KONICA MINOLTA

IHRE DATEN
IN SICHEREN HÄNDEN

SySS
THE PENTEST EXPERTS.

Giving Shape to Ideas

DATEN SPEICHERN JA, **ABER BITTE AUF NUMMER SICHER**

Multifunktionale Systeme verfügen heutzutage über vielfältige Funktionen, die natürlich auch speicherintensiv sind und demnach schon lange nicht mehr ohne zusätzlichen Datenspeicher in Form einer internen Systemfestplatte auskommen. Damit bleibt für viele Kunden die Frage, was am Ende einer Vertragslaufzeit mit den persönlichen Daten auf der Festplatte geschieht. Wie sicher werden diese gespeichert? Lassen sie sich wieder rekonstruieren?

Um die Daten auf der internen Festplatte optimal zu schützen, bietet Ihnen Konica Minolta bei den bizhub Systemen bereits im Standard eine Vielzahl an Sicherheitsfunktionen und setzt damit einen marktführenden Maßstab. Ebenso die Norm: Alle bizhub Systeme von Konica Minolta werden selbstverständlich nach Common Criteria „EAL3 Augmented with ALC_FLR.2“ zertifiziert.

Doch was steckt im Detail dahinter?

Die Konica Minolta bizhub Systeme der neuesten Generation verfügen zum Schutz der Systemfestplatte bereits im Standard über folgende Funktionen:

- Die Festplatte wird durch ein Kennwort geschützt, welches im BIOS verankert ist.
- Die gespeicherten Daten werden auf Basis des Advanced Encryption Standard (AES) verschlüsselt, der die 256-Bit-Schlüssellänge unterstützt.
- Die Daten auf der Festplatte können durch 8 verschiedene Modi überschrieben werden, angefangen vom Überschreibungsmuster 0x00 (Japan Electronic & Information Technology Association, russischer Standard GOST) bis hin zur 7-fachen Überschreibung mit verschiedenen Datenmustern inkl. Verifizierung (US Air Force Standard AFSSI5020).
- Ergänzend erfolgt eine temporäre Datenüberschreibung für z. B. kurzzeitig ausgelagerte Druckdaten, die je nach Konfiguration umgehend mit einfachem Muster 0x00 oder mit 0x00/0xff/0x61 überschrieben werden, mit anschließender Verifizierung.
- Auf dem Dokumentenserver gespeicherte Daten können nach vordefinierten Zeiten automatisch gelöscht werden.

Die bei den bizhub Systemen verwendeten Mechanismen gehen teilweise sogar über die standardmäßigen Schutzmaßnahmen eines Betriebssystems hinaus. Das heißt für Sie als Anwender: Ihre Daten sind über die vielfältigen Sicherheitsfeatures der Festplatte bestens geschützt. Somit ist gewährleistet, dass die Anwenderdaten auch vertraulich bleiben. Bei Bedarf können Sie die Daten dann nach High-End-Standards nicht rekonstruierbar löschen.

OBJEKTIV BETRACHTET
EINE SICHERE SACHE

Für Konica Minolta hat die Sicherheit der Kundendaten oberste Priorität. Im Zuge eines sogenannten Penetrationstests prüfte die Fa. SySS GmbH bei einem bizhub C284 System die Qualität der Datensicherung auf Herz und Nieren.

Wer ist die Firma SySS GmbH?

1998 vom heutigen Geschäftsführer Sebastian Schreiber gegründet, beschäftigt die SySS GmbH heute ein Team von 47 Mitarbeitern. (Stand: 14.05.2013).

Das Unternehmen berät genauso unabhängig wie objektiv. Bei den Tests kommen deswegen auch überwiegend freie Softwareprodukte zum Einsatz. Der Geschäftsführer Sebastian Schreiber ist in Fachkreisen bekannt durch seine Auftritte auf Messen, wie z. B. der CeBIT oder der it-sa, sowie durch Fernsehauftritte bei Stern TV und genießt in der Branche ein sehr hohes Ansehen. Dies untermauert auch die Kundenliste der SySS GmbH mit Referenzen von über 60 Unternehmen, die zu den Top 100 in Deutschland gehören.

Nähere Informationen finden Sie unter www.syss.de.

Sebastian Schreiber

Was wurde getestet?

Für den Test wählten wir das Konica Minolta System bizhub C284 mit der Firmware-Version A2X00Y0-3000-G00-56 (ProductID: 1.3.6.1.4.1.18334.1.1.1.2.1.84.2.1). Das getestete System wurde vorab gemäß den Konica Minolta bizhub SECURE Richtlinien geschützt – das heißt, es wurde die Festplattenverschlüsselung aktiviert sowie mit individuellem 20-stelligen alphanumerischen Kennwort versehen und es wurde ein 20-stelliges alphanumerisches Festplattenkennwort vergeben.

Während des Prüfverfahrens lag das Hauptaugenmerk auf der Extraktion von Daten von der Festplatte, zusätzlich testeten die Sicherheits-Spezialisten die Angreifbarkeit über das LAN, das Webinterface sowie die Netzwerkdatensicherheit.

Wie wurde getestet?

Vorab fertigten die Prüfer eine forensische Kopie der internen Festplatte an und extrahierten die Daten. Das Resultat der Testreihe: Der SySS GmbH war es nicht möglich, Daten aus dem Printer Cache zu extrahieren!

KONICA MINOLTA

„Die SySS GmbH konnte keine Unregelmäßigkeiten in den verwendeten Löschmethoden des Multifunktionsdruckers feststellen. Nach dem Löschen der Festplatte war es nicht möglich, gedruckte Dokumente zu extrahieren. Im Hinblick auf die Datensicherheit hat die SySS GmbH keine Einwände, mit der implementierten Methode Druckdaten sicher zu löschen.

Ein Versuch, jedwede Daten wieder herzustellen, nachdem die Datenüberschreibungsmethode ‚Modus 8' erfolgreich durchgeführt wurde, blieb erfolglos. Die SySS GmbH konnte keine Schwächen in der Sicherheit der Datenspeicherung von Druckdaten feststellen. Die SySS GmbH empfiehlt, um einen wirksamen Schutz gegen Brute-Force-Angriffe zu bieten, sehr starke Verschlüsselungsphrasen mit mindestens 20 oder mehr Zeichen zu verwenden.

Ein mögliches Angriffsszenario besteht darin, den Linux-Computer, der für den Betrieb des Druckers zuständig ist, durch das Ausnutzen von noch nicht bekannten Schwachstellen, beispielsweise über den am Drucker erreichbaren Internet-Browser, zu kompromittieren. Im Rahmen des Tests konnte die SySS GmbH keine Schwächen in der Druckdatenverarbeitung des Gerätes feststellen."

Statement der Firma SySS GmbH

```
Disk  /dev/sdc - 320 GB / 298 GiB (RO) - WDC WD3200BUCT-63TWBYO
Partition                      Start        End    Size in sectors
No partition                 0  0    1 38913  80 63 625142448 [Whole disk]

0 files saved in /media/0ce86979-8000-4bc9-97b1-d1ede3731670/recup_dir directory.
Recovery completed.
```

Fazit: Auch beim Thema Datensicherheit überzeugen die bizhub Systeme mit höchsten Standards.