Jailbreaking Your MFP for More Security

—

MFPs, sensible Druckdaten und IT-Sicherheit: Ein Erfahrungsbericht

Kurzinhalt

Aktuelle MFPs (Multi Function Printer) bieten verschiedene Möglichkeiten, die Druckdaten vor unberechtigtem Zugriff zu schützen. Mittlerweile stehen eine Vielzahl von Erweiterungen zur Absicherung der Geräte zur Verfügung, wie beispielsweise IPsec, das sichere Löschen, die Verschlüsselung der Festplatte oder auch die Authentifizierung der Benutzer gegen eine Windows-Domain. Im Rahmen des Vortrags wird insbesondere der Aspekt von Angreifern mit temporärem physischen Zugriff auf die Geräte sicherheitskritisch betrachtet. Dies geschieht am Beispiel eines aktuellen MFPs der Firma Canon, die generellen Ergebnisse sind jedoch vermutlich auf andere Geräte und Hersteller übertragbar.

Der Autor arbeitet in einem sicherheitskritischen Bereich, in dem an alle technischen Geräte bestimmte Mindestanforderungen an die Datensicherheit und -sparsamkeit gestellt werden. Insbesondere wurde gefordert, dass Druckdaten nur solange wie unbedingt notwendig auf dem Gerät vorliegen und anschließend sicher gelöscht werden. Dies soll verhindern, dass durch gezielten Diebstahl des MFPs oder auch nur der Festplatte auch sensible Daten erlangt werden können. Im Laufe des letzten Jahres wurde nach einer entsprechenden Evaluierung ein MFP des Typs C5051i der Firma Canon angeschafft, ausgestattet mit einer optionalen Komponente für das sichere Löschen von Druckdaten. Dieser MFP wird als Fallstudie im Rahmen des Vortrags verwendet.

Schon im Testbetrieb mit unkritischen Druckdaten zeigte sich, dass obwohl das Gerät explizit mit der Option des sicheren Löschens ausgestattet war, diese Funktionalität im Gerät nur unzureichend implementiert war. Der MFP speicherte die Druckjobdaten offensichtlich selbst über einen Neustart hinweg auf der Festplatte, sodass mindestens Daten wie Titel und Seitenzahlen oder auch die Telefonnummern von ein- und ausgehenden Fax-Übertragungen vorliegen. Widersprüchlicherweise spricht Canon selber davon, dass sämtliche Datenspuren restlos vernichtet werden („overwrites any traces of data“). Interessant hierbei ist, dass die Funktion des sicheren Löschens Common Criteria EAL3 zertifiziert ist. Erst bei genauerer Durchsicht der Zertifizierungsunterlagen zeigt sich, dass anscheinend nicht das restlose Löschen aller Daten, sondern nur der Druckbilddaten zertifiziert wurde. Da der lokale Servicepartner wie auch Canon das ungewünschte Verhalten nicht ändern konnten, wurde die Firmware des MFPs schließlich selbstständig angepasst und um die Funktion des sicheren Löschen erweitert.

Der Zugriff auf das Betriebssystem des MFP ist dabei denkbar einfach. Die Festplatte

enthält eine auf Debian GNU/Linux basierende Betriebssysteminstallation. Im Gerät ist i686-Hardware verbaut, sodass auch wenig versierte und wenig Hardware-affine Personen sehr leicht eigene Anpassungen vornehmen können. Was in diesem speziellen Fall eher für eine einfache Lösung des Problems spricht, kann im Allgemeinen zu einem sehr großen Risiko beim regulären Betrieb des MFPs werden. Ist ein solches Gerät einem Angreifer nur kurze Zeit unbeobachtet zugänglich, so kann dieser durch das Lösen einer einzelnen Schraube Zugriff auf die Festplatte nehmen. Hierdurch stehen quasi alle Möglichkeiten offen: Das Gerät selber kann trojanisiert werden und so Druckjobs abgefangen und Anmeldedaten von Benutzern aufgezeichnet werden. Zudem kann der MFP für andere Zwecke oder Angriffe missbraucht werden. Der Vortrag stellt das Vorgehen bei der Analyse, interessante Auffälligkeiten auf dem System sowie die Anpassungen der Firmware vor.

Schon vor der Auswahl des Geräts wurde vermutet, dass viele MFPs herstellerseitige Wartungsschnittstellen (Backdoors) implementiert haben, um Servicetechnikern an den normalerweise vorhandenen Authentifizierungsmechanismen vorbei Zugriff auf die Geräte zu ermöglichen. Es stellte sich heraus, dass diese Vermutung richtig ist. Eine einfache Tastenkombination ruft ein umfangreiches verstecktes Servicemenü auf. Hier lassen sich viele Druckparameter einstellen. Aber auch viele sicherheitsrelevante Parameter sind hier und teilweise nur über dieses, dem normalen Käufer nicht zugängliche, Menü erreichbar. Dies bedeutet in der Praxis, dass ein lokaler Angreifer mit einfachen Tastenkombinationen am Gerät zum Beispiel die potentiell vorhandene Verschlüsselung der Festplatte oder auch das sichere Löschen einfach abschalten kann. Auch ist es möglich, dass Administratorpasswort zurückzusetzen und so die normalen Administrationsfunktionen zu erreichen. Angreifern sind hier Tür und Tor geöffnet. Leider weigern sich Servicepartner regelmäßig, Informationen zu diesen Funktionen überhaupt herauszugeben. Über Drittquellen lässt sich aber die offizielle Dokumentation der Schnittstelle beschaffen. Eine Absicherung der Funktion ist bei vielen älteren Canon-MFPs nicht vorgesehen, die Tastenkombination kann lediglich zwischen zwei festen und bekannten Tastenkombinationen gewechselt werden. Erst in neueren Versionen der MFP-Software lässt sich überhaupt ein Kennwort für die Funktion setzen. Bei der Rücksprache mit einem Servicetechniker, der Canongeräte im großen Stil betreut, zeigte sich, dass diese Funktion offensichtlich kaum genutzt wird, was bedeutet, dass vermutlich viele MFPs von Canon anfällig für Angriffe am Bedienfeld sind. Auch hier stellt sich die Frage, welchen Vorteil die Zertifizierung einzelner Funktionen und das Vertrauen der Kunden darauf bietet, wenn die gesamte Sicherheit so einfach kompromittiert werden kann. Auch die von Canon bereitgestellte Dokumention zu Absicherung von MFPs geht nicht auf die Serviceschnittstelle ein.

Der Vortrag orientiert sich zwar an einem speziellen verbreiteten Gerät, allerdings sind die vorgestellten Problematiken insbesondere von Angreifern mit physischem Zugriff auf den MFP vermutlich leicht übertragbar. Es stellt sich grundsätzlich die Frage, ob MFPs überhaupt in der gängigen Weise eines großen Geräts an zentraler Stelle sicher betrieben werden können oder ob die Geräte nicht generell als potentiell kompromittiert betrachtet werden sollten. Der Vortrag gibt Anregungen, die aktuellen Sicherheitskon-

zepte bezüglich MFPs zu überdenken und gegebenenfalls anzupassen. Er zeigt an einem einfachen und verständlichen Beispiel mit viel Praxisbezug, wie simpel eine Kompromittierung einer oft als Blackbox angesehenen Hardware möglich ist und was aus der Kompromittierung für die Sicherheit des gesamten Netzwerk folgt. Die vorgestellten Erfahrungen sollen helfen, bei der eigenen Beschaffung entsprechender Geräte die richtigen Anforderungen und Fragen stellen zu können, so dass zum Beispiel potentielle vorhandene Servicezugänge zumindest dokumentiert sind.