SSH

Inhaltsverzeichnis

- 1. Wofür wird SSH genutzt?
- 2. Wie funktioniert SSH?
- 3. Warum ist SSH sicher?
- 4. Was ist der Unterschied zwischen SSH und einer normalen Anmeldung?
- 5. Was ist ein SSH-Port?
- 6. Warum ist SSH ein beliebtes Angriffsziel?
- 7. Kurz zusammengefasst

SSH steht für Secure Shell und ist eine sichere Verbindungsmethode, um einen entfernten Server zu steuern.

Mit SSH kannst du dich von deinem eigenen Computer aus auf einem anderen Rechner anmelden, zum Beispiel auf einem Linux-Server im Internet.

---

1. Wofür wird SSH genutzt?

SSH wird hauptsächlich genutzt, um:

- sich auf einem Server anzumelden
- Befehle auf einem entfernten System auszuführen
- Server zu verwalten, ohne direkt davor zu sitzen
- Dateien sicher zu übertragen

Gerade bei Linux-Servern ist SSH der wichtigste Zugangsweg.

---

2. Wie funktioniert SSH?

Vereinfacht gesagt passiert Folgendes:

1. Dein Computer baut eine Verbindung zum Server auf
2. Die Verbindung wird verschlüsselt
3. Du meldest dich mit Benutzername und Passwort oder einem Schlüssel an
4. Du kannst den Server über die Kommandozeile steuern

Alles, was du eingibst oder empfängst, ist dabei **verschlüsselt**.

---

3. Warum ist SSH sicher?

Früher wurden oft unverschlüsselte Verbindungen genutzt. Dabei konnten Passwörter mitgelesen werden.

SSH verhindert das, weil:

- alle Daten verschlüsselt übertragen werden
- Passwörter nicht im Klartext gesendet werden
- moderne Verschlüsselungsverfahren verwendet werden

Deshalb steht das „S“ in SSH für **Secure** (sicher).

4. Was ist der Unterschied zwischen SSH und einer normalen Anmeldung?

Bei einem normalen PC sitzt du direkt davor.
Bei SSH steuerst du den Server **aus der Ferne**, oft über das Internet.

Du siehst dabei meist **keine grafische Oberfläche**, sondern arbeitest mit Textbefehlen.

---

5. Was ist ein SSH-Port?

Ein **Port** ist wie eine Tür am Server.
Standardmäßig nutzt SSH **Port 22**.

Über diesen Port weiß der Server, dass es sich um eine SSH-Verbindung handelt.
Der Port kann aus Sicherheitsgründen geändert werden.

---

6. Warum ist SSH ein beliebtes Angriffsziel?

Weil man mit SSH direkten Zugriff auf einen Server bekommt.

Angreifer versuchen oft:

- Benutzernamen zu erraten
- Passwörter automatisch auszuprobieren

Darum sind zusätzliche Schutzmaßnahmen wie:

- starke Passwörter
- SSH-Keys
- geänderter SSH-Port
- Fail2Ban

sehr wichtig.

---

7. Kurz zusammengefasst

SSH ist eine sichere, verschlüsselte Verbindung, mit der du einen entfernten Server über die Kommandozeile verwalten kannst.