brother
at your side

Brother Sicherheits-Tipps

April 2016

DIE VERSTECKTEN GEFAHREN IHRES DRUCKERS UND WAS SIE DAGEGEN TUN KÖNNEN

Die Druck- und Scanumgebungen in Unternehmen werden immer vielseitiger und leistungsfähiger. Mit diesen Fortschritten gehen jedoch auch erhöhte Sicherheitsrisiken einher. Und nur wenige Organisationen schützen sich davor.

Sicherheitsmassnahmen bei der Arbeit sind heute alltäglich. Unternehmen setzen zahlreiche Tools ein, um sich zu schützen. Diese reichen von Badges oder Schlüsseln zur Zugangskontrolle bis hin zu Netzwerksicherheits-Software zum Schutz von Informationen.

In einem Bereich aber haben viele Unternehmen immer noch potenzielle Sicherheitslücken: In der Art und Weise, wie IT-Geräte wie Drucker oder Scanner an das sonst sichere Netzwerk angeschlossen werden.

2015 befragte Brother in einer Umfrage über 2'500 KMUs zu den Herausforderungen ihrer Unternehmen. 75% erklärten, dass Informationssicherheit in ihrer Firma ein wichtiges Thema sei und 59% gaben an, dass die Informationssicherheit bei Entscheidungen zum Druck- und Dokumentenmanagement eine zentrale Rolle spiele.

Diese Bedenken steigen mit der Zunahme der Sicherheitsprobleme in allen Branchen. Eine ebenfalls 2015 durchgeführte Quocirca-Studie mit 200 Unternehmen zeigte zum ersten Mal auf, dass die Sicherheit heute ganz oben auf der Tagesordnung steht: 75% der Befragten gaben an, dass die Sicherheit ein wichtiges oder sehr wichtiges Thema (durchschnittliche Bewertung 4.01 von 5) sei. Insgesamt setzen 74% der Unternehmen sichere Drucklösungen ein oder planen, solche in Zukunft einzusetzen.

Wie genau sehen die Gefahren aus?

Im Wesentlichen gibt es vier Möglichkeiten, wie Netzwerkdrucker oder -scanner für ein Unternehmen eine Gefahr darstellen können.

1. **UNBEABSICHTIGTE WEITERGABE VON VERTRAULICHEN INFORMATIONEN BEIM DRUCKEN**
2. **UNBEABSICHTIGTE WEITERGABE VON VERTRAULICHEN INFORMATIONEN BEIM SCANNEN**
3. **UNERLAUBTE NETZWERKZUGRIFFE AUFGRUND VON UNZUREICHENDER SICHERHEIT**
4. **PHYSISCHER ZUGANG ZU UNGESICHERTEN GERÄTEN DURCH UNBERECHTIGTE BENUTZER**

Um Unternehmen dabei zu helfen, diese häufigen Sicherheitsbedrohungen zu beseitigen, hat Brother die spezifischen Risiken, die Systembetreuer kennen sollten, sowie die Technologien, mit denen ein besserer Schutz und somit eine bessere Sicherheit gewährleistet werden kann, zusammengestellt.

1. UNBEABSICHTIGTE WEITERGABE VON VERTRAULICHEN INFORMATIONEN BEIM DRUCKEN

Wo liegen die Gefahren?

Egal, wie effektiv die Sicherheitsrichtlinien Ihres Unternehmens sind: Wenn jemand zu einem Drucker gehen und nicht abgeholte Seiten einfach mitnehmen kann, sind Ihre Daten in Gefahr.

Die meisten von uns sitzen nicht gleich neben dem Drucker, den wir benutzen. Es besteht also immer das Risiko, dass unsere nicht abgeholten Druckaufträge – möglicherweise streng vertrauliche Dokumente – für andere zugänglich sind.

Was können Unternehmen dagegen tun?

Die einzige Möglichkeit, dieses Problem effektiv zu bekämpfen, besteht darin, den Druck zu verzögern, bis der berechtigte Benutzer beim Gerät ist. Dies geht am besten mit einer PIN oder einem sicheren Kartenleser. Je nach Grösse und Anforderungen des Unternehmens empfiehlt Brother mehrere verschiedene Lösungen. Eine Möglichkeit ist **Secure Print**. Diese Funktion ist vor allem für Leute geeignet, die nur gelegentlich vertrauliche Dokumente drucken. Mit Secure Print können die Benutzer den Druckprozess verzögern, bis sie beim Drucker stehen. Wenn Sie also etwas Vertrauliches drucken müssen, geben Sie diesem Auftrag beim Senden an den Drucker einfach eine PIN-Nummer. Wenn Sie regelmässig vertrauliche Dokumente drucken, empfehlen wir **Active Directory Secure Print**. Mit dieser Funktion wird der Zugriff auf alle Funktionen am Drucker generell eingeschränkt, indem dieser für nicht berechtigte Personen grundsätzlich gesperrt wird. Zur Freischaltung des Druckers und Abholung der Druckaufträge müssen die Benutzer sich dann zuerst mit ihrem bestehenden Windows® Active Directory-Benutzernamen und -Passwort authentifizieren. In beiden Fällen wird der Druckauftrag auf dem internen Speicher des Druckers gespeichert, bis er abgeholt wird.

Um Active Directory Secure Print verwenden zu können, muss ein Unternehmen bereits Microsoft® Active Directory benutzen. Für Unternehmen, die dies nicht tun, bietet Brother aber auch die Möglichkeit des sicheren Druckens auf LDAP-fähigen Datenbankservern. Dies funktioniert gleich wie Active Directory Secure Print, aber die Kommunikation erfolgt über einen LDAP-fähigen Server.

Für zusätzliche Sicherheit mit Active Directory- oder LDAP Secure Print-Funktionen kann eine zeitliche Begrenzung für die Speicherung von nicht abgeholten Druckaufträgen im Gerätespeicher festgelegt werden. So bleiben vertrauliche Dokumente nicht auf unbestimmte Zeit im Gerät.

Für Unternehmen, in denen die Notwendigkeit des Druckens von vertraulichen Informationen je nach Benutzer unterschiedlich ist, ist ein netzwerkbasierter Ansatz wohl eine bessere Lösung. Brother's PrintSmart Secure Pro beispielsweise speichert die Dokumente auf einem zentralen Server anstatt auf dem Gerät. Dies bedeutet, dass der Benutzer mit seiner PIN oder mittels NFC Card-Authentifizierung seine Dokumente bei einem beliebigen, an den PrintSmart-Server angeschlossenen Drucker im Gebäude abholen kann. Ausserdem können die Systembetreuer so die Nutzung enger überwachen.

Aber trotz all dieser Massnahmen gibt es noch einen Schwachpunkt: Mit der richtigen Software können Ihre Daten beim Versand an den Drucker abgefangen werden. Um Sie davor zu schützen, enthalten die Geräte von Brother Transport Layer Security (TLS) und Secure Socket Layer (SSL) Verschlüsselung, also dieselbe Technologie, die im Onlinehandel verwendet wird, um Bank- und Kreditkartendetails zu schützen. Ihre vertraulichen Dokumente können also für die Übertragung mit bis zu 256-bit verschlüsselt werden.

2. UNBEABSICHTIGTE WEITERGABE VON VERTRAULICHEN INFORMATIONEN BEIM SCANNEN

Wo liegen die Gefahren?

Auch wenn Ihr Drucker sicher ist: Das nächste potenzielle Sicherheitsrisiko ist nicht weit entfernt. Gescannte Dokumente können vom Benutzer auf verschiedene Weise gespeichert oder geteilt werden. Das Teilen von gescannten Dokumenten per E-Mail oder übers Web birgt ein grosses Risiko für vertrauliche Daten, weil damit Dokumente mit einem relativ kleinen Fehler schnell in falsche Hände gelangen. Und das Schlimmste: Es können unbeschränkt viele Kopien des Dokuments gemacht werden.

Was können Unternehmen dagegen tun?

Die einfachste Lösung besteht darin, Ihre gescannten Dokumente in PIN-**geschützte PDF-Dokumente** zu verwandeln. Die Einzelscanner/Multifunktionsscanner von Brother können jede neue PDF-Datei mit einer vierstelligen PIN schützen, damit sie von niemandem ohne Erlaubnis geöffnet werden kann.

Alternativ kann auf vielen Brother Einzel- und Multifunktionsscannern auf **SFTP gescannt** werden. Das Netzwerkprotokoll Secure File Transfer Protocol sorgt für einen vertraulichen, sicheren Datenfluss. Durch die engere Überwachung des Zugriffs auf SFTP-Server können Unternehmen sogar das ganze Netzwerk sicherer machen, indem sie einen Gateway zu und aus ihrem System komplett schliessen.

Unterstützte Dienste abhängig vom Modell

3. UNERLAUBTE NETZWERKZUGRIFFE AUFGRUND VON UNZUREICHENDER SICHERHEIT

Wo liegen die Gefahren?

Es ist üblich, dass Tablets und Laptops Zertifikate, Benutzernamen und Passwörter benötigen, wenn sie an ein sicheres Netzwerk angeschlossen werden. Für Drucker dagegen ist dies oft nicht der Fall, obwohl deren Anschluss ans Netzwerk eine genauso grosse Gefahr für die Sicherheit des gesamten Netzwerks darstellen kann.

Was können Unternehmen dagegen tun?

Externe Bedrohungen

Da Brother Geräte verschiedene eingebaute Verschlüsselungsarten enthalten, gibt es mehrere Möglichkeiten, die Sicherheit zu erhöhen und die Sicherheitslücke zu schliessen.

802.1x: Die Geräte von Brother entsprechen alle dem sehr hohen Sicherheitsstandard IEEE 802.1x, ob sie nun festverdrahtet oder Teil eines drahtlosen Netzwerks in einem Unternehmen sind.

IPsec: Mehrere Brother Geräte können mit IPsec schnell, ein-fach und kostengünstig direkt an interne oder externe sichere Umgebungen angeschlossen werden. Da IPsec bei diesen Geräten bereits eingebaut ist, muss keine Middlewear oder Fremdhardware installiert werden, um beide Endpunkte miteinander zu verbinden.

SNMPv3: Die Geräte von Brother erfüllen strenge Netzwerksicherheitsrichtlinien und verstehen daher alle Anweisungen in verschlüsselten SNMP-Versionen 1, 2 & 3 (MD5 und SHA1), und zwar auch bei der Ferneinrichtung und der routinemässigen Wartung.

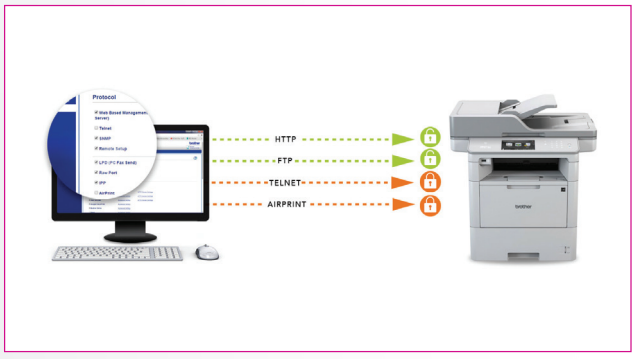
Auch wenn Unternehmen ihre eigenen Druckerflotten-Verwaltungstools und nicht das Programm Brother BRAdmin verwenden, um ihre Geräte zentral zu verwalten, lassen sich Brother Drucker schnell und einfach in ihre sicheren Netzwerke integrieren.

Interne Bedrohungen

Verschlüsselungsverfahren schützen effizient vor externen Gefahren. Wenn aber interne Mitarbeiter Netzwerkdrucker mittels Remote-Zugriff bedienen können, können Netzwerke verwundbar sein. Um alle damit zusammenhängenden Probleme zu verhindern, unterstützen Brother Drucker **passwortgeschützte eingebettete Webserver,** bei denen nach fünf Minuten Inaktivität die Verbindung abbricht.

Ausserdem unterstützen sie die **IP-Sperre**, mit welcher der Zugriff auf das Gerät über das Netzwerk verhindert werden kann. In diesem Beispiel erlaubt der Drucker nur Verbindungen von Benutzern mit den folgenden IP-Adressen: 10.45.12.1, 12.45.12.45, 10.45.12.46 & 10.45.12.47.

Die **Protokollüberwachung** ist weniger restriktiv und ermöglicht die Blockierung von nicht erforderlichen Protokollen, ohne den Zugriff komplett auf alles zu sperren (z.B. FTP oder SMTP). Das untenstehende Beispiel zeigt, wie ein IT-Mitarbeiter die folgenden Funktionen blockiert hat: Telnet, AirPrint, Proxy & FTP Server.



4. PHYSISCHER ZUGANG ZU UNGESICHERTEN GERÄTEN DURCH UNBERECHTIGTE BENUTZER

Wo liegen die Gefahren?

Auch mit all diesen Funktionen zur Verbesserung der Sicherheit kann man immer noch zu den Druckern gehen und versuchen, Daten abzurufen. Es sei denn, sie stehen in einem abgeschlossenen, sicheren Raum. Vor allem für kleine und mittlere Unternehmen mit wenig oder keiner IT-Infrastruktur ist eine physische Sicherung besonders wichtig.

In der anfangs erwähnten Umfrage, die Brother 2015 durchgeführt hat, sagten zwei Drittel der Entscheidungsträger, dass die Informationssicherheit bei Entscheidungen zum Druck- und Dokumentenmanagement eine zentrale Rolle spiele. Unter anderem äusserten sie Bedenken zur Art und Weise, wie Dokumente beim Drucker aufbewahrt werden.

Was können Unternehmen dagegen tun?

Für diese Unternehmen bietet Brother eine Reihe an Sicherheitsfunktionen, mit denen vermieden werden kann, dass unberechtigte Personen die Geräte manipulieren.

Setting Lock macht genau, was Sie davon erwarten. Diese Funktion schränkt den Zugriff auf die Geräteeinstellungen über das Bedienfeld ein. Diese Lösung ist ideal für Unternehmen, welche die Funktionalitäten nicht einschränken, aber sicherstellen möchten, dass unberechtigte Benutzer keine Einstellungen verändern können.

Die Funktion **Secure Function Lock** geht einen Schritt weiter, indem sie den Zugriff auf die Geräte- einstellungen und auf gewisse Funktionen verhindert. So können Systembetreuer mit der Zuteilung von persönlichen PINs oder NFC-Zugriffskarten entscheiden, wer was mit welchem Gerät machen kann und so zum Beispiel auch regeln, wer faxen und scannen kann, oder monatliche Limiten festlegen.

Der untenstehende Screenshot zeigt die Secure Function Lock-Einstellungsseite des eingebetteten Webservers des Geräts. Er zeigt, dass für unberechtigte Benutzer alle Funktionen gesperrt sind. Dies ist in der ersten Zeile “Public Mode” ersichtlich. User 1 hat uneingeschränkten Zugriff auf alle Funktionen (zweite Zeile). User 2 kann keine Faxe senden oder empfangen und hat eine Drucklimite von 100 Sei- ten. Diese Limite kann von einem Systembetreuer manuell angepasst oder gelöscht werden oder nach einer gewissen Zeit automatisch gelöscht werden.

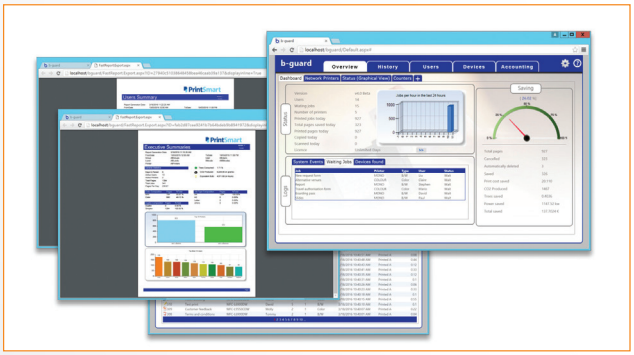
In Unternehmen, in denen mehrere Benutzer dieselben Drucker verwenden oder die Drucker an öffentlich zugänglichen Stellen platziert werden müssen, kann es schwierig sein, Missbrauch zu vermeiden, ohne die normale Nutzung zu beeinträchtigen. Aber mit der Authentifizierung über Brother Active Directory oder LDAP können Mitarbeiter einfach mit ihrem bestehenden Netzwerk-Login auf die Drucker zu- greifen.

Das Gesamtpaket

Für Unternehmen, die ihre Sicherheit im Griff haben und genau sehen möchten, wie ihre Geräte verwendet werden, bietet Brother mit **PrintSmart Secure Pro** eine innovative, kostengünstige Software-Lösung, mit der die Sicherheit verbessert, die Effizienz gesteigert, die Druckkosten transparent gemacht und die Papierverschwendung reduziert werden kann. Über eine einfache Benutzeroberfläche erhalten die Systembetreuer eine bessere Übersicht und alle notwendigen Informationen zur Druckernutzung in ihrem Unternehmen. So können sie die Aktivitäten verwalten und überwachen und die Druckkosten verfolgen, kontrollieren und reduzieren.

Brother Drucker lassen sich auch einfach in Druckmanagement-Lösungen Dritter integrieren. **Brother Solutions Interface (BSI)** ist eine offene Schnittstellen-Plattform, die es Dritten erlaubt, ihre eigenen Lösungen für Brother Geräte zu entwickeln.

Die Unternehmen können also die Benutzeroberfläche ganz an ihre Bedürfnisse anpassen.



Empfehlungen

Die von Druckern und Scannern ausgehende Gefahr für die Daten- und Netzwerksicherheit von Unternehmen muss zweifellos in jeder Branche ernst genommen werden. Es gibt jedoch keine Standardlösung. Die Systembetreuer müssen die für ihre Risiken, ihre Infrastruktur und die bestehende Sicherheit geeignete Lösung wählen. Kann ein Unternehmen die folgenden drei Punkte bestätigen:

1. **Die Geräte wurden gesichert**
2. **Die Daten werden bei der Übermittlung und nach dem Drucken geschützt**
3. **Das Netzwerk ist vor unerlaubtem Zugriff geschützt**

kann es zuversichtlich sein, dass seine Druck- und Scangeräte gegen allfällige Sicherheitsprobleme gewappnet sind.

[1]Quelle: Brother SMB Research, durchgeführt von B2B International bei 2’502 Unternehmen im Vereinigten Königreich, Frankreich, Deutschland und den USA

[2]Quelle: Quocirca Managed Print Services Landscape, 2015. Umfrage bei 200 Unternehmen mit mindestens 1’000 Mitarbeitern im Vereinigten Königreich, Frankreich, Deutschland und den USA