LSI-Info T#09

DRUCKER UND MULTIFUNKTIONS-GERÄTE

Version 1.0 vom: 06.12.2022

Management Summary

Das alt bekannte Sprichwort: „Eine Kette ist nur so stark wie ihr schwächstes Glied." kann auf viele Bereiche unseres beruflichen Alltags übertragen werden, so auch auf IT-Systeme. Oft wird bei dem Thema IT-Sicherheit am Arbeitsplatz nur auf das direkt und unmittelbar vor einem liegenden System und die damit verbundenen Komponenten geachtet. Neben dem sogenannten Arbeitsplatz-PC sollte noch weitere Hardware berücksichtigt werden. Dazu zählen neben Tastatur und Maus auch Multifunktionsgeräte und Drucker. Diese haben teilweise eine große Vielfalt an Funktionalitäten, wie beispielsweise die Übermittlung des Tonerstands an einen Dienstleister über das Netzwerk. Dadurch bieten diese Geräte Angreifern ein beliebtes Einfalltor in die IT-Systeme.

HINTERGRUND

Bei aktuellen Multifunktionsgeräten und Druckern wird oft keine Kabelverbindung für die Kommunikation benötigt. Viele dieser Geräte können mit anderen Endgeräten direkt über WLAN oder über Bluetooth kommunizieren. Zu den Kommunikationspartnern gehören neben dem PC auch Tablet und Smartphone. So angenehm die Funktionalitäten den beruflichen Alltag machen, so viele Gefahren bergen diese ohne vernünftige Konfiguration.

Neben dem Ausbreiten von Angreifern im Netzwerk, durch einen Angriff auf ein Multifunktionsgerät oder Drucker, können auch alle Daten der zu druckenden Dokumente und Zugangsdaten abgefangen werden. Diese abgegriffenen Daten können verkauft, veröffentlicht oder gleich für weitere Angriffe genutzt werden. Diese Gefahren bestehen vor allem bei Geräten, die keine regelmäßigen Updates für das Betriebssystem eingespielt bekommen.

KONFIGURATION

Multifunktionsgeräte bieten eine sehr große Funktionsvielfalt. Nach dem Minimalprinzip sollten alle nicht benötigten Schnittstellen und Funktionen deaktiviert werden.
Dazu zählt auch ein- und ausgehender Internetzugriff. Dieser ist soweit wie möglich einzuschränken.
Um die Geräte mit den herstellerspezifischen Updates versorgen zu können, muss vorher entschieden werden wie dies geschieht, zum Beispiel über HTTPS. Für die Kommunikation im Netzwerk sollte auf TCP/IP und DNS gesetzt werden. Für die sichere Kommunikation zu anderen Komponenten, wie Druckservern oder Endgeräten, wird eine Absicherung mittels SSL/TLS empfohlen, dafür bietet sich die Nutzung des IPP (Internet Printing Protocol) an. SNMPv3 sollte, sofern es genutzt wird, nur einen lesenden Zugriff besitzen. Bei der Nutzung von IPv4 sollte das entsprechende v6-Pendant, zum Beispiel DHCPv6, deaktiviert werden. Das gleiche gilt auch umgekehrt bei der Nutzung von IPv6.

Alle nicht benötigten Protokolle und Dienste sollten deaktiviert werden.

Es ist daher zu prüfen, ob Protokolle wie AirPrint, APIPA, Bonjour/Apple, BOOTP/RARP, SMB/CIFS, FTP, LDAP, LLMNR, mDNS, NetBIOS, NFS, SLP, WINS, WS-Print, WS-Discovery, TELNET und SMTPIMAP/POP3 benötigt werden. Falls nicht sollten entsprechende Protokolle deaktiviert werden.

Auch die Nutzung von USB-Ports zum Druck sollte durch eine Sperrung vermieden werden. Zudem sollten Drucker und Multifunktionsgeräte in eigenen von Client und Server getrennten Netzwerksegmenten, beispielsweise VLANs, organisiert werden. Eine Kommunikation mit anderen Segmenten sollte geregelt sein, zum Beispiel über Printserver/Accounting-Server. Über die genannten Server kann auch die Kommunikation zwischen Multifunktionsgeräten und Druckern zum Dienstleister ermöglicht werden, um den Tonerstand abzufragen oder einen anderen Service zu gewährleisten. Bei der Kommunikation sollte, neben dem Einsatz eines Accounting-Servers, auch ein Standardprotokoll mit einem Standard-Port verwendet und freigeschalten werden.

WEITERE TIPPS

- Festlegen der benötigten Funktionen, Protokolle und Dienste ggf. nach Geräteklassen.
- Standard-Admin-Passwörter der Drucker und Multifunktionsgeräte ändern und jedem Gerät ein individuelles starkes Passwort geben. Dies kann beispielsweise aus einer komplexen, der Allgemeinheit unbekannten Zeichenkombination ergänzt mit Teilen des internen Namens des Multifunktionsgeräts, des Modell, der Seriennummer oder der Netzwerk-ID bestehen. (siehe LSI-Info A#03_Umgang_mit_Passwörtern)
- Bei auftretenden Sicherheitsvorfällen, zum Beispiel bei Verschlüsselung, sollten auch Druckgeräte betrachtet werden, da einige Modelle Firmware auf Windows Basis besitzen und ebenfalls kompromittiert werden könnten.
- Der Aufstellungsort der Multifunktionsgeräte und Drucker sollte ebenfalls berücksichtigt werden. Der Ort sollte für unberechtigte Personen möglichst nicht zugänglich sein. Die Konsole sollte generell mit einer PIN gesperrt sein.
- Für den Druck sensibler Dokumente und vor allem für zugängliche Standorte sollte der „Follow-Me“-Druck beziehungsweise das „vertrauliche Drucken“ eingerichtet und verwendet werden. Hiermit wird der Druckjob in einer Warteschlange zwischengespeichert und kann nur vom Auftraggeber nach erfolgreicher Anmeldung, mittels PIN oder Chipkarte, am Gerät gestartet werden.
- Um dem Abgreifen von Daten entgegenwirken zu können, sollten Druckaufträge verschlüsselt übertragen werden.

- Bei Multifunktionsgeräten und Druckern sollte eine Festplattenverschlüsselung mit einem möglichst langen Schlüssel eingesetzt werden.
- Gelöschte Druckaufträge sollten sicher gelöscht werden. Das heißt die gelöschten Daten dürfen nicht rekonstruierbar sein. Dies kann zum Beispiel mit dem Überschreiben der Daten durch Zufallswerte realisiert werden.
- Wenn die Auslieferung und Einrichtung des Multifunktionsgeräts oder Druckers durch einen Dienstleister erfolgt, sollte die durch die Kommune festgelegte Konfiguration durch den Dienstleister umgesetzt werden. Dies kann vertraglich festgelegt werden.
- Multifunktionsgeräte sollten auch im Notfallvorsorgekonzept berücksichtigt werden.
    - Ausfallzeiten sollen so gering wie möglich gehalten werden, zum Beispiel durch redundante Print- und Accounting-Server und eine gleichmäßige Aufteilung der Druckgeräte auf die Server.
    - In kritischen Umgebungen sollten Ersatzgeräte bereitgehalten werden.
    - Auf angemessene Reaktionszeiten in Wartungsverträgen sollte geachtet oder eine Liste mit Fachhändlern für Ersatzgeräte und -teile geführt werden.

QUELLEN UND WEITERE INFORMATIONEN

- BSI IT-Grundschutz: Baustein SYS.4.1: Drucker, Kopierer und Multifunktionsgräte
- Drucker und Multifunktionsgeräte im Netzwerk:
  https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_015.pdf
- LSI-Info A#03 Umgang mit Passwörtern :
  https://www.lsi.bayern.de/mam/aktuelles/lsi-info_a03_umgang_mit_passwoertern_v1.01.pdf
- BayIT-SiR 13: 5. Regelungen (nur im Behördennetz abrufbar)
  https://bayernrecht.beck.de/Bcid/Y-100-G-BayVV_2003_4_F_988_217

KONTAKT

Weitere Informationen finden Sie unter:

https://lsi.bayern.de/kommunen/

Für Unterlagen und Beratung wenden Sie sich bitte per E-Mail an:

Beratung-Kommunen@lsi.bayern.de.

Gerne ist das kommunale Beratungsteam auch telefonisch unter 0911 21549-523 für Sie erreichbar.

Landesamt für Sicherheit in der Informationstechnik – Leitfaden T#09 Drucker (Stand: 06.12.2022)