Änderung bei RDP-Dateien durch Microsoft-Updates ab April 2026

Erstellt mit Unterstützung von ChatGPT

Kurzbeschreibung

Microsoft hat mit den **Sicherheitsupdates ab April 2026** das Verhalten beim Öffnen von **Remote-Desktop-Dateien (`.rdp`)** geändert.

Seit diesem Update zeigt der Windows-Remotedesktopclient `mstsc.exe` beim Öffnen einer `.rdp`-Datei zusätzliche Sicherheitsdialoge an. Hintergrund ist der Schutz vor Phishing-Angriffen über manipulierte RDP-Dateien. Eine `.rdp`-Datei kann nicht nur das Verbindungsziel enthalten, sondern auch lokale Ressourcen des Benutzers an den entfernten Computer weiterreichen, zum Beispiel Zwischenablage, Drucker, Laufwerke, Kamera oder Smartcards. Microsoft beschreibt diese Änderung ausdrücklich als Schutzmaßnahme gegen missbräuchliche RDP-Dateien.

Temporäre Lösung #1 - Mit GPO/-Reg-Eintrag deaktivieren

Es gibt einen temporären Workaround, der das alte Dialogverhalten wiederherstellt. Der wird derzeit häufig so gesetzt:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Terminal Services\Client]
"RedirectionWarningDialogVersion"=dword:00000001
```

Oder per PowerShell als Administrator:

```
New-Item -Path "HKLM:\Software\Policies\Microsoft\Windows NT\Terminal Services\Client" -Force
| Out-Null
New-ItemProperty `
  -Path "HKLM:\Software\Policies\Microsoft\Windows NT\Terminal Services\Client" `
  -Name "RedirectionWarningDialogVersion" `
  -PropertyType DWord `
```

```
    -Value 1 `
    -Force
```

Das ist für kleine Kunden praktisch, aber sicherheitlich und strategisch unschön. Microsoft hat die Änderung bewusst eingeführt, um RDP-Datei-Missbrauch zu verhindern; ein Workaround kann später wieder entfernt oder geändert werden. Für Kunden ohne Domäne müsstest du ihn manuell, per RMM, Intune, Script, Fernwartung oder Installer setzen.

> Ich würde das nur als **Übergangslösung** einsetzen.

Lösung #2 - RDP-Dateien signieren

> Mircosoft empfiehlt RDP-Dateien mit einem Code-Signing-Zertifikat zu signieren. Das ist auch die Lösung die ich empfehle und in meinem Lösungen einsetzen.

Da inzwischen alle mir bekannten Code-Signing-Zertifikate mit einer 2FA-Lösung arbeiten kommt eigentlich nur noch eine eigene CA in Frage.

Damit ein PC eine signierte RDP-Datei akzeptiert muss die Root-CA, das Signing-Cert und ein Registry-Eintrag vorhanden sein.

Betroffene Systeme

Die Änderung betrifft laut Microsoft unter anderem:

```
Windows 11
Windows 10
Windows Server 2025
Windows Server 2022
Windows Server 2019
Windows Server 2016
Windows Server 2012 R2
Windows Server 2012
```

Die neue Warnlogik gilt für den **Remotedesktopverbindungsclient** beim Öffnen von `.rdp`-Dateien.

Ab wann tritt die Änderung auf?

Die Änderung wurde mit den **April-2026-Sicherheitsupdates** eingeführt.

Für Windows 11 24H2/25H2 ist der relevante Patchstand beispielsweise:

```
April 2026 Sicherheitsupdate
KB5083769
Windows 11 24H2: Build 26100.8246
Windows 11 25H2: Build 26200.8246
```

Neuere kumulative Updates enthalten diese Änderung ebenfalls. Ein PC mit einem älteren Build, zum Beispiel `26200.8039`, hat diese Änderung möglicherweise noch nicht.

Prüfen kann man den Buildstand mit:

```
winver
```

oder per PowerShell:

```
Get-ComputerInfo | Select-Object OsName, OsVersion, OsBuildNumber, WindowsVersion
```

Was hat sich geändert?

Vor dem Update

Vor dem April-2026-Update konnte eine `.rdp`-Datei weitgehend direkt geöffnet werden.

Wenn in der Datei beispielsweise folgende Einstellungen gesetzt waren:

```
redirectclipboard:i:1
redirectprinters:i:1
```

wurden Zwischenablage und Drucker normalerweise automatisch gemäß RDP-Datei aktiviert.

Es konnte zwar weiterhin eine Zertifikatswarnung erscheinen, wenn der entfernte RDP-PC kein vertrauenswürdiges Serverzertifikat hatte, aber die lokalen Ressourcen wurden meistens wie in der `.rdp`-Datei definiert verwendet.

Nach dem Update

Nach dem Update zeigt Windows beim Öffnen einer `.rdp`-Datei zusätzliche Sicherheitsdialoge an.

Microsoft unterscheidet dabei im Wesentlichen zwei Dialogarten:

1. **Einmaliger Erklärdialog beim ersten Öffnen einer `.rdp`-Datei**
2. **Wiederkehrender Sicherheitsdialog bei jeder `.rdp`-Datei**

Microsoft beschreibt, dass beim ersten Öffnen einer `.rdp`-Datei nach dem Update ein einmaliger Hinweis erscheint, der die Risiken von RDP-Dateien erklärt. Nach Bestätigung erscheint dieser Dialog für das Benutzerkonto nicht erneut.

Zusätzlich erscheint bei jeder `.rdp`-Datei ein Sicherheitsdialog, bevor die Verbindung aufgebaut wird. Dieser Dialog zeigt unter anderem:

```
Remotecomputer / Zieladresse
Herausgeber der RDP-Datei
angeforderte lokale Ressourcen
```

Alle lokalen Ressourcen, die durch die `.rdp`-Datei angefordert werden, sind zunächst deaktiviert und müssen vom Benutzer aktiv erlaubt werden. Dazu gehören zum Beispiel Zwischenablage, Drucker, Laufwerke, Kamera oder Smartcards.

Welche Auswirkungen hat das praktisch?

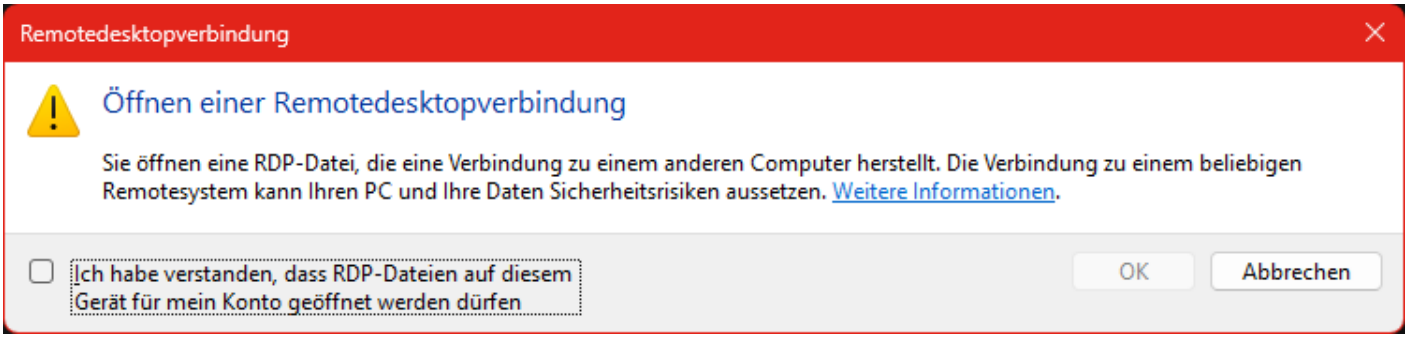
Wenn eine `.rdp`-Datei lokale Ressourcen anfordert, werden diese nicht mehr stillschweigend übernommen. Der Benutzer muss sie im Dialog aktiv auswählen.

Typische betroffene Einstellungen sind:

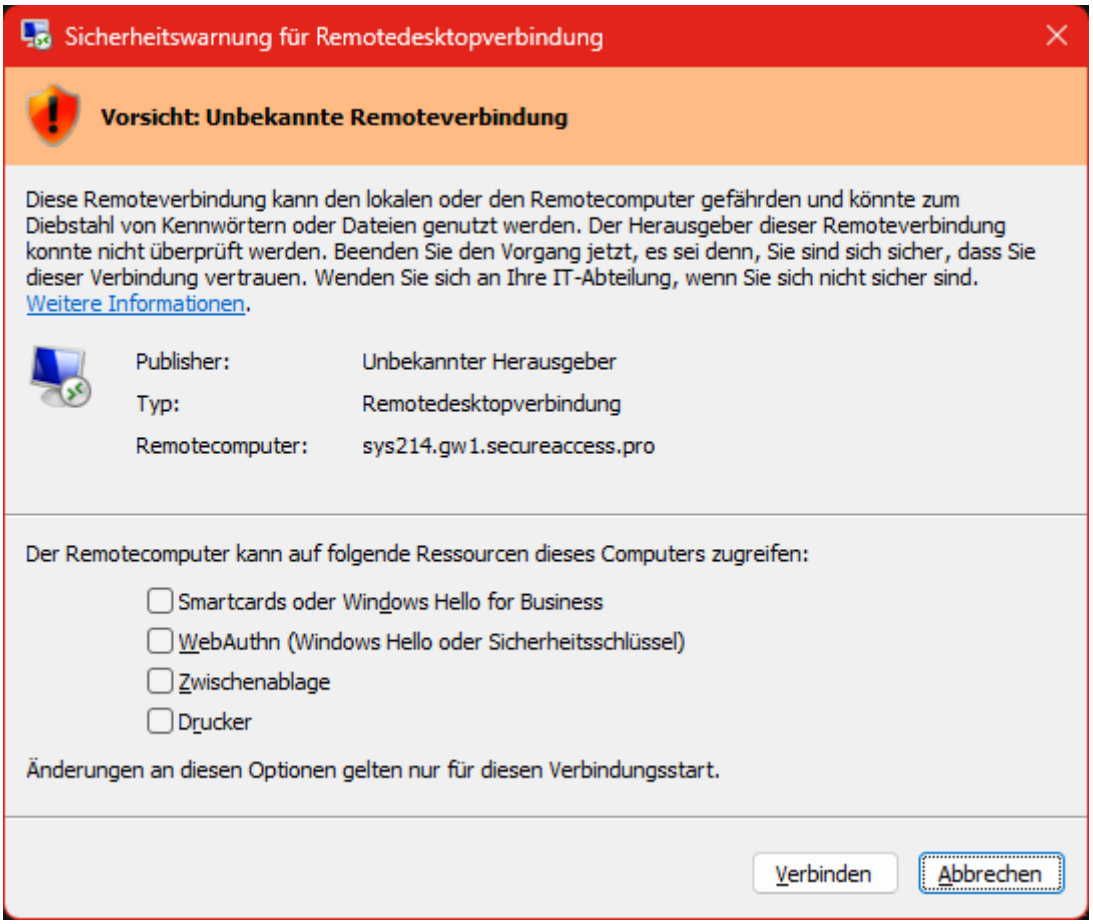
```
redirectclipboard:i:1
redirectprinters:i:1
drivestoredirect:s:*
redirectcomports:i:1
redirectsmartcards:i:1
devicestoredirect:s:*
audiocapturemode:i:1
camerastoredirect:s:*
```

Das führt dazu, dass Benutzer nach dem Update zum Beispiel jedes Mal gefragt werden, ob sie die Zwischenablage oder Drucker freigeben möchten.

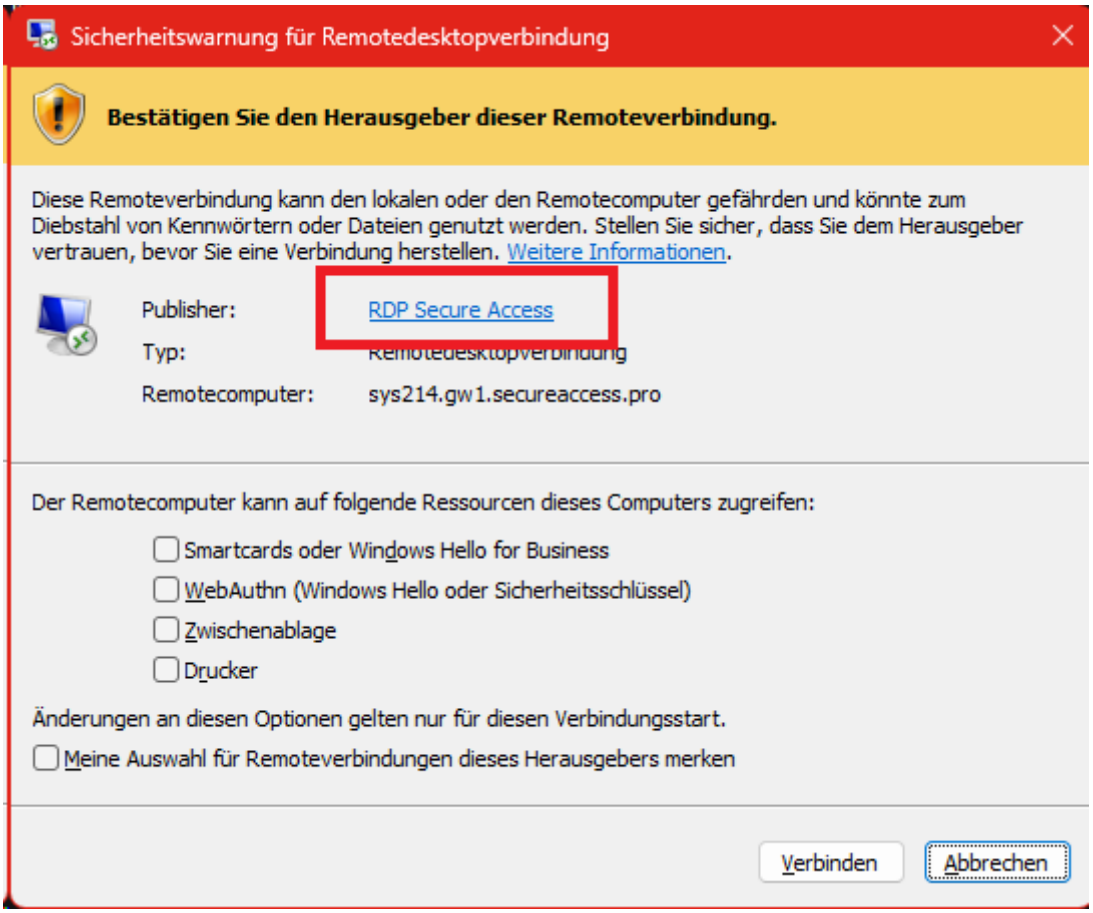
Screenshot - Einmalige Sicherheitswarnung bei der 1. RDP-Verbindung



Screenshot - Sicherheitswarnung vor jeder RDP-Verbindung - Kein Zertifikat - Kein Reg-Schlüssel



Screenshot - Sicherheitswarnung vor jeder RDP-Verbindung - Mit Zertifikat - Kein Reg-Schlüssel



Warum hat Microsoft das geändert?

Eine `.rdp`-Datei ist nicht nur eine einfache Verknüpfung. Sie kann festlegen:

```
zu welchem Server verbunden wird
welche Anzeigeeinstellungen verwendet werden
welche lokalen Geräte weitergeleitet werden
ob Drucker, Zwischenablage oder Laufwerke verfügbar sind
welche Gateway- und Authentifizierungseinstellungen genutzt werden
```

Angreifer können manipulierte RDP-Dateien per E-Mail oder Download verteilen. Öffnet ein Benutzer eine solche Datei, kann sein PC mit einem fremden System verbunden werden und dabei lokale Ressourcen freigeben. Genau dieses Risiko möchte Microsoft reduzieren.

Unterschied zwischen RDP-Serverzertifikat und RDP-Dateisignatur

Wichtig ist die Unterscheidung zwischen zwei verschiedenen Zertifikatsthemen.

RDP-Serverzertifikat

Das RDP-Serverzertifikat betrifft die Identität des entfernten Computers.

Wenn der Ziel-PC kein vertrauenswürdiges Zertifikat hat, erscheint eine Meldung ähnlich:

```
Die Identität des Remotecomputers kann nicht überprüft werden.
```

Dieses Zertifikat liegt auf dem Zielsystem, also auf dem RDP-PC oder RDP-Server.

RDP-Dateisignatur

Die RDP-Dateisignatur betrifft die Herkunft und Unveränderheit der `.rdp`-Datei.

Wenn eine `.rdp`-Datei nicht signiert ist oder der Herausgeber nicht verifiziert werden kann, zeigt Windows sinngemäß:

```
Unbekannter Herausgeber
Unbekannte Remoteverbindung
```

Ein korrektes RDP-Serverzertifikat entfernt daher nicht automatisch den neuen `.rdp`-Dateidialog. Beide Themen sind getrennt.

Wann wird der Herausgeber angezeigt?

Wenn eine `.rdp`-Datei digital signiert ist und Windows die Zertifikatskette prüfen kann, kann Windows den Herausgeber anzeigen.

Beispiel:

```
Herausgeber: RDP Secure Access
```

Wenn die Datei nicht signiert ist oder die Zertifikatskette nicht vertraut wird, erscheint stattdessen:

```
Unbekannter Herausgeber
```

Damit Windows eine intern signierte `.rdp`-Datei als vertrauenswürdig akzeptiert, müssen auf dem Client passende Vertrauenseinstellungen vorhanden sein.

Typischer Aufbau:

```
Root-CA-Zertifikat im lokalen Zertifikatsspeicher
RDP-Signer-Zertifikat bzw. dessen Zertifikatskette vertrauenswürdig
SHA1-Thumbprint des Signer-Zertifikats in der RDP-Trusted-Publisher-Policy
```

Die relevante Richtlinie heißt:

```
Specify SHA1 thumbprints of certificates representing trusted .rdp publishers
```

Welche Registry-/Policy-Einstellung ist relevant?

Für vertrauenswürdige `.rdp`-Publisher wird der SHA1-Thumbprint des Signaturzertifikats hinterlegt.

Registry-Pfad:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services]
"AllowSignedFiles"=dword:00000001
"TrustedCertThumbprints"="SHA1_THUMBPRINT_DES_RDP_SIGNER_ZERTIFIKATS"
```

Wichtig: Hier gehört der SHA1-Thumbprint des **Signer-Zertifikats** hinein, nicht der Thumbprint der Root-CA.

Temporärer Kompatibilitäts-Workaround

Es gibt eine Policy/Registry-Einstellung, mit der das alte Dialogverhalten vorübergehend wiederhergestellt werden kann:

```
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Terminal Services\Client]
"RedirectionWarningDialogVersion"=dword:00000001
```

Per PowerShell als Administrator:

```
New-Item -Path "HKLM:\Software\Policies\Microsoft\Windows NT\Terminal Services\Client" -Force
| Out-Null; New-ItemProperty -Path "HKLM:\Software\Policies\Microsoft\Windows NT\Terminal
Services\Client" -Name "RedirectionWarningDialogVersion" -PropertyType DWord -Value 1 -Force |
```

```
Out-Null
```

Diese Lösung ist als Übergangslösung zu verstehen. Microsoft hat die neue Warnlogik aus Sicherheitsgründen eingeführt; daher sollte man nicht davon ausgehen, dass dieser Workaround dauerhaft unverändert bestehen bleibt.

Empfohlene Zielkonfiguration

Für verwaltete RDP-Dateien empfiehlt sich folgender Ablauf:

```
1. RDP-Datei vollständig erzeugen
2. RDP-Datei serverseitig signieren
3. Signierte RDP-Datei an den Benutzer ausliefern
4. Auf dem Client Root-CA bzw. Zertifikatsvertrauen einrichten
5. Auf dem Client den Signer-Thumbprint als vertrauenswürdigen RDP-Publisher setzen
```

Die `.rdp`-Datei darf nach dem Signieren nicht mehr verändert werden, sonst wird die Signatur ungültig.

Zusammenfassung

Seit dem April-2026-Sicherheitsupdate behandelt Windows `.rdp`-Dateien deutlich restriktiver. Beim Öffnen einer `.rdp`-Datei werden lokale Ressourcen wie Zwischenablage, Drucker oder Laufwerke nicht mehr automatisch anhand der Datei freigegeben, sondern müssen vom Benutzer aktiv bestätigt werden. Die Änderung dient dem Schutz vor RDP-Phishing und betrifft insbesondere Umgebungen, in denen `.rdp`-Dateien dynamisch erzeugt und heruntergeladen werden.

Für eine saubere Lösung müssen `.rdp`-Dateien signiert und die entsprechenden Herausgeberzertifikate bzw. Policies auf den Windows-Clients eingerichtet werden. Alternativ kann kurzfristig der Registry-Workaround `RedirectionWarningDialogVersion=1` verwendet werden.

Quellen:

- https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/remotepc/understanding-security-warnings
- https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/rdpsign
- https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-admx-terminalserver

- https://support.microsoft.com/en-gb/topic/windows-11-version-25h2-update-history-99c7f493-df2a-4832-bd2d-6706baa0dec0
- https://support.microsoft.com/en-gb/topic/april-14-2026-kb5083769-os-builds-26200-8246-and-26100-8246-22f90ae5-9f26-40ac-9134-6a586a71163b
- https://support.microsoft.com/en-us/topic/may-12-2026-kb5089549-os-builds-26200-8457-and-26100-8457-28ec2a99-4bbe-481d-a340-5c6cf18d9acb
- https://support.microsoft.com/de-de/topic/21-m%C3%A4rz-2026-kb5085516-betriebssystembuilds-26200-8039-und-26100-8039-out-of-band-09e85404-1cb6-4ed4-9ca5-3e40d74307b9
- https://github.com/nfedera/rdpsign
- https://gpsearch.azurewebsites.net/default.aspx?lang=en-US&policyid=2540
- https://gpedit.tplant.com.au/en-us/policy/TerminalServer/TS_CLIENT_TRUSTED_CERTIFICATE_THUMBPRINTS_2/

Revision #16
Created 17 May 2026 08:45:30 by Stefan Kittel
Updated 17 May 2026 09:28:19 by Stefan Kittel