

Stellungnahme

Sicherheit bei digitalen Reprografiegeräten (Kopierern, Druckern und Multifunktionsgeräten)

04.06.2008

Seite 1

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.200 Unternehmen, davon 900 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software, IT-Services und Telekommunikationsdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für bessere ordnungspolitische Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel. +49. 30. 27576-0
Fax +49. 30. 27576-400
bitkom@bitkom.org
www.bitkom.org

Generelle Aussagen zur Datensicherheit auf Reprografiegeräten

In einem TV-Bericht am 3.6.2008 wurden angebliche Sicherheitslücken bei digitalen Reprografiegeräten (Drucker, Kopierer, Multifunktionsgeräte) thematisiert. Der Bericht weist zum einen zu Recht auf ein Sicherheitsproblem hin: Viele Anwender sind sich nicht bewusst, dass die Daten ihrer Ausdrucke, Scans oder Kopien auf den Festplatten von Reprografiegeräten gespeichert werden, etwa in Copyshops, aber auch in Unternehmen. Deshalb ist die Aufklärung der Verbraucher durch die Medien und die Hersteller dieser Systeme sehr wichtig.

Ansprechpartner

Marc Thylmann
Pressesprecher
Technologien & Dienste
Tel. +49.30.27576-111
Fax +49.30.27576-51-11
m.thylmann@bitkom.org

Allerdings wird in dem Bericht auch behauptet, dass die mangelnde Ausstattung der Geräte zu Sicherheitslücken führt. Gebe man ein – im Internet verfügbares – Service-Passwort bei einem solchen System ein, so erhalte man Administratorrechte über das System und könne Ausdrucke, Kopien, Scans umleiten und manipulieren. Fakt jedoch ist: Das Service-Passwort – das Service-Techniker bei Wartungsarbeiten nutzen – ermöglicht keinen Zugang zu gedruckten Dateien, sondern lediglich zu den Hardware-Spezifikationen des Systems. Bei dem gestellten Fallbeispiel konnte die Kontrolle über den Kopierer mit dem Service-Passwort nur deshalb erlangt werden, weil entgegen der Sicherheitsrichtlinie ein zusätzliches Passwort nicht aktiviert und personalisiert wurde.

Dr. Ralph Hintemann
Bereichsleiter
IT-Infrastruktur & Digital
Office
Tel. +49.30.27576-250
Fax +49.30.27576-409
r.hintemann@bitkom.org

Es gibt also kein spezielles Sicherheitsproblem bei Reprografiegeräten. Bei der richtigen Sicherheitsstrategie von Unternehmen und dem nötigen Problembewusstsein wird ein Höchstmaß an Sicherheit erreicht. Zwar sind Dokumente auf Zwischenspeichern in solchen Geräten von sich aus nicht Zugangsgeschützt. Alle im BITKOM organisierten Anbieter von Druckerhardware bieten passende Hard- und Softwarelösungen an. Die Lösungen entsprechen den international geforderten Sicherheitsstandards.

Präsident

Prof. Dr. Dr. h. c. mult.
August-Wilhelm Scheer

Hauptgeschäftsführer

Dr. Bernhard Rohleder

Dazu gehören unter anderem die Netzwerk-Authentifizierung (für den Zugriff auf das System müssen Anwender einen Benutzercode und ein Passwort eingeben), geschütztes Drucken (vor dem Ausdruck geschützter Jobs muss direkt am Bedienpanel des Systems ein Passwort eingegeben werden), ein Data Security Kit (nach Abschluss jedes Druck-, Kopier- oder Scanauftrages werden alle Daten, die

Stellungnahme

Sicherheit bei digitalen Reprografiegeräten Seite 2

während der Ausführung auf der Festplatte gespeichert wurden, gelöscht und eine Datenüberschreibungs-Funktionalität, die Daten aus dem Speicher oder von der Festplatte des Systems löscht, indem diese mit beliebigen Zeichen überschrieben werden.

.....
Genaue Informationen zu den Sicherheitsfunktionen der Reprografiegeräte gibt es bei den jeweiligen Herstellern.
—