Zusammenfassung der wichtigsten Erkenntnisse zum ERR_CERT_INVALID-Fehler

Schritte	Grund	Lösung
1. Uhrzeit überprüfen	Falsche Zeit kann den Vergleich von SSL-Zertifikatsdaten fehlerhaft machen.	Stellen Sie sicher, dass die Uhrzeit auf Ihrem Computer korrekt ist.
2. Chrome aktualisieren	Veraltete Browser-Versionen können zu Zertifikatsfehlern führen.	Installieren Sie die neueste Version von Google Chrome.
3. Zertifikate überprüfen	Ungültige Zertifikate führen zum Fehler.	Klicken Sie auf das Zertifikatsymbol in der Adressleiste und überprüfen Sie Zertifikats-Details.
4. Cache und Cookies leeren	Veraltete Daten im Cache können das Problem verstärken.	Löschen Sie den Cache und die Cookies in den Chrome-Browser-Einstellungen.
5. Zertifikat neu laden	Manchmal kann das Zertifikat beim ersten Laden falsch gehandhabt werden.	Verwenden Sie die Option "Advanced" und laden Sie das Zertifikat neu.
6. VPN/Antivirus deaktivieren	VPNs und Antivirus-Programme können Zertifikate als unsicher markieren.	Deaktivieren Sie VPN und Antivirus-Software temporär und versuchen Sie erneut, auf die Website zuzugreifen.
7. Incognito-Modus testen	Der Incognito-Modus umgeht lokale Daten wie Cache oder Cookies.	Öffnen Sie die Website im Incognito-Modus.
8. Zertifikat-Chain überprüfen	Wenn ein Zertifikat in einer Kette fehlt oder ungültig ist, kann das zu Fehlern führen.	Überprüfen Sie die Zertifikat-Chain in den Zertifikatsdetails.
9. Zertifikat neu ausstellen	Selbstsignierte oder abgelaufene Zertifikate können Ungültigkeitswarnungen auslösen.	Erstellen Sie ein neues Zertifikat, falls möglich, und installieren Sie es ordnungsgemäß auf Ihrem Server.

Detaillierte Schritt-für-Schritt-Anleitung zur Lösung des ERR_CERT_INVALID-Fehlers

1. Überprüfen Sie die Uhrzeit auf Ihrem Computer

Manchmal kann eine falsche Systemzeit zu SSL-Zertifikatsfehlern führen, da der Browser das Zertifikat mit der falschen Uhrzeit abgleicht und es als ungültig erkennt.

Vorgehen:

- **Windows**: Öffnen Sie Einstellungen > "Uhrzeit & Sprache" > "Datum & Uhrzeit" und stellen Sie sicher, dass "Uhrzeit automatisch festlegen" aktiviert ist.
- **macOS**: Gehen Sie zu **Systemeinstellungen** > **Datum & Uhrzeit** und aktivieren Sie die Option, die Zeit automatisch einzustellen.

---

2. Aktualisieren Sie Google Chrome

Ein veralteter Browser kann Probleme beim Verarbeiten von SSL-Zertifikaten haben.

Vorgehen:

- Klicken Sie auf die drei Punkte in der oberen rechten Ecke von Chrome.
- Wählen Sie **Hilfe** > **Über Google Chrome**.
- Chrome sucht automatisch nach Updates und installiert diese, falls verfügbar.

---

3. Zertifikate im Browser überprüfen

Falsche oder ungültige Zertifikate sind oft der Hauptgrund für den ERR_CERT_INVALID-Fehler. Es ist wichtig, das Zertifikat der Webseite zu überprüfen.

Vorgehen:

- Klicken Sie auf das **Sperrschloss**-Symbol links neben der Adressleiste.
- Wählen Sie **Zertifikat** anzeigen (oder einen ähnlichen Punkt je nach dem verwendeten Browser).
- Überprüfen Sie die Gültigkeit des Zertifikats, um festzustellen, ob es abgelaufen oder ungültig ist.

---

4. Cache und Cookies löschen

Veraltete oder fehlerhafte Cache-Daten können verhindern, dass der Browser das richtige Zertifikat lädt.

Vorgehen:

- Gehen Sie zu Chrome-Einstellungen > **Datenschutz und Sicherheit** > **Browserdaten löschen**.
- Wählen Sie "Cookies und andere Websitedaten" und "Bilder und Dateien im Cache" aus.
- Klicken Sie auf **Daten löschen**.

---

5. Zertifikate neu laden

In einigen Fällen kann der Browser das Zertifikat beim ersten Laden einer Seite falsch interpretieren. Manuelles Neuladen kann dies beheben.

Vorgehen:

- Klicken Sie auf **Erweitert** bei der Fehlermeldung und dann auf **Weiter zur Webseite (unsicher)**, wenn Sie sicher sind, dass die Seite vertrauenswürdig ist.
- **ACHTUNG**: Dies sollte nicht die Standardlösung sein und nur verwendet werden, wenn die Ursache klar ist.

---

6. VPN und Antivirus-Software deaktivieren

VPNs und Antivirus-Software greifen häufig in die Zertifikate ein und können diese als unsicher markieren.

Vorgehen:

- **VPN deaktivieren**: Schalten Sie Ihren VPN-Client aus. Falls Sie noch keinen sicheren VPN nutzen, können Sie NordVPN ausprobieren.
- **Antivirus deaktivieren**: Probieren Sie, vorübergehend Ihre Antivirus-Software abzuschalten und erneut zu testen.

---

7. Incognito-Modus verwenden

Der Incognito-Modus speichert keine Daten im Cache oder Cookies, was helfen kann, das Problem zu diagnostizieren.

Vorgehen:

- Öffnen Sie ein **Inkognito-Fenster** durch Klicken der drei Punkte oben rechts und anschließend **Neues Inkognito-Fenster**.
- Besuchen Sie die problematische Webseite erneut.

---

8. Zertifikat-Chain überprüfen

SSL-Zertifikate sind oft in Ketten von mehreren Zertifikaten organisiert. Wenn eines in der Kette fehlt oder abgelaufen ist, tritt der ERR_CERT_INVALID-Fehler auf.

Vorgehen:

- Klicken Sie auf das **Schloss-Symbol** in der Adressleiste.
- Gehen Sie auf **Details** oder **Zertifikat anzeigen**.
- Überprüfen Sie, ob die gesamte **Zertifikat-Chain** vollständig und gültig ist.

---

9. SSL-Zertifikat neu generieren

Falls das SSL-Zertifikat abgelaufen ist oder ein selbstsigniertes Zertifikat verwendet wird, müssen Sie ein neues Zertifikat erstellen und installieren.

Vorgehen:

- Loggen Sie sich beim Anbieter Ihres SSL-Zertifikats ein.
- Erstellen Sie ein neues Zertifikat oder erneuern Sie es und installieren Sie es auf Ihrem Server.
- Wenn Sie Hilfe benötigen, können Plattformen wie Let's Encrypt kostenlose SSL-Zertifikate anbieten.

Zusätzliche Empfehlungen vom Experten

Manchmal ist es verlockend, unsichere Webseiten zu ignorieren und einfach auf „Fortfahren“ zu klicken. **Das sollten Sie nur tun, wenn Sie 100% sicher sind**, dass die Seite vertrauenswürdig ist. In meiner Erfahrung habe ich gesehen, wie Premium-Sicherheitslösungen von zertifizierten Anbietern wie **NordPass** helfen können, sicher auf Seite zuzugreifen und gleichzeitig eine geschützte Verbindung aufrechtzuerhalten. Wenn Sie regelmäßig online sensible Daten eingeben, kann es auch sinnvoll sein, einen Passwortmanager wie NordPass zu verwenden, der auch die Sicherheit Ihrer Passwörter mit starken Verschlüsselungen sicherstellt.

Häufig gestellte Fragen zum ERR_CERT_INVALID-Fehler

1. Warum tritt der ERR_CERT_INVALID-Fehler plötzlich auf?

Der Fehler kann durch mehrere Faktoren verursacht werden, darunter eine falsch eingestellte Systemzeit, abgelaufene oder ungültige SSL-Zertifikate, veraltete Browser-Versionen oder Sicherheitssoftware, die in den SSL-Prozess eingreift.

2. Ist es sicher, „Fortfahren“ zu drücken, wenn ERR_CERT_INVALID angezeigt wird?

Nein, das sollten Sie nur sehr vorsichtig tun. Oft bedeutet dies, dass die Verbindung zu der Seite nicht sicher ist, und Ihre Daten könnten abgefangen oder manipuliert werden.

3. Könnte ein Virus diesen Fehler auslösen?

Ja. In seltenen Fällen können Malware-Programme diesen Fehler erzeugen, indem sie gefälschte Zertifikate in Ihrem System platzieren. Eine vollständige Systemüberprüfung mit einem hochwertigen Antivirus-Programm ist ratsam.

4. Kann eine Webserver-Fehlkonfiguration diesen Fehler auslösen?

Ja, Webserver können fehlerhaft konfiguriert sein, und es können falsche oder abgelaufene Zertifikate installiert sein. In solchen Fällen liegt der Fehler nicht an Ihrem Computer, sondern an der Webseite selbst.

Mit den obigen Schritten dürften die meisten Fälle des ERR_CERT_INVALID-Fehlers schnell und zuverlässig gelöst werden.