Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Drucker und Multifunktionsgeräte im Netzwerk

Bürogeräte – wie Drucker, Scanner, Kopierer, Faxgeräte oder die Kombination dieser als Multifunktionsgeräte – sind heutzutage üblicherweise fester Bestandteil der Office-IT und anderer IT-Infrastrukturen. Im Gegensatz zu anderen Komponenten der Infrastruktur, beispielsweise Anwender-PCs oder Server, wird der Sicherheit dieser Geräte jedoch meist kaum Beachtung geschenkt.

1 Bedrohungslage

Moderne Drucker oder Multifunktionsgeräte bieten zunehmend Dienste an, die einen Zugriff über das Netzwerk mithilfe von Protokollen, wie HTTP, FTP, TELNET oder SNMP, ermöglichen. Gleichzeitig eröffnen sich hierüber prinzipiell auch Möglichkeiten für Angriffe. Zudem sind diese Dienste mitunter nicht sicher implementiert, wohl aber in der Standardkonfiguration aktiviert oder sie können gar nicht deaktiviert werden. Insbesondere Geräte, die durch externe Netzzugänge über das Internet erreicht werden können, sind in besonderem Maße durch Angriffe bedroht.

Zusätzlich zu diesen Diensten sind gerätespezifische Protokolle (z. B. Printer Control Language, PCL oder Printer Job Language, PJL) und möglicherweise undokumentierte Zugangsmöglichkeiten (Debugging-Schnittstellen) implementiert. Diese können für unberechtigte Zugriffe verwendet werden. Auch Cross Site Scripting und ähnliche Angriffe über bzw. auf die Webschnittstelle sind ggf. möglich. Somit kann ein Angreifer durch eine manipulierte E-Mail oder Webseite über einen lokalen Client unberechtigten Zugriff auf den Drucker erlangen.

Analog zu Betriebssystemen und Anwendungen für PCs existieren auch Exploits[1] für Drucker und Multifunktionsgeräte und die darauf implementierten Dienste und Schnittstellen. Diese reichen von Denial-of-Service Angriffen bis hin zur Ausführung von fremdem Code auf dem Gerät. Erforderliche Patches zur Behebung von solchen Schwachstellen werden häufig nicht durch die Betreiber eingespielt. Mitunter werden auch keine Patches durch die Hersteller zur Verfügung gestellt.

Authentisierungsmechanismen können evtl. umgangen werden, da die Geräte i. d. R. nicht gegen Brute Force Angriffe geschützt sind und somit ein automatisiertes Ausprobieren von Passwörtern oder den Missbrauch von Standardpasswörtern möglich ist. Zudem ermöglichen es insbesondere ältere SNMP-Versionen und andere Schnittstellen, Passwörter in Erfahrung zu bringen.

Aufgrund dieser Schwachstellen kann ein Angreifer beispielsweise:

1 Printer Exploitation Toolkit (PRET), http://hacking-printers.net

- Gescannte oder gedruckte Dokumente herunterladen (Verlust von Intellectual Property, Verletzung von Datenschutzbestimmungen),
- Eigene Dokumente zum Drucken hochladen,
- Änderungen an der Gerätekonfiguration vornehmen (z. B. IP-Adresse ändern, Zugriffsberechtigungen bzw. ACLs modifizieren, Druckeinstellungen ändern, Manipulation der Firmware, Herbeiführen von Verschleißerscheinungen, etc.),
- Missbrauch von Druckern als Einfallstor für Angriffe auf das lokale Netzwerk.

Insbesondere der erste der genannten Punkte kann einen signifikanten Schaden verursachen, da gerade größere Bürogeräte in der Regel über einen nicht-flüchtigen Speicher verfügen und dort sämtliche gedruckten oder gescannten Dokumente speichern. Dies muss sowohl bzgl. des (externen) Wartungspersonals als auch bei der Entsorgung von Geräten berücksichtigt werden. Darüber hinaus könnten durch Innentäter, Wartungspersonal oder Lieferanten Manipulationen an der Hardware vorgenommen oder die Festplatten in Geräten ausgetauscht werden.

2 Empfohlene Maßnahmen

Zusätzlich zu allgemeinen Maßnahmen im Rahmen des IT-Sicherheitsmanagements sollten die folgenden Maßnahmen bzgl. der Geräte selbst ergriffen werden, sofern diese vom jeweiligen Produkt unterstützt werden:

- Drucker sollten nicht aus dem Internet heraus erreichbar sein
- Beschränkung des Zugriffs von Druckern in das Internet
- Verwendung eines von Clients und Servern separierten Netzbereichs für Drucker. Falls möglich sollte der Zugriff auf Drucker nicht direkt von Clients aus möglich sein, sondern nur über Druckerserver erfolgen können.
- Änderung sämtlicher Standardpasswörter. Dabei ist zu beachten, dass ggf. für verschiedene Zugriffsmöglichkeiten mehrere separate Passwörter verwendet und entsprechend geändert werden müssen.
- Aktivieren der sicheren Kommunikation zu den Geräten oder anderen Komponenten, wie Druckerservern, sowohl für Dokumente als auch für Authentisierungsdaten. Hierzu bietet sich die Nutzung von IPP (Internet Printing Protocol) an, welches eine Absicherung mittels SSL/TLS ermöglicht.
- Nutzung von Zugangsberechtigungen (Access Control List, ACL)
- Aktivieren der Verschlüsselung des eingebauten Dateisystems (Harddrive, Ramdisk)
- Aktivieren des sicheren Löschens der internen Datenträger / Speicher nach Abarbeitung von Aufträgen
- Deaktivieren unsicherer bzw. nicht-benötigter Dienste (z. B. FTP, SNMP, TELNET, etc.)
- Sicherstellung der Aktualität der Firmware. Einige Hersteller bieten Tools an, um die Versionsstände der Drucker von zentraler Stelle aus zu überwachen und zu aktualisieren. Im Falle von Beschränkungen des Zugriffs auf das Internet ist zu gewährleisten, dass Patches manuell eingespielt werden.
- Nutzung weiterer Features, wie z. B. vertrauliches Drucken (Ausgabe von Dokumenten nur nach PIN-Eingabe)
- Beachtung der Hersteller-Dokumentation bzw. -Empfehlungen zu Sicherheitsaspekten

Die genannten Punkte sollten auch bei der Auswahl bzw. Beschaffung von Geräten berücksichtigt werden. Zudem sollten weitere Kriterien geprüft werden, wie beispielsweise fest-codierte Passwörter oder Passwort-Policies (z. B. Mindestlängen).

Weiterführende Informationen zur Absicherung von Bürogeräten liefert auch der IT-Grundschutz des BSI[23].

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.

2 Drucker, Kopierer und Multifunktionsgeräte – Baustein: https://www.bsi.bund.de/dok/10095868
3 Drucker, Kopierer und Multifunktionsgeräte – Umsetzungshinweise: https://www.bsi.bund.de/dok/10095954