LU13c - Partitions- und Laufwerksverschlüsselung

Die Partitions- oder Laufwerksverschlüsselung bezieht sich auf den Prozess, bei dem eine gesamte Festplattenpartition oder ein komplettes Laufwerk verschlüsselt wird. Im Gegensatz zur Dateiverschlüsselung, bei der nur einzelne Dateien oder Ordner verschlüsselt werden, wird hier das gesamte Dateisystem und alle darin enthaltenen Daten geschützt. Dies bedeutet, dass selbst wenn jemand physischen Zugriff auf das Laufwerk oder die Partition hat, die Daten ohne den richtigen Entschlüsselungsschlüssel nicht gelesen werden können.

Ein bekanntes Produkt für diese Verschlüsselung ist BitLocker, welches in Windows seit Version 7 enthalten ist. BitLocker ermöglicht die Verschlüsselung von einzelnen Partitionen oder eines gesamten Laufwerks und bietet eine umfassende Sicherheit für die auf dem Laufwerk gespeicherten Daten. Es verwendet starke Verschlüsselungsalgorithmen wie AES (Advanced Encryption Standard) mit einer Schlüssellänge von 128 oder 256 Bit. BitLocker unterstützt auch die Authentifizierungsmethoden wie die Eingabe eines Passworts, die Verwendung eines TPM (Trusted Platform Module)-Chips oder den Einsatz eines speziellen USB-Schlüssels.

Eine andere bekannte Option ist VeraCrypt. VeraCrypt ermöglicht die Erstellung verschlüsselter virtueller Festplatten oder die Verschlüsselung ganzer Partitionen. Es unterstützt verschiedene Verschlüsselungsalgorithmen wie AES, Serpent und Twofish. VeraCrypt bietet auch eine Vielzahl von Authentifizierungsmethoden wie Passwörter, Keyfiles und TPM-Unterstützung.

Es gibt auch spezialisierte Hardware-Lösungen für die Partitionsverschlüsselung wie die Selbstverschlüsselnden Laufwerke (Self-Encrypting Drives, SEDs). Diese Festplatten oder SSDs verfügen über integrierte Hardware-Verschlüsselungsfunktionen und sind in der Lage, Daten automatisch während der Speicherung zu verschlüsseln und zu entschlüsseln.

Die Partitions- oder Laufwerksverschlüsselung bietet einen umfassenden Schutz für alle auf dem Laufwerk oder der Partition gespeicherten Daten und stellt sicher, dass selbst bei physischem Zugriff auf das Gerät keine sensiblen Informationen offengelegt werden. Durch die Verwendung von entsprechenden Produkten können Benutzer eine zusätzliche Sicherheitsebene für ihre Daten implementieren.

---

m231-AnG

Andre Probst, Marcel Suter

From:
https://wiki.bzz.ch/ - **BZZ - Modulwiki**

Permanent link:
https://wiki.bzz.ch/modul/m231/learningunits/lu13/partcrypt

Last update: **2024/03/28 14:07**