Sonninstraße 3, 20097 Hamburg, Germany
Tel.: (040) 23 76-0 · Fax: (040) 23 76-2660
www.sharp.de
Zweigniederlassung Österreich
Handelskai 342, 1020 Wien, Austria
Tel.: (01) 7 27 19-0 · Fax: (01) 7 27 19-109
www.sharp.at

SHARP

BR-SEC 11/09