EMPFEHLUNG: IT IM UNTERNEHMEN

Schutz von Daten auf USB-Sticks

Sinkende Speicherpreise führen zu größeren Speicherkapazitäten verfügbarer USB-Sticks.

Diese für den Nutzer sehr vorteilhafte Entwicklung erhöht jedoch auch das Risiko, im Falle des Verlustes erhebliche Mengen privater und/oder sensibler Daten zu verlieren. So können diese leicht in falsche Hände geraten und Vertrauliches kann schnell öffentlich werden.

Um Daten auf Speichermedien, wie USB-Sticks, gegen ungewollten Zugriff zu schützen, existiert eine Reihe von Lösungsansätzen, die für jeweils unterschiedliche Anwendungsfälle geeignet sind. Die Entscheidung für das eine oder andere Verfahren wird vom Schutzbedarf der Daten und nicht zuletzt von den Kosten der Lösung bestimmt.

Bei den verfügbaren Lösungen kann man zwischen Host-basierten und autarken Ansätzen unterscheiden.

1 Host-basierte Lösungen

Der Zugriffsschutz beruht bei Host-basierten Lösungen auf dem Zusammenspiel des USB-Sticks mit einer herstellerspezifischen Authentisierungssoftware, die auf dem PC, an dem der USB-Stick verwendet werden soll, ausgeführt wird. Die Authentisierung wird dabei in der Regel über ein auf dem Host-PC einzugebendes Passwort oder biometrisch durch einen Fingerabdruck-Sensor realisiert. Daher ist die Funktion unmittelbar an das Betriebssystem des betreffenden PCs gekoppelt.

2 Autarke Lösungen

Die zum Schutz der Daten erforderlichen Zugangsinformationen werden bei autarken Lösungen vom USB-Stick selbst z. B. über einen integrierten Fingerabdruck-Sensor und/oder über eine PIN-Eingabe erfasst. Bei dieser Variante ist für die Authentisierung keine Kommunikation mit dem Host-PC erforderlich. Die Schutzmechanismen sind in diesem Fall vollständig auf dem USB-Stick realisiert, was zu einer Unabhängigkeit vom Betriebssystem führt.

Für beide Lösungen gilt jedoch, dass

- bislang keine Standards oder Normen im Bereich der Sicherheitsfunktionen für USB-Sticks existieren. Bei den Schutzmechanismen handelt es sich also um proprietäre Lösungen des jeweiligen Herstellers. Demzufolge ist die Qualität sehr unterschiedlich.
- die Daten auf dem USB-Stick bei Verwendung dieser angebotenen Möglichkeiten vor Zugriff geschützt, aber in den meisten Fällen nicht verschlüsselt sind.

3 Empfehlung

Die in USB-Sticks direkt integrierten Schutzmechanismen sollten grundsätzlich immer Verwendung finden, um Daten bei Verlust vor unbefugtem Lesen zu schützen. USB-Sticks mit integrierter Hardware-Verschlüsselung bieten in der Regel ein deutlich höheres Schutzniveau, als jene, die nur einen Zugriffsschutz verwirklichen, ohne die Daten selbst zu verschlüsseln. Bei allen Verfahren sollte darauf geachtet werden, dass ein Fehlbedienungszähler ein systematisches Durchtesten des Passwortes, der PIN oder eines Fingers[*)] verhindert.

Sind die Anforderung an die Vertraulichkeit sehr hoch, empfiehlt das BSI, sensible Daten auf dem USB-Stick zusätzlich mit einem geeigneten Verschlüsselungsprogramm (z. B. VeraCrypt) zu schützen, wobei sichergestellt sein muss, dass das Passwort den Anforderungen hinsichtlich Länge und zu verwendender Zeichen genügt. So kann ein Maximum an Sicherheit gewährleistet werden. Dieses Verfahren kann auch bei USB-Sticks angewendet werden, die nicht über die beschriebenen Sicherheitsfeatures verfügen.

4 Weiterführende Informationen

1. „NIST-zertifizierte USB-Sticks mit Hardware-Verschlüsselung geknackt“ Quelle: https://www.heise.de/-894962.htm (04.01.2010)
2. „Verpfuschte Sicherheit“ Quelle: c't 2008, Heft 16, S. 44
3. „Halbe Sicherheit: Der Padlock von Corsair schützt Daten bei Verlust vor unbefugtem Zugriff – ein bisschen“ Quelle: https://www.heise.de/-1898308.htm (04.07.2008)

[*)] Bei einem Stick mit Fingerabdruck-Sensor sollte man zusätzlich darauf achten, statt der Fingerkuppen möglichst andere Teile des Fingers zu verwenden, um Angriffe durch Klonen von Fingerabdrücken zu erschweren.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an info@cyber-allianz.de gesendet werden.