USB-Sticks, die etwa als Werbegeschenke verteilt werden, können Schadsoftware enthalten.

Risiken beim Aufladen von Geräten über die USB-Schnittstelle: Smartphones können Träger von Schadsoftware werden.

Einfallstor für Schadsoftware

USB-Sticks können Schadsoftware enthalten, die auf andere Geräte übertragen werden kann. IT-Experten des Innenministeriums geben Tipps zur Risikominimierung.

Über eine USB-Schnittstelle (Universal Serial Bus) können verschiedene Geräte an einen Computer angeschlossen werden. Dies umfasst etwa Maus, Tastatur, Digitalkameras und externe Speichermedien, wie USB-Sticks. Auch Verbindungen zu externen Adaptern für WLANs, Bluetooth, UMTS und andere erfolgen über die USB-Schnittstelle. USB-Devices haben sich zu gefährlichen Einfallstoren für Schadsoftware entwickelt, deren Auswirkungen von Benutzern häufig unerkannt bleiben. Durch einen sorgfältigen Umgang mit USB-Devices lassen sich Gefahren vermindern.

Virenschutz einsetzen. Wird ein infizierter USB-Stick an einen Computer angesteckt, kann Schadsoftware ohne Zutun des Benutzers übertragen werden. Diese stammt entweder von kompromittierten Geräten oder kann sich auf manipulierten USB-Sticks befinden, die beispielsweise als Werbegeschenk verteilt werden. Die Weitergabe eines infizierten USB-Sticks und dessen Verwendung auf anderen Geräten ermöglicht die Verbreitung von Schadsoftware. Datenverlust, Veränderung von Daten, Übermittlung von Informationen an Dritte bis hin zu technischen Störungen und Fehlverhalten des infizierten Rechners können die Folgen sein.

Experten raten, einen Virenschutz auf dem PC zu installieren und diesen aktuell zu halten. Moderne Antivirenprodukte führen automatisiert eine Schadsoftware-Überprüfung auf USB-Speichermedien durch, erkennen diese und stellen Methoden zu deren Bereinigung zur Verfügung.

Daten verschlüsseln. USB-Sticks können große Mengen an Daten speichern. Um einen Missbrauch und eine unerwünschte Datenweitergabe zu vermeiden (z. B. durch Diebstahl oder Verlust des USB-Sticks), sollten die darauf befindlichen Daten verschlüsselt werden. Eine von vielen Möglichkeiten zur Verschlüsselung von Festplatten und USB-Sticks bietet das „Open-Source"-Verschlüsselungswerkzeug *TrueCrypt*. Eine weitere Sicherheitsmaßnahme ist der *TrueCrypt*-Container. Darunter versteht man einen verschlüsselten Bereich für sensible Daten am USB-Stick. Dieser Container erscheint im Dateimanager neben den unverschlüsselt abgelegten Dateien als vollständige Datei auf. Um auf die unverschlüsselt abgelegten Daten am USB-Stick zuzugreifen ist die Installation von *TrueCrypt* nicht notwendig.

Auch Betriebssystemanbieter stellen Lösungen zur Verschlüsselung von Wechseldatenträgern zur Verfügung. Darüber hinaus gibt es von diversen Anbietern auch vom Betriebssystem unabhängige verschlüsselte USB-Sticks. Der Zugriff auf die Daten ist nur mit einem Kennwort möglich. Eine Verschlüsselungssoftware auf Notebooks oder PCs wird bei diesen USB-Sticks nicht benötigt, da sich diese auf dem USB-Speicher befindet. Unabhängig von der gewählten Verschlüsselung ist auf die Wahl sicherer Passwörter zu achten. Dies wäre z. B. bei einer Kombination von mindestens acht Zeichen, bestehend aus Buchstaben, Ziffern und Sonderzeichen sowie der Berücksichtigung von Groß- und Kleinschreibung der Fall.

Daten sicher löschen. Werden USB-Sticks oder andere Wechseldatenträger weitergegeben oder an fremden Computern verwendet, sollten vorher alle Daten gelöscht werden. Die übliche Datenlöschung der am USB-Stick abgelegten Informationen reicht oft nicht aus, da gelöschte Daten wiederhergestellt werden können. Selbst durch eine vollständige Formatierung des USB-Sticks bleiben Daten wiederherstellbar.

Will man die Wiederherstellung der Daten verhindern und sicher gehen, dass diese vollständig gelöscht werden, sind die Daten zunächst auf konventionelle Weise zu entfernen. Anschließend ist der gesamte Speicherbereich auf dem Wechseldatenträger mit einem speziellen Programm mehrfach zu überschreiben.

Gratisprogramme zum sicheren Löschen von Daten sind beispielsweise „Secure Eraser", „CCleaner" oder „WipeDisk". Kann ein USB-Stick aufgrund eines Defektes nicht überschrieben werden, sollten die einzelnen Speicherchips zerstört werden.

Fotos: Egon Weissheimer

Vorsicht bei USB-Zubehör. Dazu gehören (Funk-)Tastaturen, (Funk-)Mäuse, DVB-T-Sticks für den Fernsehempfang am Computer sowie sonstiges Zubehör wie etwa der USB-Tassenwärmer oder USB-Ventilator. Bei diesen USB-Devices besteht das Risiko, dass sie nicht durch Software, sondern durch Änderung der Hardware (Manipulation oder Präparierung) eine Gefahr für das Gerät darstellen, an dem sie eingesetzt werden.

In USB-(Funk-)Tastaturen eingebaute Chips zum Beispiel können die Tastenanschläge aufzeichnen und diese Informationen (z. B. Passwörter) über das Internet an einen Server übertragen. Bekannt sind auch Manipulationen von USB-Zubehör, die an einem Computer geheime Befehle ausführten oder Schadsoftware installierten. Jedes USB-Device lässt sich so präparieren, dass es vom System als Tastatur wahrgenommen wird und dem Computer „vorgegebene Tastendrücke“ liefert. Je nach Betriebssystem kann durch simulierte Tastendrücke das System sabotiert oder eine Schadsoftware aus dem Internet geladen werden. Beim Einsatz von USB-Zubehör sollte man auf die Herkunft und den sorgfältigen Einsatz achtetn. Fragwürdiges Zubehör sollte mit Vorsicht und auf Geräten mit sensiblen Daten nicht eingesetzt werden.

Risiken beim Aufladen von Geräten über die USB-Schnittstelle. Auch Smartphones können „Träger“ von Schadsoftware werden. Die Malware ist dabei mitunter nicht auf ein Fehlverhalten oder auf Datenmanipulationen am Smartphone ausgerichtet, sondern zielt darauf ab, Computer zu infizieren, an die das Smartphone entweder zum Aufladen des Akkus oder zum Übertragen von Musik oder Fotos angeschlossen wird.

Die Schadsoftware versteckt sich auf dem Smartphone und wird aktiv, sobald das Telefon über die USB-Schnittstelle an den Computer angeschlossen wird. Dadurch kann nicht nur Schadsoftware vom Smartphone auf den Computer übertragen werden, es können auch Daten vom Computer auf das Telefon geladen und unbemerkt weiterversendet werden. Auch für diese Fälle gilt, dass man Sorgfalt walten lässt und beispielsweise sein Smartphone nicht an fremden Computern zum Aufladen des Akkus anschließt. *Manfred Stopfer*