LU13b - Dateiverschlüsselung

Die Dateiverschlüsselung ist ein Sicherheitsmechanismus, bei dem einzelne Dateien oder ganze Ordner mithilfe eines Verschlüsselungsalgorithmus in eine unleserliche Form umgewandelt werden. Durch die Verschlüsselung werden die Informationen geschützt und können nur von Personen gelesen werden, die im Besitz des richtigen Entschlüsselungsschlüssels sind. Es gibt verschiedene Arten von Verschlüsselungsalgorithmen, darunter symmetrische und asymmetrische Verschlüsselung.

- Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung wird derselbe Schlüssel sowohl für die Verschlüsselung als auch für die Entschlüsselung verwendet. Der Schlüssel muss sicher zwischen den Parteien ausgetauscht werden, die Zugriff auf die verschlüsselten Dateien haben sollen. Ein bekanntes Produkt für die symmetrische Verschlüsselung ist VeraCrypt.

- Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung werden zwei mathematisch zusammenhängende Schlüssel verwendet - ein öffentlicher Schlüssel zum Verschlüsseln der Datei und ein privater Schlüssel zum Entschlüsseln der Datei. Der öffentliche Schlüssel kann frei zugänglich sein und wird verwendet, um die Datei zu verschlüsseln, während der private Schlüssel geheim gehalten werden muss und zum Entschlüsseln verwendet wird. Ein bekanntes Produkt für die asymmetrische Verschlüsselung ist Pretty Good Privacy (PGP).

- Cloud-Speicher-Verschlüsselung

Für die sichere Speicherung von Dateien in der Cloud gibt es spezielle Verschlüsselungslösungen. Ein Beispiel dafür ist Boxcryptor, das eine transparente Verschlüsselung für Cloud-Speicheranbieter wie Dropbox, Google Drive und OneDrive ermöglicht. Es verschlüsselt die Dateien auf dem Gerät, bevor sie in die Cloud hochgeladen werden, und sorgt so für zusätzliche Sicherheit und Datenschutz.

- TLS-Verschlüsselung (Transport Layer Security)

Bei der Übertragung von Dateien über das Internet wird häufig TLS (Transport Layer Security) verwendet. Dieses Protokoll ermöglichen eine sichere Kommunikation zwischen einem Client und einem Server. Eine der Hauptfunktionen von TLS besteht darin, die Daten während der Übertragung zu verschlüsseln und so vor Abhören oder Manipulation zu schützen.

Insgesamt bieten Dateiverschlüsselungsprodukte und TLS-Verschlüsselung wichtige Sicherheitsfunktionen, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, sowohl während der Übertragung als auch in Ruhe. Durch die Nutzung dieser Technologien können Benutzer sicherstellen, dass ihre sensiblen Dateien vor unbefugtem Zugriff geschützt sind.

---

m231-AnG

Andre Probst, Marcel Suter

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

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

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