Fehler in TPM Firmware

Die Verschlüsselung von Datenträgern in modernen Computern und mobilen Endgeräten wird durch die TPM Technologie (Trusted Platform Module) erreicht. TPM kann verwendet werden, wenn das jeweilige Gerät über den dazu benötigten und fest eingebauten Chip verfügt und die Funktion aktiviert ist.

Bei Geräten bestimmter Hersteller kommen TPM Lösungen von Infineon zum Einsatz (z. B. Fujitsu). Seit Herbst 2017 wird von dort und durch Microsoft eine Aktualisierung der Firmware der TP-Module empfohlen. Die Notwendigkeit des Updates wird durch die Hersteller mit einer entdeckten Schwachstelle bei der Erzeugung der Schlüssel begründet. Durch das Update können die alten bzw. anfälligen Schlüssel entfernt werden. Die Hersteller machen darauf aufmerksam, dass es notwendig sein kann die Datenträger im Zuge der Aktualisierung der TPM Firmware einer Entschlüsselung und Wiederverschlüsselung zu unterziehen.

Für nähere Informationen wenden Sie sich bitte an Ihre IT Administration oder den Gerätehersteller.