

## ***Merkblatt zum datenschutzgerechten Einsatz der Multifunktionsgeräte***

Beim Einsatz der Multifunktionsgeräte ergeben sich folgende **Datenschutzprobleme**:

1. Auf den Geräten ist ein Webserver installiert, über den mittels des „http“-Protokolls Druck- und Fax-Journale einsehbar sind. Weiterhin ist dies mit einer Software, die man sich von der Internet-Seite von NRG herunterladen kann, über das SNMP-Protokoll möglich. Anhand sprechender Dateinamen (z. B. „Kündigung von Herrn Müller“, „Sicherheitsrisiken beim Einsatz des neuen BMW-Modells“) können sensible Informationen in Erfahrung gebracht werden. Die Faxjournale enthalten u.a. die vollständigen Faxnummern der Adressaten. Über die Inverssuche kann der Adressat herausgefunden werden.
2. Das Standard-Administrator-Passwort ist einfach zu erraten. Mehrere Fehlversuche bei der Eingabe des Administrator-Passwortes führen nicht zum Sperren des Zugangs.
3. In der Default-Einstellung speichern die Multifunktionsgeräte Dokumente beim Drucken, Kopieren, Scannen und Faxen - teilweise aus technischen Gründen (z. B. Mehrfachkopien, Sortierung etc.) - in einem geschützten Bereich, der auch nicht vom Administrator einsehbar ist. Wenn jedoch die Default-Einstellung geändert oder beim Kopieren, Scannen oder Faxen bewusst die Option „Dokument bzw. Datei speichern“ gewählt wird, kann das Schriftstück von anderen eingesehen werden.

### **Maßnahmen:**

- A) Die Beseitigung der Datenschutz-Probleme erfolgt seitens der Firma NRG durch folgende Maßnahmen:*

Die Firma NRG installiert eine neue Firmware, wodurch über das „http“-Protokoll nur noch mit dem Administrator-Kennwort Einblick in die Druck- und Faxjournale genommen werden kann. Das http-Protokoll kann dann eingeschaltet werden/bleiben. Darüber sind Angaben wie Füllstand des Toners, Anzahl der Druckseiten etc. noch einsehbar.

- B) Die Leiter der Organisationseinheiten veranlassen für ihren Bereich folgende Schutzmaßnahmen:*

1. Über das SNMP-Protokoll können die Druck- und Faxjournale wohl noch eingesehen werden. Deshalb ist das SNMP-Protokoll abzuschalten.
2. Es wird ein qualifiziertes Administrator-Kennwort vergeben (entsprechende Hinweise enthält der IT-Grundschutz-Katalog, Abschnitt M 2.11 „Regelung des Passwortgebrauchs“, zu finden unter <http://www.bsi.bund.de/gshb/deutsch/m/m02011.htm>).

3. Es wird überprüft, ob die Default-Einstellungen des Gerätes dahin gehend geändert wurden, dass **alle** verarbeiteten Dokumente automatisch auf dem Dokumentenserver gespeichert werden. Wenn ja, sollten diese Einstellungen zurückgesetzt werden. Zu Alternativen wird auf das Infoblatt von NRG verwiesen.
4. Auf dem Dokumenten-Server sollten nur Vorlagen ohne sensiblen Inhalt gespeichert werden. Außerdem sollten die sicherheitsrelevanten Einstellungen nicht geändert werden.

**Zu den „sensiblen Daten“ gehören neben den personenbezogenen Daten auch die Forschungsdaten. Der Schaden für die RWTH durch das Bekanntwerden geheimer Forschungsdaten dürfte immens sein. Wer entgegen dieser Maßnahmen handelt, trägt die volle Verantwortung, wenn Unbefugte auf diesem Wege Kenntnis von sensiblen Daten erlangen.**