HOCHSCHULE harz
Hochschule für angewandte Wissenschaften (FH)

Sicherheitsempfehlungen für Netzwerkdrucker, Kopierer und Multifunktionsgeräte

Version	1.0
Datum	03.04.2009

Herausgeber	Rechenzentrum Hochschule Harz
Erreichbar unter	E-Mail: rz@hs-harz.de

Inhalt

Abkürzungen

SSL	Secure Socket Layer
TLS	Transport Layer Security
IT	Informationstechnik
IP	Internet Protokoll
SNMP	Simple Network Management Protocol
ACL	Access Control List

1 Einleitung

Zur Grundausstattung der heutigen Büroräume gehören Drucker und Kopierer. Da es ineffizient ist für jeden IT-Arbeitsplatz einen Drucker bereitzustellen, werden diese an zentralen Stellen mit Netzanbindung aufgestellt. Sie sind daher eine kostengünstige und Platz sparende Lösung. Druckaufträge werden nicht direkt an den Drucker weitergereicht sondern an einen Druckserver weitergeleitet, der wiederum erst dem Drucker den Auftrag zuteilt.

Moderne Druck- und Kopierer Systeme verfügen heute über eigene Betriebssysteme, Protokolle, Ports, Festplatten und Anwendungsprogramme. Sie können drucken, faxen, mailen, kopieren und scannen, besitzen einen Netzanschluss im LAN, Wireless oder über Bluetooth und sind intern und extern erreichbar. Die Wartungsarbeiten erfolgen über den vorhandenen Netzanschluss und nicht mehr lokal.

Drucker und Kopierer stehen dazu noch oft in Gängen und an Stellen die dem Publikumsverkehr zugänglich sind.

Diese Mulitfunktionsgeräte haben damit viele Funktionen und Komponenten eines Servers übernommen und müssen dementsprechend mit den gleichen Sicherheitsanforderungen bewertet werden. Ein Drucker oder Kopierer kann ebenso viele vertrauliche Informationen oder Daten über das Netzwerk preis geben, wie jeder andere Rechner mit Netzwerkanschluss.

Wie auch ein Server müssen Drucker und Kopierer mit einem Virenschutz, Diebstahlsicherung, Zugriffsberechtigungen, Sicherung der gespeicherten Daten und zentraler Verwaltung der Passworte und Authentifizierung gewartet und eingerichtet werden.

Auflistung der Multifunktionsgeräte

- Drucker
- Scanner
- Kopierer
- All-in-One Geräte
- Faxgeräte
- Printerports

2 Gefährdungslagen

Nachfolgende Gefährdungslagen wurden nach dem [BSI] aufgelistet.

1. unzureichende Regelungen in der Organisation:
    - mangelhafte Betriebsmittelverwaltung beeinträchtigt den termingerechten Arbeitsablauf,
    - unzureichend Wartung und Protokollierung der Geräte,
2. unbefugter Zutritt zu Räumen mit Drucker, Kopierern und Multifunktionsgeräten,
3. Sorglosigkeit im Umgang mit Informationen, vertrauliche Dokumente landen im Papierkorb,
4. ungeregelte Nutzung der Drucker und Kopierer, die Nutzung erfolgt unautorisiert,
5. Komplexität der Drucker und Kopierer:
    - Nicht benötigte Funktionen und Protokolle sind nicht deaktiviert,
    - der volle Funktionsumfang wird nicht genutzt zur Sicherung der Daten,
6. unzureichender Schutz der Kommunikation zwischen Druckern, Druckserver und IT_Arbeitsplätzen,
    - Druckaufträge können abgefangen oder umgeleitet werden,
    - Druckaufträge können verändert werden,
    - Falsche Druckaufträge werden ausgelöst,
7. Manipulation / Zerstörung der IT-Geräte,
8. Diebstahl der Geräte oder Teile wie Festplatten,
9. Manipulation der Software:
    - Konfigurationsänderungen der Software und Einstellungen direkt am Gerät,
    - Abruf von Informationen über das angebundene Netzwerk

- Auslesen von Informationen über die Befehlsaufforderung über eine gesendete E-Mail an den Drucker,

10. Auswertung von Restinformationen von Druckern und Kopierern, sehr oft werden in den Speichern der Geräte schutzbedürftige Informationen abgelegt
11. unzureichende Druckserversicherheit
    - Manipulation der Verwaltung von Druckern
    - Manipulation der Benutzerverwaltung und Protokollierung
    - Veränderung der Daten auf dem Kommunikationsweg

3 Kriterien für die Beschaffung von Druckern, Kopierern und Multifunktionsgeräten

Jegliche Form der Beschaffung sollte zentral erfolgen, bei Beschaffung von Multifunktionsgeräten in anderen Einrichtungen sollte dies an der zentralen Stelle bekanntgegeben werden. Nachfolgende Kriterien zur Beschaffung von Multifunktionsgeräten wurden nach dem [BSI] aufgelistet.

1. grundlegende funktionale Anforderungen
    - muss des Geräte netzfähig sein,
    - Prüfung der Angemessenheit der Leistungsfähigkeit mit der Größe des Benutzerkreises,
    - Druckertyp und Druckverfahren beachten,
    - Erweiterungsmöglichkeiten mit zusätzlichen Funktionen im Anschluss.
2. Allgemeine Sicherheit
    - unterstützt das Gerät Protokolle (browserbasiert => SSL/TLS) für eine sichere Administration,
    - können Informationen verschlüsselt gespeichert werden (Festplattenverschlüsselung),
    - gibt es die Möglichkeit der Authentisierung direkt am Gerät über Passwort oder PIN-Eingabe,
    - sind Möglichkeiten vorhanden um das Gerät vor Diebstahl zu sichern,
    - kann eine Manipulation der Hardware des Gerätes verhindert werden, z.B. durch Schlösser.
3. Sicheres Löschen
    - kann nach jedem Kopiervorgang der Nutzer die Informationen selbst löschen,

- ist es möglich die gesamte Festplatte zu löschen,
- werden Informationen zum Löschen angezeigt auf dem Display.

4. Netztechnische Sicherheit
    - besitzt das Gerät netztechnische Sicherheit wie Portfilter,
    - muss das Gerät Wireless- oder Bluetoothfähig sein, da der Einsatz von Funktechniken mit höheren Sicherheitsrisiken verbunden ist,
    - unterstützt das Gerät, die Verschlüsslung der Kommunikation.
5. Wartbarkeit
    - bietet der Hersteller regelmäßige Updates,
    - können Wartungsverträge abgeschlossen werden,
    - bietet der Händler einen technischen Kundendienst an.
6. Kosten
    - Anschaffungskosten beachten,
    - laufende Kosten, einschließlich Wartung, Betrieb und Support müssen eingeplant werden.

4 Geeignete Aufstellung von netzfähigen Multifunktionsgeräten

Maßnahme 1:

Der Zugriff der Netzwerkdrucker sollte geregelt sein. Wo sicherheitsrelevante Informationen gedruckt bzw. kopiert werden muss sichergestellt werden dass nur befugte Personen Zugriff haben. Der Kreis der Berechtigten Personen sollte so klein wie möglich sein.

Maßnahme 2:

Die Authentifizierung direkt an den Geräten ermöglichen, das Dokument wird erst ausgedruckt wenn sich der Benutzer am Gerät direkt authentisiert hat. Bei mehrmaliger Eingabe sollte der Druckauftrag automatisch gelöscht werden.

Maßnahme3:

Die Druckaufträge können mit dem Namen des Empfängers gekennzeichnet werden, dies kann automatisch durch die Druckprogramme erfolgen.

Maßnahme 4:

Shredder neben dem Drucker aufstellen damit vertrauliche Papiere nicht im Papierkorb landen

5 Schutz von Informationen

Maßnahme 1:

Die zu druckenden Informationen werden häufig auf internen Festplatten der Geräte temporär oder permanent gespeichert. Es sollte gewährleistet werden, dass diese Informationen nach dem Druck gelöscht werden

Maßnahme 2:

Verschlüsselung aller Dokumente die auf den Festplatten der Drucker gespeichert werden

Maßnahme 3:

Bei Informationen mit erhöhtem Schutzbedarf ist zu beachten dass einfaches Löschen nicht ausreicht. Einige Geräte besitzen hierfür ein „Sicheres Löschen“, dies ist eine Löschfunktion mit zusätzlichem Überschrieben.

Maßnahme 4:

Maßnahmen ergreifen um einen Angreifer den Zugriff auf den Speicher zu erschweren, z.B. durch die Versiegelung der Geräte und Aufstellung der Geräte so dass sich niemand unbeobachtet daran zu schaffen machen kann.

Maßnahme 5:

Sicherung des Zugriffs auf alle Netzwerkeinstellung direkt vom Gerät aus, das Bedienfeld sollte für die Anwender gesperrt sein.

Maßnahme 6:

Die Funktion Wahlwiederholung für Druckaufträge sollte ausgeschaltet sein. Hiermit können alte Druckaufträge noch mal abgerufen werden.

6 Kommunikation zwischen den Geräten

Maßnahme 1:

So wenig unterschiedliche Protokolle nutzen innerhalb eines Systems. Wenn z.B. kein Zugriff über Webbrowser auf den Druckserver nötig ist, da entsprechende Managementtools vorhanden sind, kann das http Protokoll deaktiviert werden.

Maßnahme 2:

Druckdaten über die Standardprotokolle erfolgen im Klartext und werden über das Netzwerk geleitet, daher sollte die Kommunikation der IT-Systeme mit Transport Layer Security / Secure Socket Layer (TLS/SSL) verschlüsselt werden.

Maßnahme 3:

Schließen aller nicht benötigten Ports, im Standard Betrieb unterstützen Drucker und Kopierer zahlreiche Protokolle und horchen auf den verschiedensten Ports ob ein Druckauftrag für Sie da ist.

Maßnahme 4:

Das Protokoll Simple Network Management Protokoll Version 3 (SNMPv3) unterstützt Benutzerauthentifizierung und Datenverschlüsselung, daher ist der Einsatz des Protokolls anzuraten.

Maßnahme 5:

Die meisten Druckserver bietet das Anlegen einer Zugriffskontrollliste (ACL) an. Hier können IP-Adressenbereiche definiert werden, die auf den Drucker Zugriff haben.

Maßnahme 7:

Druckserver sollten keine Verbindungen zu anderen IT-Systemen besitzen außer den angeschlossenen Druckern.

7 Beschränkung der Zugriffe auf ein Gerät

Maßnahme 1:

Beschränkung auf notwendige Zugriffe, nur so wenig Administratoren wie nötig

Maßnahme 2:

Absicherung der Administrationszugriffe, der Zugriff auf Konfigurationseinstellungen erfolgt erst nach einer erfolgreichen Authentifikation und verschlüsselt.

Maßnahme 3:

Verzicht auf nicht benötigte Funktionen, durch:

- Blockierung aller Ports die nicht benötigt werden
- Eingrenzung das nur von dem angegebenen Druckserver ausgedruckt werden darf, wo dies möglich ist
- Blockierung der Kommunikation zwischen Druckern und externen Netzen am zentralen Sicherheitsgateway

Maßnahme 4:

Netzsegmentierung, empfehlenswert ist alle Drucker und Kopierer in einen logischen Netz zusammenzufassen.

8 Notfallvorsorge

Bei längerem Ausfall kann es zu einer erheblichen Beeinträchtigung der Geschäftsprozesse kommen, daher sind hier entsprechende Maßnahmen zur Notfallvorsorge aufgelistet.

Maßnahme 1:

Es sollten immer genügend Verbrauchsmaterialien zur Verfügung stehen.

Maßnahme 2:

Die Konfigurationseinstellungen sollten schnell wieder herstellbar sein, daher ist eine ausreichende Dokumentation unerlässlich.

Maßnahme 3:

Zentrale Komponenten, wie der Druckerserver, sollten redundant ausgelegt werden.

Maßnahme 4:

Für lokal angeschlossene Drucker sollten bei höheren Schutzbedarf und hohen Verfügbarkeitsansprüchen Ersatzgeräte vorhanden sein.

Maßnahme 5:

Es sollte eine Liste geführt werden mit Fachhändlern bei denen unproblematisch neue Geräte beschafft werden können.

Maßnahme 6:

Für die Dokumentation sollte eine Reviewplanung vorhanden sein.

9 Entsorgung von Druckern, Kopierern und Multifunktionsgeräten

Wenn schützenwerte Daten enthalten sind müssen Geräte so entsorgt werden, dass keine Rückschlüsse auf die Daten möglich sind daher werden hier geeignete Maßnahmen aufgelistet für die Entsorgung von Geräten:

Maßnahme 1:

Zwischengespeicherte Informationen auf den internen Festplatten müssen gelöscht werden, einige Hersteller bieten hierfür Funktionen an

Maßnahme 2:

Konfigurationseinstellungen (IP-Adresse, Hinweise auf die Netzstruktur) sollten gelöscht werden.

Maßnahme 3:

Passworte die gespeichert wurden für die Administration oder der Benutzerauthentifizierung müssen zurückgesetzt werden.

Maßnahme 4:

Löschen der Zertifikate die für die Verschlüsselung eingebunden waren.

Maßnahme 5:

Vernichtung der Verbrauchsmaterialien wie Tonertrommeln, da unter Umständen auf die ausgedruckten Dokumente geschlossen werden kann.

Maßnahme 6:

Sind hoch sicherheitsrelevante Daten auf der internen Festplatte vorhanden, sollte diese physikalisch unbrauchbar gemacht werden.

Maßnahme 7:

Werden schutzbedürftige Geräte gesammelt sollten diese unter Verschluss gehalten werden.

Maßnahme 8:

Wenn die Festplatte ausgebaut werden kann, sollte diese separat gelöscht und entsorgt werden. Nach dem Löschen wird kontrolliert ob das Löschen erfolgreich war.

10 Benutzerrichtlinien für den Umgang mit Multifunktionsgeräten

Da die Komplexität und Sicherheitsanforderungen steigen auch an den Umgang mit Druckern, Kopierern und Multifunktionsgeräten, sollte eine Benutzerrichtlinie erarbeitet werden. Folgende Inhalte sollten konkretisiert werden.

- Die Benutzer sind über den berechtigten Personenkreis unterrichtet
- Eine Zeitnahe Abholung der Ausdrucke ist gewünscht
- Ausdrucke die keinem zugeordnet werden können, werden gesammelt und geschreddert
- Hoch vertrauliche Informationen sollten nicht auf allgemein zugänglichen Druckern und Kopierern vervielfältigt werden
- ein einmal gescanntes Dokument kann beliebig oft ausgedruckt werden, hier sollte der Speicher nach der Benutzung gelöscht werden. Dies kann oft nur direkt am Gerät erfolgen, daher hier Anweisungen direkt am Gerät anbringen.

11 Realisierung

Nachfolgende Tabelle zeigt den Realisierungstand im Rechenzentrum der Hochschule.

Geeignete Aufstellung von netzfähigen (Abschnitt 4)		
Maßnahme1		
Maßnahme 2	✓	
Maßnahme 3		
Maßnahme 4		
Schutz von Informationen (Abschnitt 5)		
Maßnahme1	✓	Festplatten nicht vorhanden
Maßnahme 2	✓	Festplatten nicht vorhanden
Maßnahme 3	✓	Festplatten nicht vorhanden
Maßnahme 4	✓	Festplatten nicht vorhanden
Maßnahme 5	✓	Bedienfeld ist gesperrt
Maßnahme 6	✓	Festplatten nicht vorhanden
Kommunikation zwischen den Geräten (Abschnitt 6)		
Maßnahme1	✓	Alle weitere Protokolle werden deaktiviert
Maßnahme 2		
Maßnahme 3		

Maßnahme 4		
Maßnahme 5		
Maßnahme 6		
Maßnahme 7		
Beschränkung der Zugriffe auf ein Gerät (Abschnitt 7)		
Maßnahme1	✔	Administration im Rechenzentrum
Maßnahme 2	✔	Nutzer mit Passwortkennung erforderlich
Maßnahme 3		
Maßnahme 4	✔	Das Druckernetz ist nur intern zu erreichen.
Notfallvorsorge (Abschnitt 8)		
Maßnahme1	✔	
Maßnahme 2		
Maßnahme 3	✔	Festplatte ist gespiegelt
Maßnahme 4	✔	
Maßnahme 5	✔	Lieferantenverzeichnis vorhanden
Maßnahme 6	✔	Innerhalb des Notfallkonzeptes des Rechenzentrums verankert, mit einer jährlichen Reviewprüfung.
Entsorgung von Druckern, Kopierern und Multifunktionsgeräten (Abschnitt 9)		
Maßnahmen 1-8		Obliegt dem Dezernat Liegenschaften

12 Zusammenfassung

Drucker, Kopierer und Multifunktionsgeräte sind hoch komplexe Systeme, die in Ihren Sicherheitsanforderungen den Standards eines Servers entsprechen. Daher ist eine Nutzerverwaltung genauso Pflicht wie Regelungen zum Umgang, Regelungen zur Einstellung von Netzwerkeinstellungen und Nutzung der Verschlüsselungsfunktionalitäten