Festplattenverschlüsselung

Rubrik: IT-Sicherheit

Die Festplattenverschlüsselung ist ein Verfahren zum Schutz gespeicherter Daten vor unbefugtem Zugriff. Dabei werden die Informationen auf einer Festplatte mithilfe eines kryptografischen Verfahrens verschlüsselt, sodass sie ohne den passenden Schlüssel nicht sinnvoll gelesen werden können. Die Technik wird sowohl bei internen und externen Festplatten als auch bei SSDs eingesetzt und dient insbesondere dem Schutz vertraulicher Daten bei Verlust oder Diebstahl eines Computers.

Bei der Verschlüsselung werden die gespeicherten Daten durch einen mathematischen Algorithmus in eine nicht unmittelbar lesbare Form umgewandelt. Für den Zugriff ist ein geeigneter kryptografischer Schlüssel erforderlich. Moderne Lösungen verwenden häufig den Verschlüsselungsstandard AES (Advanced Encryption Standard), beispielsweise im Betriebsmodus XTS, der speziell für die Verschlüsselung von Datenträgern entwickelt wurde.

Grundsätzlich wird zwischen der vollständigen Datenträgerverschlüsselung und der Verschlüsselung einzelner Partitionen oder Bereiche unterschieden. Bei einer vollständigen Datenträgerverschlüsselung (Full Disk Encryption, FDE) werden die vorgesehenen Datenbereiche eines Laufwerks verschlüsselt. Je nach Verfahren können bestimmte Start- oder Verwaltungsbereiche unverschlüsselt bleiben, damit der Computer den Startvorgang durchführen kann.

Bekannte Lösungen zur Festplattenverschlüsselung sind BitLocker unter Windows, FileVault unter macOS und LUKS unter Linux. Sie ermöglichen die Verschlüsselung von Datenträgern und bieten unterschiedliche Möglichkeiten zur Verwaltung der benötigten Schlüssel. Bei manchen Systemen kann ein Trusted Platform Module (TPM) zur geschützten Aufbewahrung oder Freigabe von Schlüsselmaterial eingesetzt werden.

Nach der erfolgreichen Entsperrung erfolgt die Ver- und Entschlüsselung der Daten normalerweise automatisch im Hintergrund. Programme können dann wie gewohnt auf Dateien zugreifen, ohne dass jede Datei einzeln entschlüsselt werden muss. Moderne Prozessoren unterstützen häufig spezielle Rechenbefehle zur Beschleunigung kryptografischer Operationen, sodass die Verschlüsselung im normalen Betrieb meist nur geringe Leistungseinbußen verursacht.

Eine Festplattenverschlüsselung schützt besonders dann, wenn ein ausgeschalteter Computer oder ein ausgebauter Datenträger in fremde Hände gelangt. Sie verhindert jedoch nicht grundsätzlich den Zugriff durch Schadsoftware oder unbefugte Personen, wenn das Laufwerk bereits entsperrt ist. Auch ein verlorener Verschlüsselungsschlüssel kann problematisch sein,

da sich die gespeicherten Daten ohne geeignete Wiederherstellungsmöglichkeiten unter Umständen nicht mehr entschlüsseln lassen.

Die Festplattenverschlüsselung ist ein wichtiger Bestandteil der IT- und Datensicherheit. Sie wird sowohl auf privaten Computern als auch in Unternehmen eingesetzt, um sensible Informationen vor unbefugtem Zugriff zu schützen. Besonders bei mobilen Geräten ist sie eine sinnvolle Ergänzung zu sicheren Anmeldeverfahren, regelmäßigen Datensicherungen und weiteren Schutzmaßnahmen.

Weiterführende Informationen

Datenträgerverschlüsselung, Vollständige Datenträgerverschlüsselung, Verschlüsselung, AES, BitLocker, FileVault, TPM, Datensicherheit