RDP & IIS Hardening auf TLS1.2

RDP Versionen:

Windows 7 und Server 2008 R2 (RDP 7.1)
Windows 8 und Server 2012 (RDP8.0)
Windows 8.1 und Server 2012 R2 (RDP8.1)

TLS 1.1+1.2 Unterstützung für Windows 7 und Server 2008 R2 aktivieren:

https://support.microsoft.com/de-de/kb/3080079

Direkt Download x64

http://www.microsoft.com/downloads/details.aspx?FamilyId=f89cecf4-8fb1-41b7-9f3c-163c844438f6

http://www.microsoft.com/downloads/details.aspx?FamilyId=1d870098-5bca-4cad-a339-b370214f53bc

Die höherwertigen Betriebssysteme wie Windows 8/8.1 Server 2012/R2, Windows 10 und Server 2016 benötigen kein Update. Diese unterstützen bereits TLS 1.2.

Wissen:

Unter Windows werden die SSL/TLS Verbindungen durch die SChannel.dll behandelt. Unter Linux würde das z.B. durch OpenSSL geschehen.

Eine Chiffre-Suite ist eine Reihe von Verschlüsselungsalgorithmen.

Hinter Key-Exchange steckt ein asymmetrischer Algorithmus. Ein gemeinsam genutzter Schlüssel (Public-Key). Wird für kleine Datenmengen eingesetzt.
Die Bulk-Encryption setzt auf einen symmetrischen Schlüssel und bringt auch bei großen Datenmenge eine tolle Leistung.
Message Authentication bedeutet die Erstellung von Hashes und Signaturen, die die Identität und Integrität von Nachrichten gewährleistet.

Das Betriebssystem wird durch einen sogenannten algorithm identifier (ALG_ID) informiert welcher Algorithmus zum Einsatz kommt.

Auf dieser Microsoft-Webseite finden wir einen Überblick an Cipher Suiten die die SChannel.dll behandelt.

Welches OS unterstützt welche Protokolle?

- Windows Server 2008 nur: SSL 2.0, SSL 3.0 und TLS 1.0.
- Ab Windows Server 2008 R2 und Windows 7 SP1 wird: SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 und TLS 1.2 unterstützt.

Informationen zur SSL/TLS History:

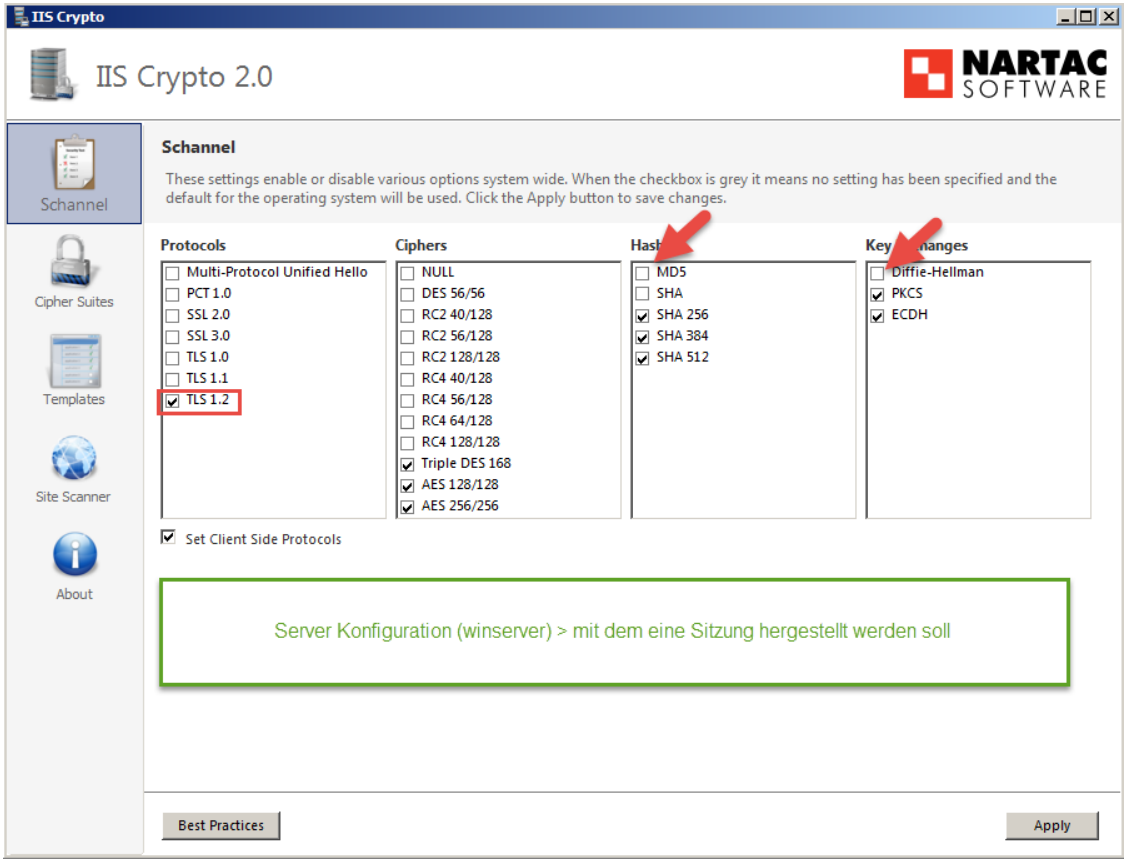
https://en.wikipedia.org/wiki/Template:TLS/SSL_support_history_of_web_browsers

Erstellt von Jörn Walter www.der-windows-papst.de – 09.10.2016

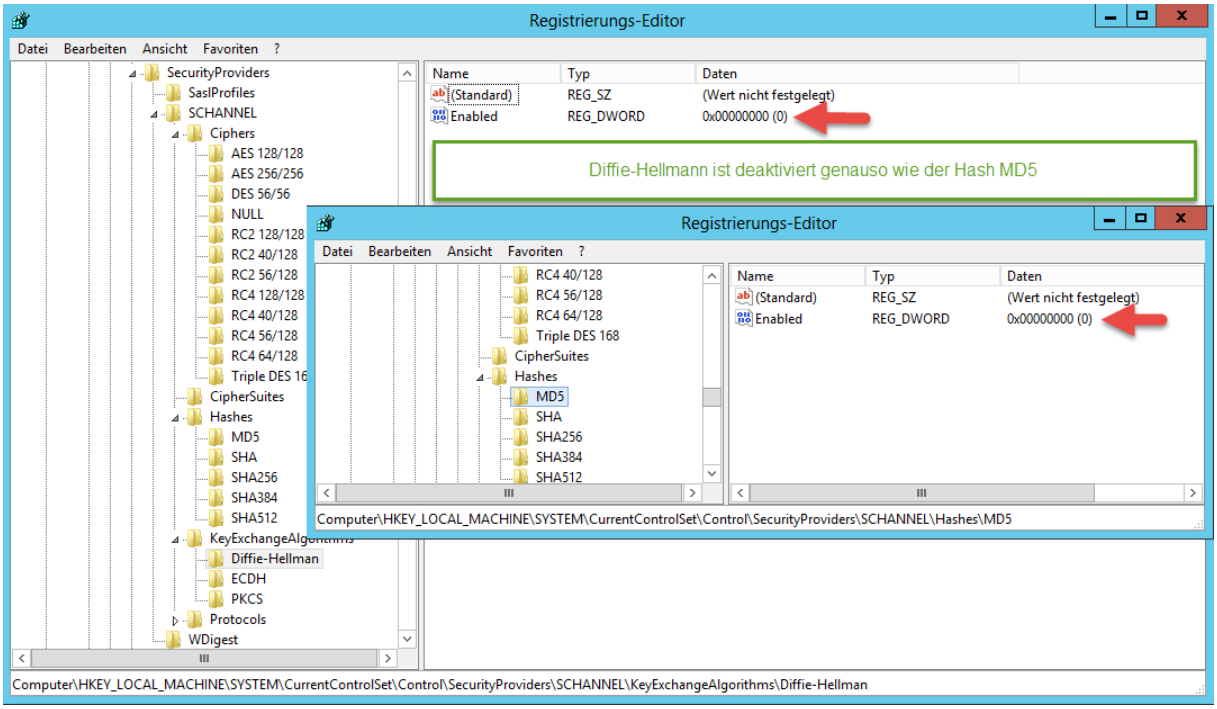
RDP & IIS Hardening auf TLS1.2

Kommen wir nun zur Praxis. An diesem Beispiel zeige ich die notwendigen Einstellungen um eine Remote Desktop Verbindung mit TLS 1.2 aufzubauen.
Achtung: Diese Einstellungen haben auch direkten Einfluss auf den IIS.

Die nötige serverseitige Einstellung:

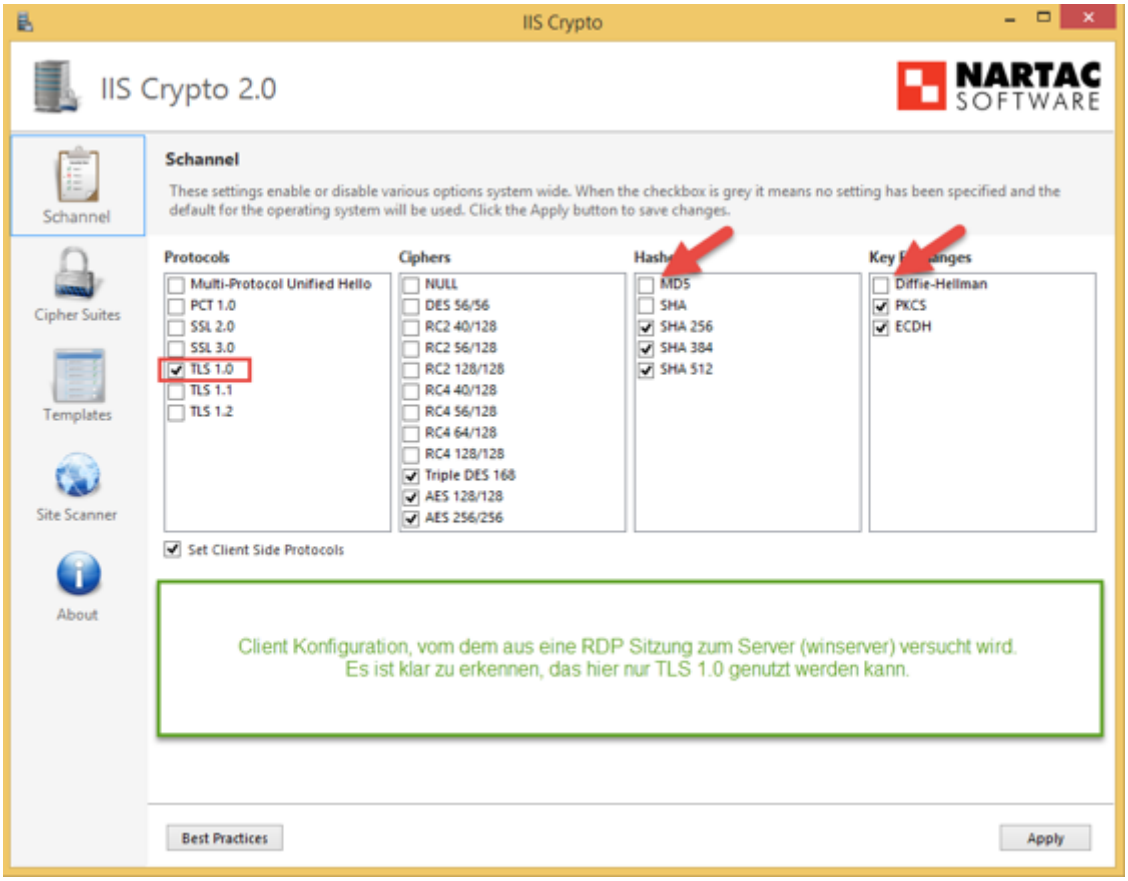


Hier sehen wir die deaktivierten Registry Einträge (roter Pfeil):

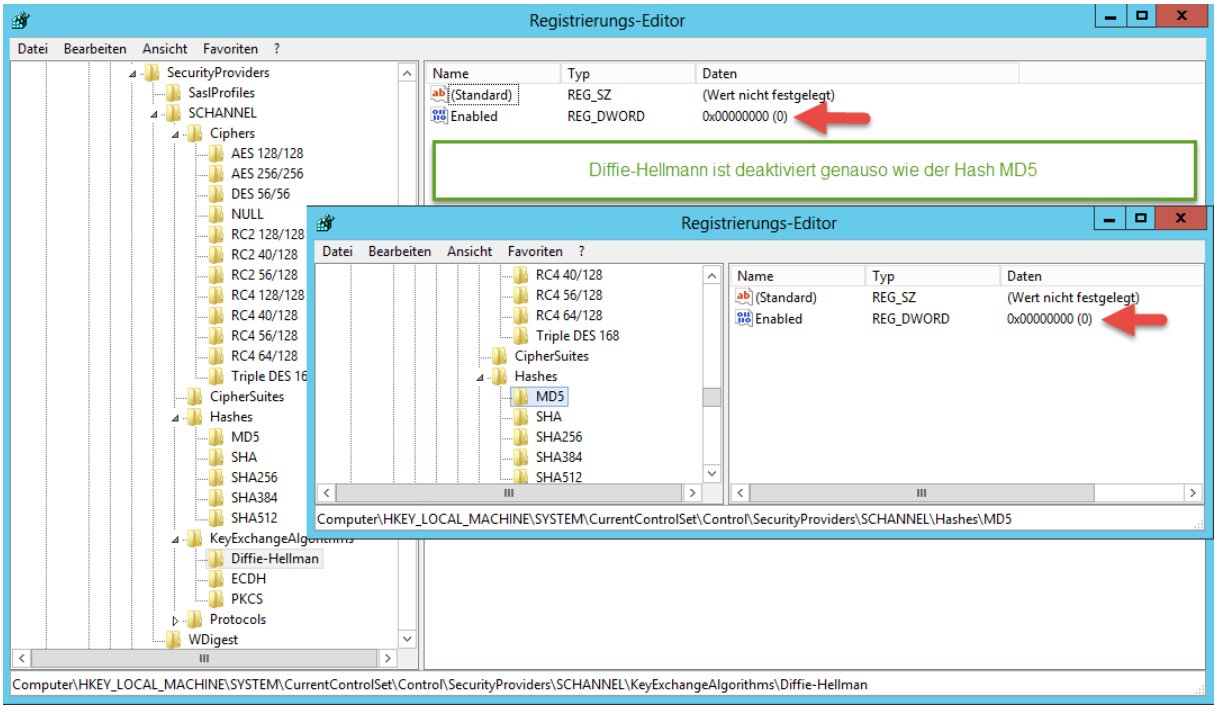


RDP & IIS Hardening auf TLS1.2

Clientseitig setzen wir die Einstellungen bewusst auf TLS 1.0. Denn dieser Versuch soll scheitern, um gleich zu erkennen, wo die Probleme liegen.

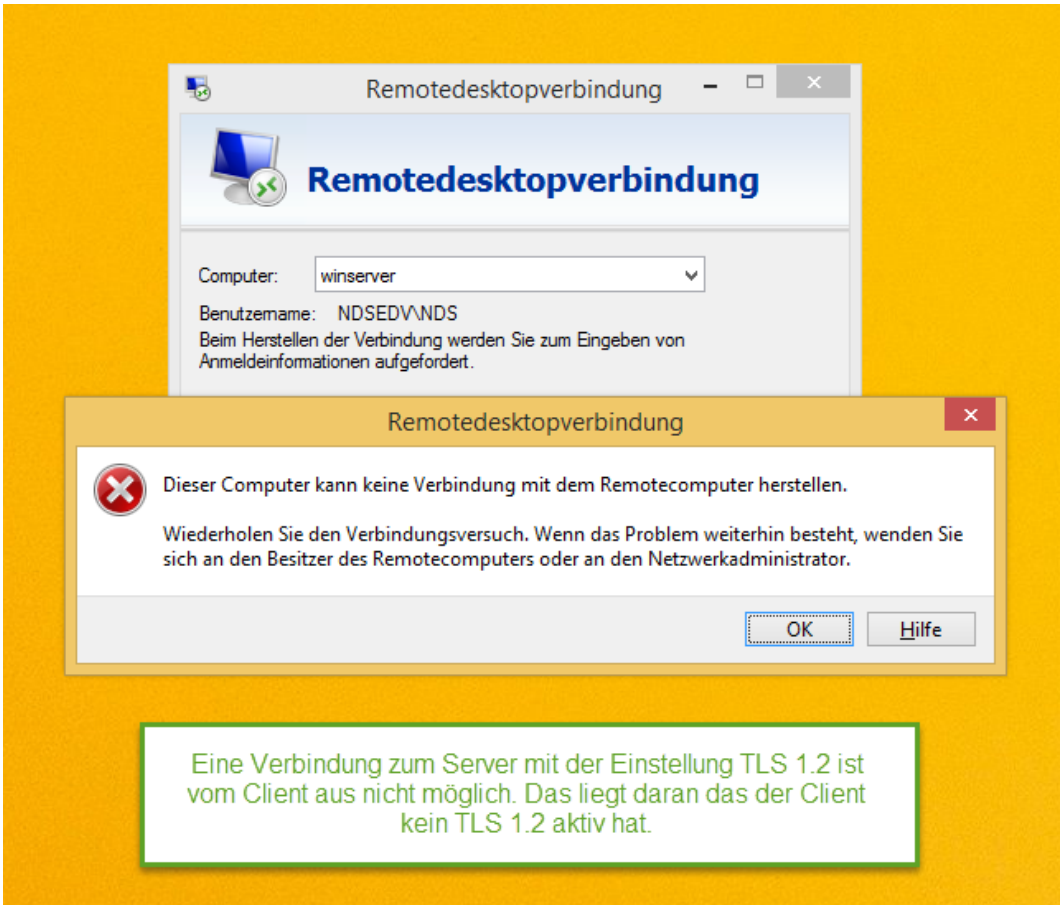


Hier sehen wir die deaktivierten Registry Einträge genau wie beim Server (winserver):



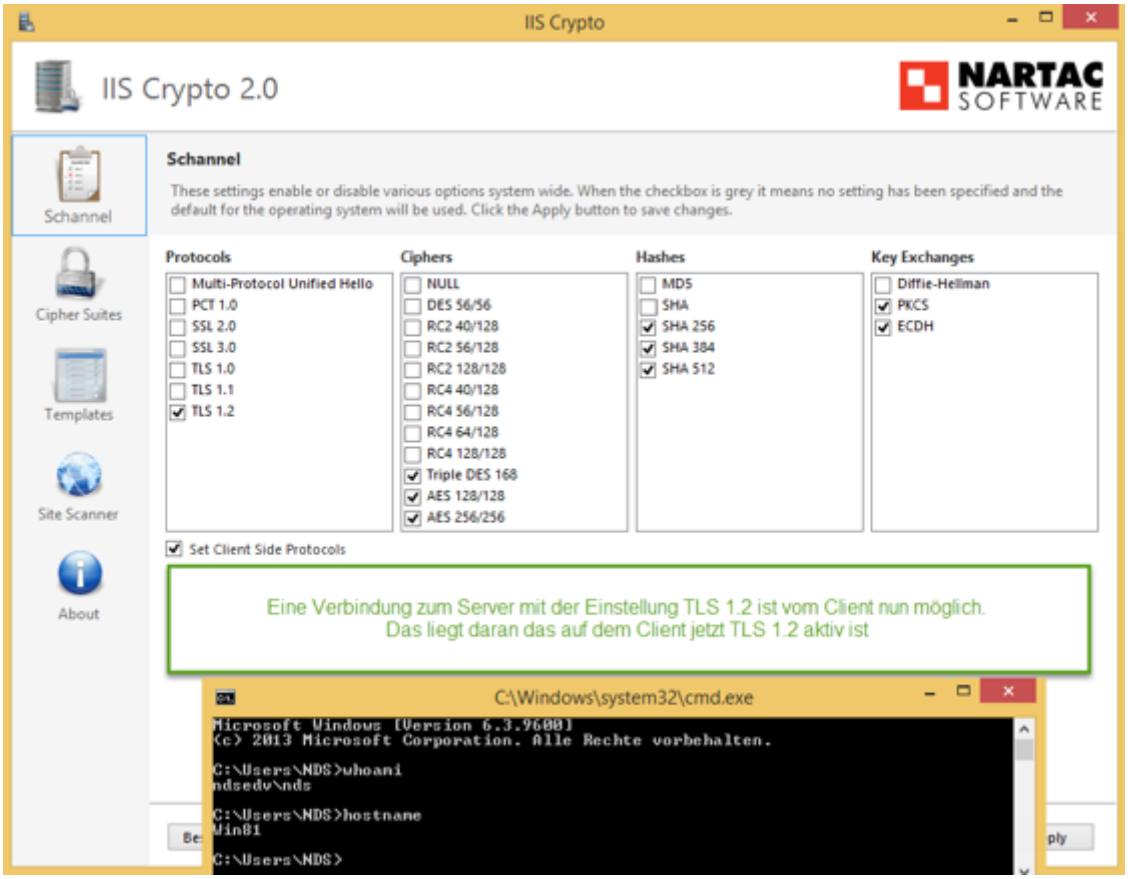
RDP & IIS Hardening auf TLS1.2

Ein RDP Verbindung zum Server (winserver) vom Client (Win81) ist so nicht möglich das liegt daran, das auf dem Client kein TLS 1.2 aktiv ist, sondern nur TLS 1.0.



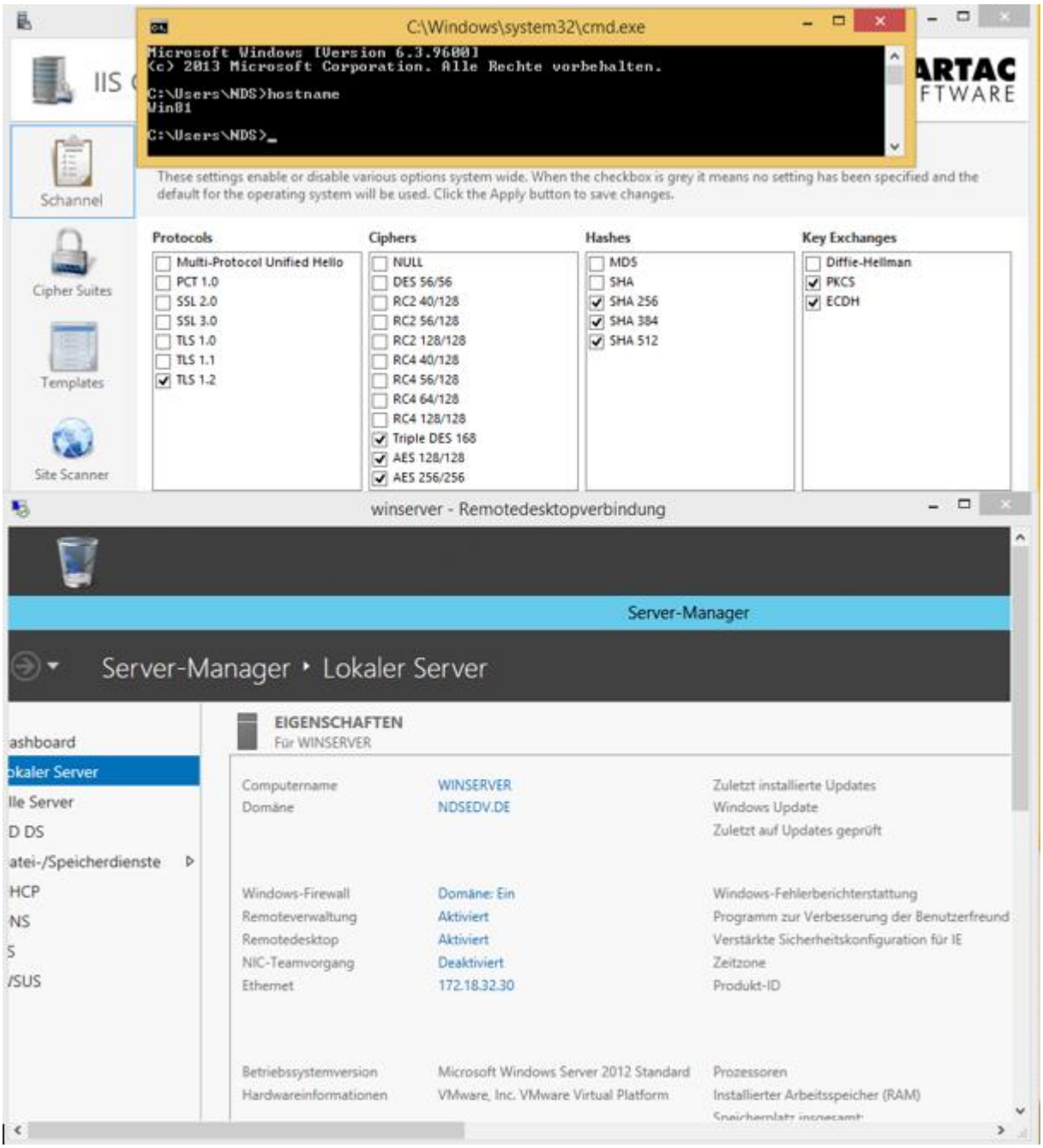
Erstellt von Jörn Walter www.der-windows-papst.de – 09.10.2016

Für den Gegenbeweis schalte ich auf dem Client (Win81) nun TLS 1.2 aktiv und starte einen erneuten Verbindungsversuch.



RDP & IIS Hardening auf TLS1.2

Eine RDP Verbindung vom Client (Win81) zum Server (winserver) ist nun möglich:

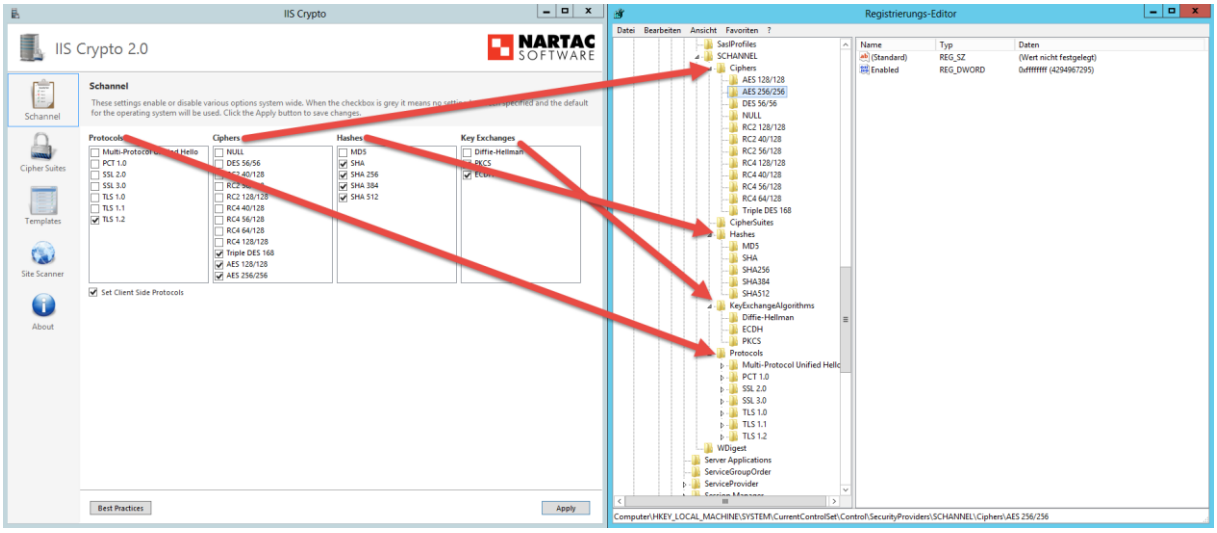


Hinweis:

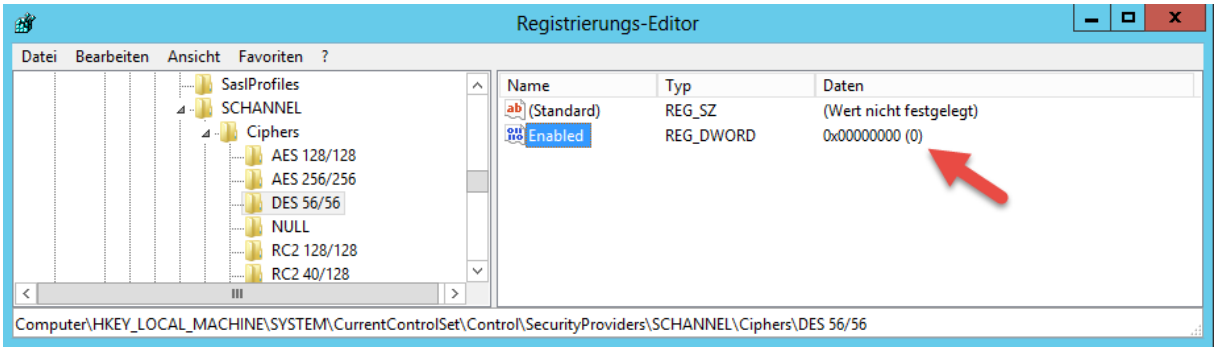
Die Einstellungen im Internet Explorer haben keinen Einfluss auf RDP Sitzungen nur in Zusammenhang mit dem IIS!

RDP & IIS Hardening auf TLS1.2

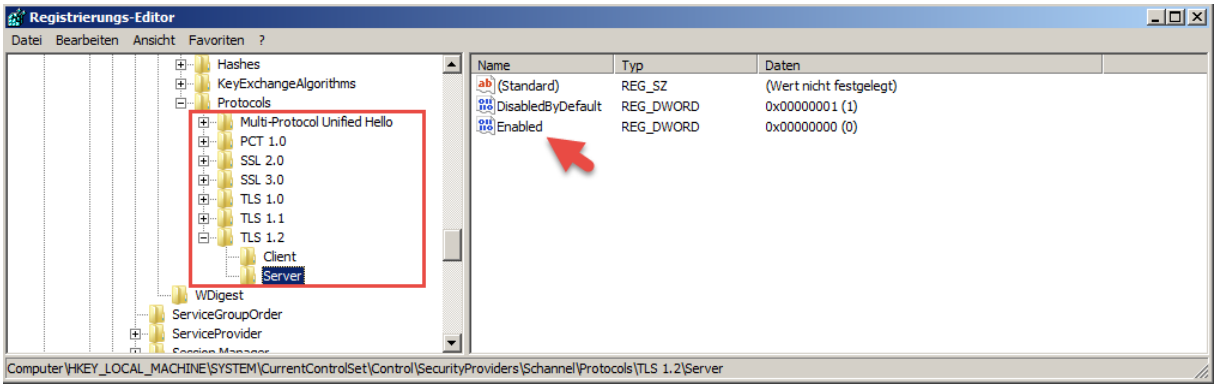
Die gesetzten Einstellungen Protocols, Ciphers, Hashes und Key Exchanges finden wir in der Registry an dieser Stelle:



Der Eintrag AES256/256 wird durch den HEX Wert 0xffffffff oder Dezimal Wert 4294967295 auf Enabled gesetzt. Stünde hier der Wert 0 wäre der Eintrag deaktiviert, wie z.B. bei DES 56/56.

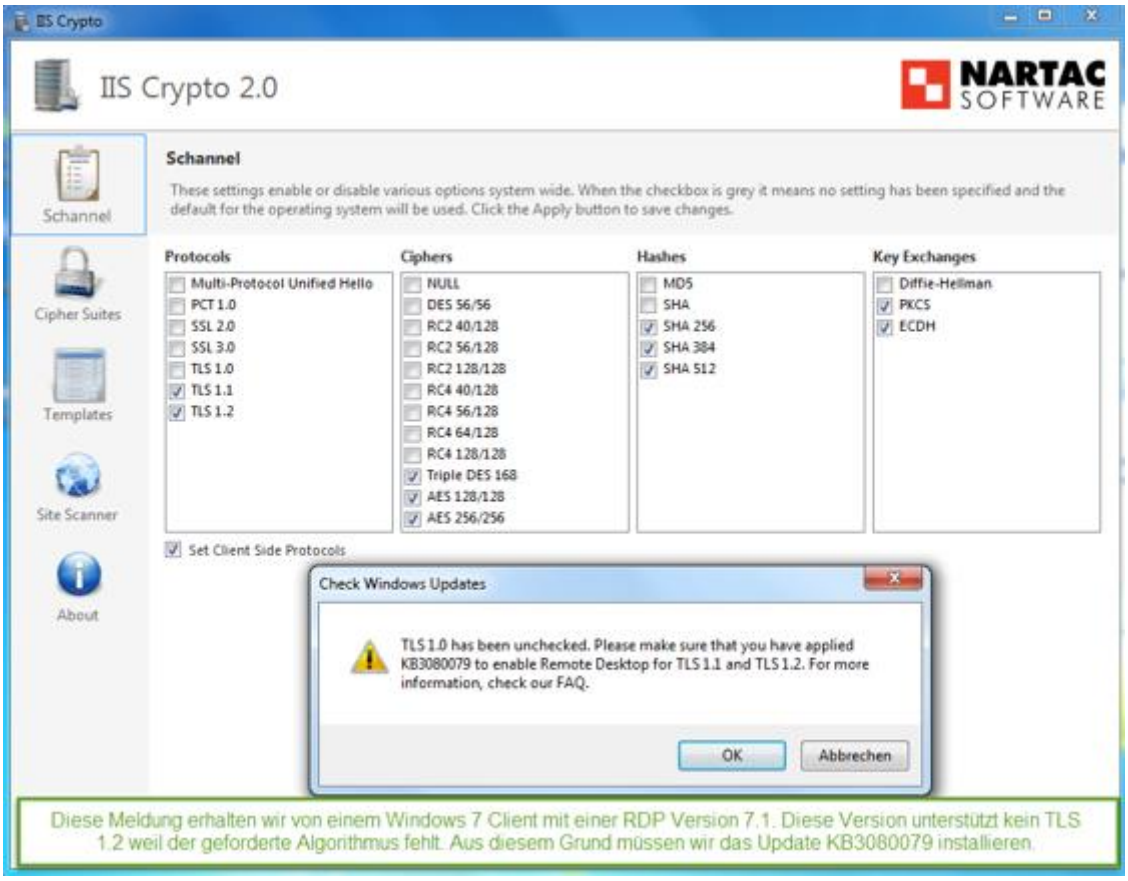


In den Grundeinstellungen verwendet der Internet Information Server (IIS) und RDP, je nach zugrundeliegendem Betriebssystem, noch das SSL Verfahren. Deshalb muss TLS 1.2 oder TLS 1.1 aktiviert und die SSL-Default-Einstellungen deaktiviert werden. Diese Einstellungen wirken ab Server 2008 R2 und Windows 7 SP1.

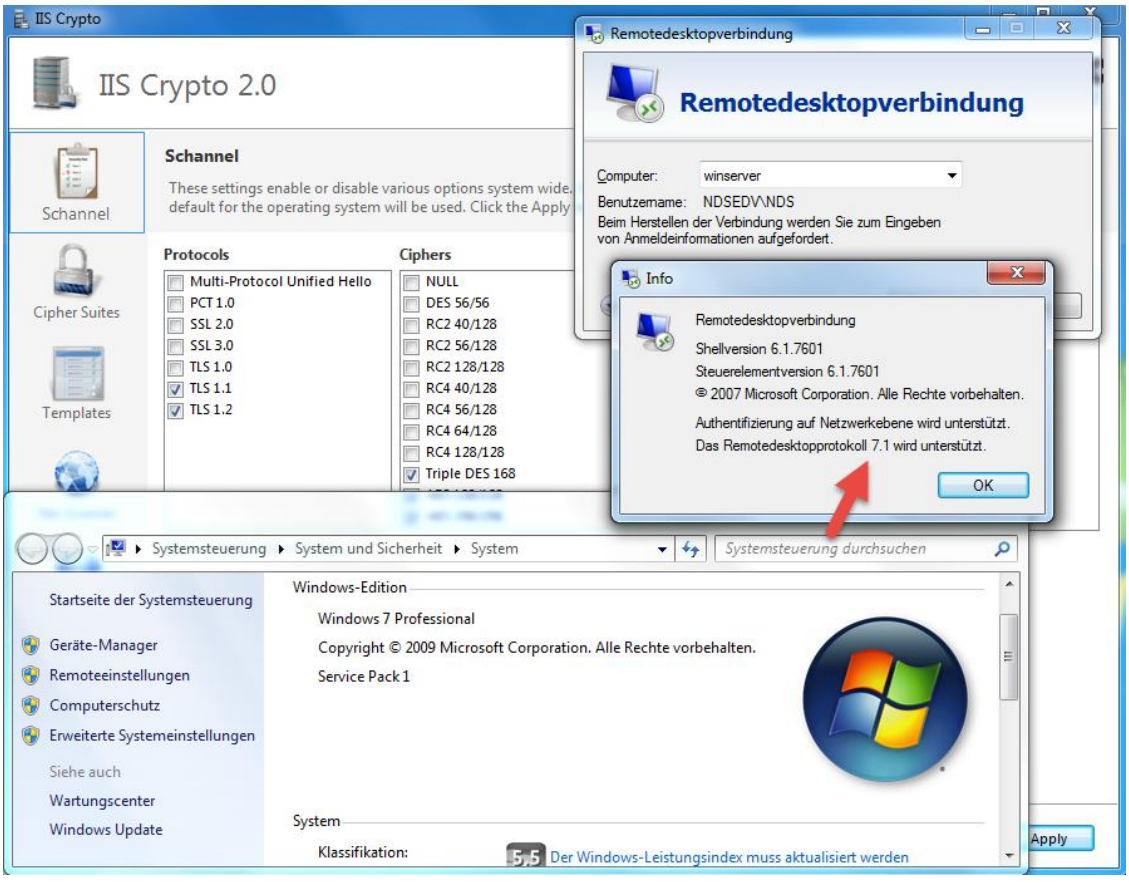


Achtung: Sobald diese Schlüssel unterhalb von Protocols vorhanden sind; DisableByDefault den Wert = 0 hat, sind nur noch diese Einstellungen (Protokolle) gültig.

Warum habe ich am Anfang der Anleitung die Downloads erwähnt? Hier die Antwort.

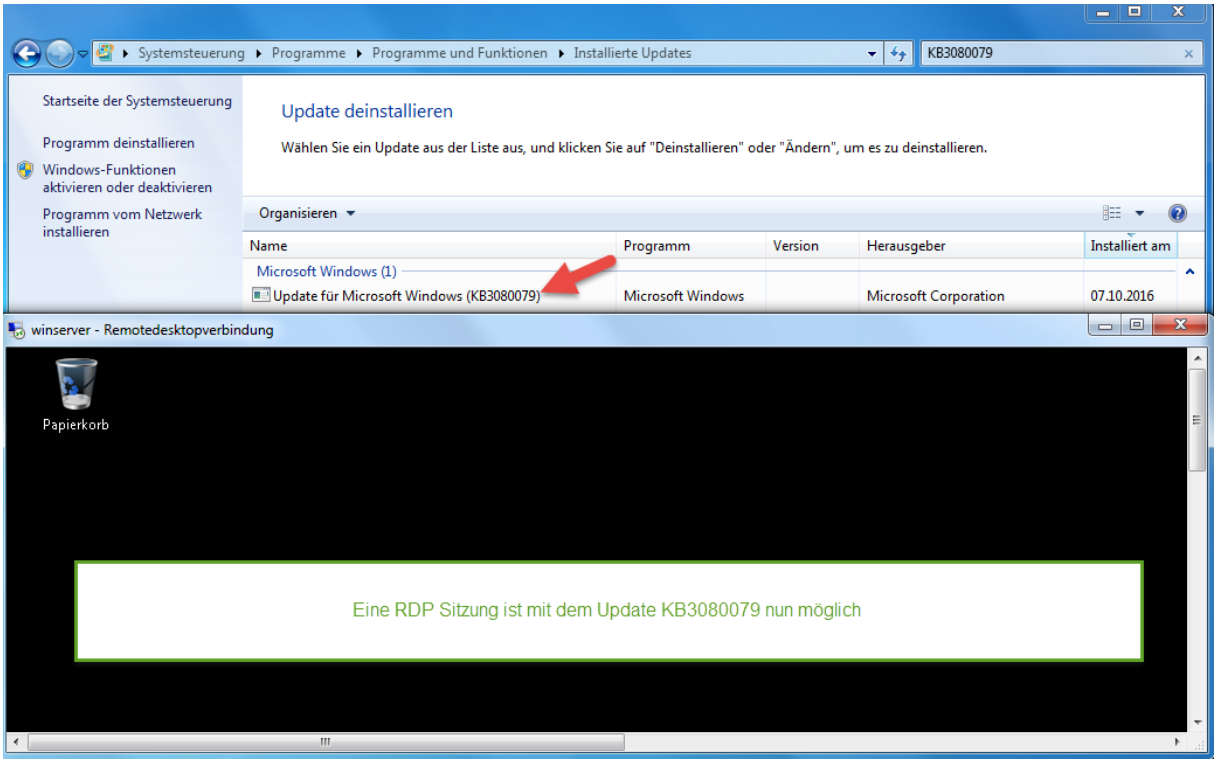


RDP Versionsinformation eines Windows 7 Client:



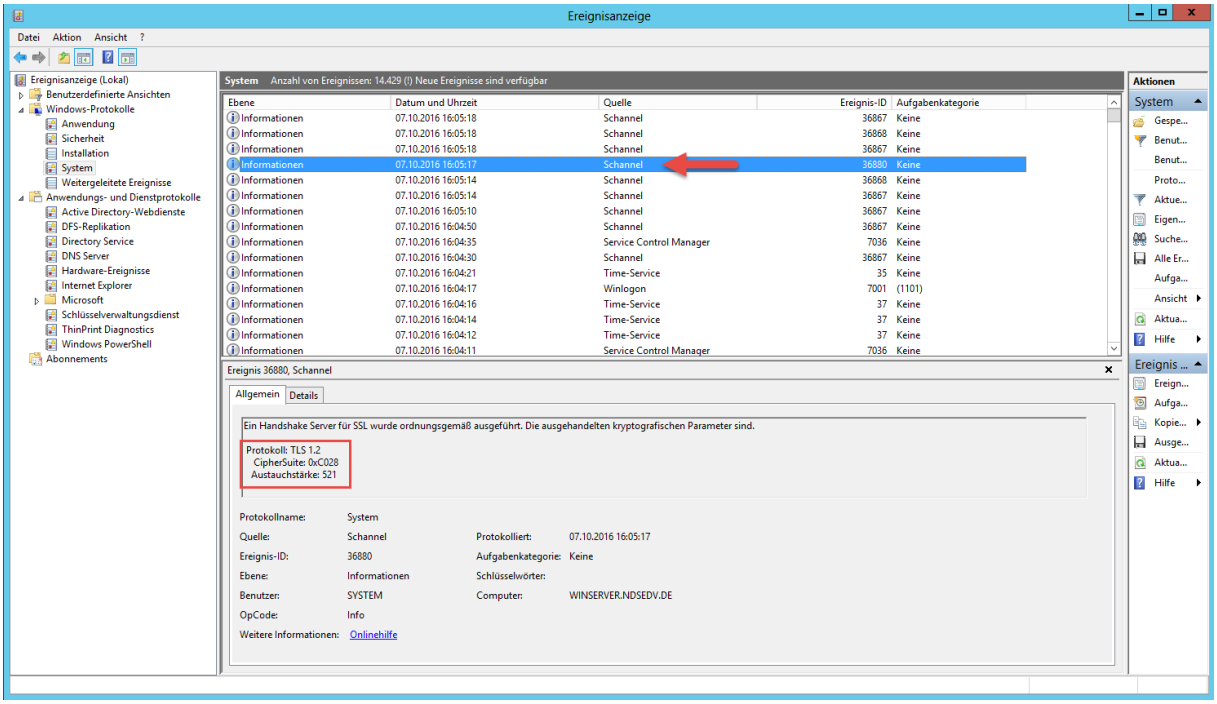
RDP & IIS Hardening auf TLS1.2

Nach der Installation des Updates können wir mit der RDP Version 7.1 eine Remote Sitzung über TLS 1.2 zum Server (winserver) aufbauen.



Das Schannel Logging lässt sich in der Registry wie folgt erhöhen. Auf diese Weise ist zu erkennen welche Verschlüsselung nun tatsächlich zum Einsatz kam.

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL]
"EventLogging"=dword:00000004
```



RDP & IIS Hardening auf TLS1.2

Verfügbare Werte fürs Logging:

Der Wert = 0 steht für Do not Log, der Wert 1 steht für Error Logging, der Wert 2 für Log Warnings und der Wert 4 steht für Log Informational and success events.

Der TLS 1.2 REG-KEY für Client und Server ab Windows 7 und Server 2008 R2:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL]

"EventLogging"=dword:00000004

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 128/128]

"Enabled"=dword:ffffffff

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 256/256]

"Enabled"=dword:ffffffff

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 128/128]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128]

"Enabled"=dword:00000000
```

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\CipherSuites]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\MD5]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA]

"Enabled"=dword: 00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA256]

"Enabled"=dword:ffffffff

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA384]

"Enabled"=dword:ffffffff

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA512]

"Enabled"=dword:ffffffff

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\ECDH]

"Enabled"=dword:ffffffff

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\PKCS]

"Enabled"=dword:ffffffff

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Multi-Protocol Unified Hello]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Multi-Protocol Unified Hello\Client]

"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Multi-Protocol Unified Hello\Server]

"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0\Client]

"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0\Server]

"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client]

"DisabledByDefault"=dword:00000001
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server]

"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client]

"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server]

"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

RDP & IIS Hardening auf TLS1.2

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client]

"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server]

"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client]

"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server]

"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]

"Enabled"=dword:ffffffff
"DisabledByDefault"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]

"Enabled"=dword:ffffffff
"DisabledByDefault"=dword:00000000

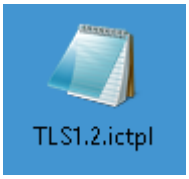
RDP & IIS Hardening auf TLS1.2

Zur Verbreitung des REG-KEYS kann auch die Commandline des Nartac Tools und ein Template eingesetzt werden:

Der Befehl dazu lautet:

iiscryptocli /template \\winserver\netlogon\TLS1.2.ictpl oder
\\winserver\netlogon\iiscryptocli.exe \\winserver\netlogon\TLS1.2.ictpl

Hier der gleichwertige Inhalt der TLS1.2.ictpl Datei zum obigen Registry-Key.




```
<?xml version="1.0" encoding="utf-16"?>
<iisCryptoTemplate xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" version="0">
  <header>
    <name>PCI 3.1</name>
    <author>Nartac Software</author>
    <lastUpdated>2016-10-07T18:15:09.1699265Z</lastUpdated>
    <description>This template is used to make your server PCI 3.1 compliant. It will disable TLS 1.0 which will break many client connections to your website. Please make sure that RDP will continue to function as Windows 2008 R2 requires an update. See our FAQ for more information. Note: The PCI council has pushed back the migration date for PCI 3.1 to June 30, 2018.</description>
    <builtIn>false</builtIn>
  </header>
  <schannel setClientProtocols="true">
    <clientProtocols>
      <schannelItem name="Multi-Protocol Unified Hello" state="Disabled" />
      <schannelItem name="PCT 1.0" state="Disabled" />
      <schannelItem name="SSL 2.0" state="Disabled" />
      <schannelItem name="SSL 3.0" state="Disabled" />
      <schannelItem name="TLS 1.0" state="Disabled" />
      <schannelItem name="TLS 1.1" state="Enabled" minimumOSVersion="Windows2008R2" />
      <schannelItem name="TLS 1.2" state="Enabled" minimumOSVersion="Windows2008R2" />
    </clientProtocols>
    <serverProtocols>
      <schannelItem name="Multi-Protocol Unified Hello" state="Disabled" />
```

```
      <schannelItem name="PCT 1.0" state="Disabled" />
      <schannelItem name="SSL 2.0" state="Disabled" />
      <schannelItem name="SSL 3.0" state="Disabled" />
      <schannelItem name="TLS 1.0" state="Disabled" />
      <schannelItem name="TLS 1.1" state="Enabled"
minimumOSVersion="Windows2008R2" />
      <schannelItem name="TLS 1.2" state="Enabled"
minimumOSVersion="Windows2008R2" />
    </serverProtocols>
    <ciphers>
      <schannelItem name="NULL" state="Disabled" />
      <schannelItem name="DES 56/56" state="Disabled" />
      <schannelItem name="RC2 40/128" state="Disabled" />
      <schannelItem name="RC2 56/128" state="Disabled" />
      <schannelItem name="RC2 128/128" state="Disabled" />
      <schannelItem name="RC4 40/128" state="Disabled" />
      <schannelItem name="RC4 56/128" state="Disabled" />
      <schannelItem name="RC4 64/128" state="Disabled" />
      <schannelItem name="RC4 128/128" state="Disabled" />
      <schannelItem name="Triple DES 168" state="Enabled" />
      <schannelItem name="AES 128/128" state="Enabled" />
      <schannelItem name="AES 256/256" state="Enabled" />
    </ciphers>
    <hashes>
      <schannelItem name="MD5" state="Disabled" />
      <schannelItem name="SHA" state=" Disabled" />
      <schannelItem name="SHA 256" state="Enabled"
minimumOSVersion="Windows2008R2" />
      <schannelItem name="SHA 384" state="Enabled"
minimumOSVersion="Windows2008R2" />
      <schannelItem name="SHA 512" state="Enabled"
minimumOSVersion="Windows2008R2" />
    </hashes>
    <keyExchanges>
      <schannelItem name="Diffie-Hellman" state="Disabled" />
      <schannelItem name="PKCS" state="Enabled" />
```

```
      <schannelItem name="ECDH" state="Enabled" />

    </keyExchanges>

  </schannel>

  <cipherSuites>

    <cipherSuiteItem name="TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P521"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P521"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P521"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P521"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P521"
state="Enabled" maximumOSVersion="Windows2012R2" />
```

```
    <cipherSuiteItem name="TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P521"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P521"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P521"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256"
state="Enabled" maximumOSVersion="Windows2012R2" />

    <cipherSuiteItem name="TLS_RSA_WITH_AES_256_GCM_SHA384" state="Enabled"
/>

    <cipherSuiteItem name="TLS_RSA_WITH_AES_128_GCM_SHA256" state="Enabled"
/>

    <cipherSuiteItem name="TLS_RSA_WITH_AES_256_CBC_SHA256" state="Enabled"
/>

    <cipherSuiteItem name="TLS_RSA_WITH_AES_128_CBC_SHA256" state="Enabled"
/>

    <cipherSuiteItem name="TLS_RSA_WITH_AES_256_CBC_SHA" state="Enabled" />

    <cipherSuiteItem name="TLS_RSA_WITH_AES_128_CBC_SHA" state="Enabled" />

    <cipherSuiteItem name="TLS_RSA_WITH_3DES_EDE_CBC_SHA" state="Enabled" />

    <cipherSuiteItem name="TLS_DHE_RSA_WITH_AES_256_GCM_SHA384"
state="Disabled" />

    <cipherSuiteItem name="TLS_DHE_RSA_WITH_AES_128_GCM_SHA256"
state="Disabled" />

    <cipherSuiteItem name="TLS_DHE_DSS_WITH_AES_256_CBC_SHA256"
state="Disabled" />

    <cipherSuiteItem name="TLS_DHE_DSS_WITH_AES_128_CBC_SHA256"
state="Disabled" />

    <cipherSuiteItem name="TLS_DHE_DSS_WITH_AES_256_CBC_SHA"
state="Disabled" />
```

```
    <cipherSuiteItem name="TLS_DHE_DSS_WITH_AES_128_CBC_SHA"
state="Disabled" />

    <cipherSuiteItem name="TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA"
state="Disabled" />

    <cipherSuiteItem name="TLS_RSA_WITH_RC4_128_SHA" state="Disabled" />

    <cipherSuiteItem name="TLS_RSA_WITH_RC4_128_MD5" state="Disabled" />

    <cipherSuiteItem name="TLS_RSA_WITH_NULL_SHA256" state="Disabled" />

    <cipherSuiteItem name="TLS_RSA_WITH_NULL_SHA" state="Disabled" />

    <cipherSuiteItem name="SSL_CK_RC4_128_WITH_MD5" state="Disabled" />

    <cipherSuiteItem name="SSL_CK_DES_192_EDE3_CBC_WITH_MD5"
state="Disabled" />

    <cipherSuiteItem name="TLS_DHE_RSA_WITH_AES_256_CBC_SHA"
state="Disabled" />

    <cipherSuiteItem name="TLS_DHE_RSA_WITH_AES_128_CBC_SHA"
state="Disabled" />

  </cipherSuites>

</iisCryptoTemplate>
```

RDP & IIS Hardening auf TLS1.2

Ermittelte Probleme mit MS SQL bei Aktivierung von ausschließlich TLS 1.2:

Eine ausschließliche TLS 1.2 Einstellung hat zu Folge, dass es unter MS SQL 2012 und 2014 zu Problemen mit gewissen Diensten kommen kann. Darunter fällt z.B. der Reporting-Service SSRS.

Im Event Viewer steht dann der Fehlercode mit der ID 17182 mit dem Hinweis auf TDSSNIClient-Initialisierung fehlgeschlagen mit Fehler 0y80090331: Grund keine SSL Unterstützung etc.

Um das Problem nicht aufkommen zu lassen sollte vorher das Kumulative Update KB3052404 installiert werden.

https://support.microsoft.com/en-us/kb/3052404

Dann gibt es unter dem SQL Server 2014 SP1 und SQL Server 2012 das Problem das der Microsoft SQLServerAgent nicht mehr lief. Dafür muss der SQL Native Client (SNAC) aktualisiert werden. Auch dafür gibt es einen Hotfix.

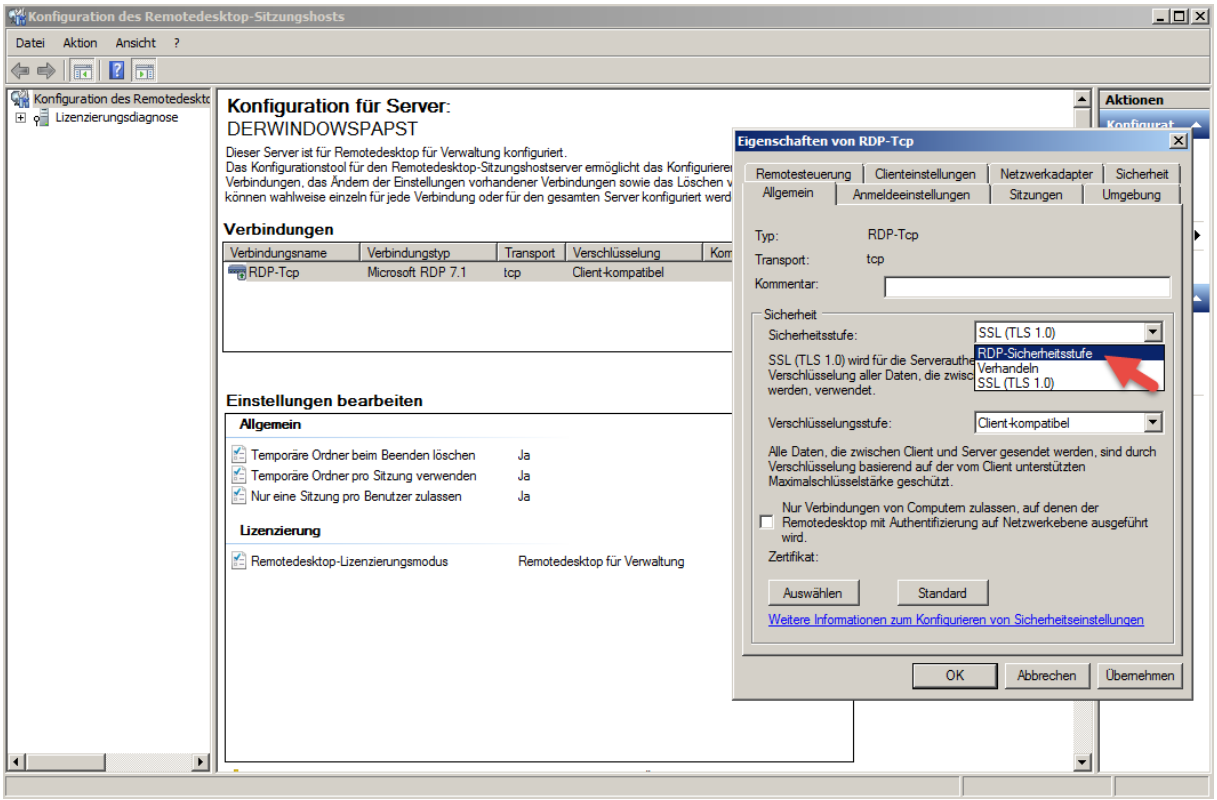
SQL Server 2014 SP1 Native Client:

https://support.microsoft.com/en-us/kb/3106660

SQL Server 2012 Native Client:

https://www.microsoft.com/en-us/download/details.aspx?id=50402

Wenn nach der Deaktivierung von TLS 1.0 unter Server 2008 R2 die Remote Desktop Verbindung nicht mehr funktioniert dann muss noch die Sicherheitsstufe angepasst und auf RDP-Sicherheitsstufe umgestellt werden. Genauso wie bei einer Server 2012 R2 RDS Farm im Connection Broker sofern zuvor TLS 1.0 im Einsatz war.



Es gibt auch Backup Tools die weiterhin TLS 1.0 benötigen aber dafür habe ich jetzt keine Lösung parat außer zu sagen, nehmt Kontakt zum Hersteller auf.

Erstellt von Jörn Walter www.der-windows-papst.de – 09.10.2016

RDP & IIS Hardening auf TLS1.2

Default Cipher Suites:

Server 2008:

```
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P521
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P521
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_RC4_128_MD5
SSL_CK_RC4_128_WITH_MD5
SSL_CK_DES_192_EDE3_CBC_WITH_MD5
TLS_RSA_WITH_NULL_MD5
TLS_RSA_WITH_NULL_SHA
```

Server 2008 R2:

```
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
```

TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_NULL_SHA256
TLS_RSA_WITH_NULL_SHA
SSL_CK_RC4_128_WITH_MD5
SSL_CK_DES_192_EDE3_CBC_WITH_MD5

Server 2012:

TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_RC4_128_MD5
SSL_CK_RC4_128_WITH_MD5
SSL_CK_DES_192_EDE3_CBC_WITH_MD5
TLS_RSA_WITH_NULL_SHA256
TLS_RSA_WITH_NULL_SHA

Server 2012 R2:

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384

TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_NULL_SHA256
TLS_RSA_WITH_NULL_SHA
SSL_CK_RC4_128_WITH_MD5
SSL_CK_DES_192_EDE3_CBC_WITH_MD5

Server 2016:

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_NULL_SHA256
TLS_RSA_WITH_NULL_SHA
SSL_CK_DES_192_EDE3_CBC_WITH_MD5
SSL_CK_RC4_128_WITH_MD5

RDP & IIS Hardening auf TLS1.2

TLS 1.1 und TLS 1.2 Registry-Key Default Einstellungen:

TLS 1.1

This subkey controls the use of TLS 1.1.

Applicable versions: As designated in the **Applies To** list that is at the beginning of this topic excluding those versions prior to Windows Server 2008 R2 and Windows 7.

Registry path: HKLM SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

To disable the TLS 1.1 protocol, create an **Enabled** entry in the appropriate subkey. This entry does not exist in the registry by default. After you have created the entry, change the DWORD value to 0. To enable the protocol, change the DWORD value to 1.

TLS 1.1 subkey table

Subkey	Description	Default
Client	Controls the use of TLS 1.1 on the client.	Enabled
Server	Controls the use of TLS 1.1 on the server.	Enabled
DisabledByDefault	Flag to disable TLS 1.1 by default.	Enabled

TLS 1.2

This subkey controls the use of TLS 1.2.

Note: For TLS 1.2 to be enabled and negotiated on servers that run Windows Server 2008 R2, you MUST create the "DisabledByDefault" entry in the appropriate subkey (Client, Server) and set it to "0". The entry will not be seen in the registry and it is set to "1" by default.

Applicable versions: As designated in the **Applies To** list that is at the beginning of this topic excluding those versions prior to Windows Server 2008 R2 and Windows 7.

Registry path: HKLM SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

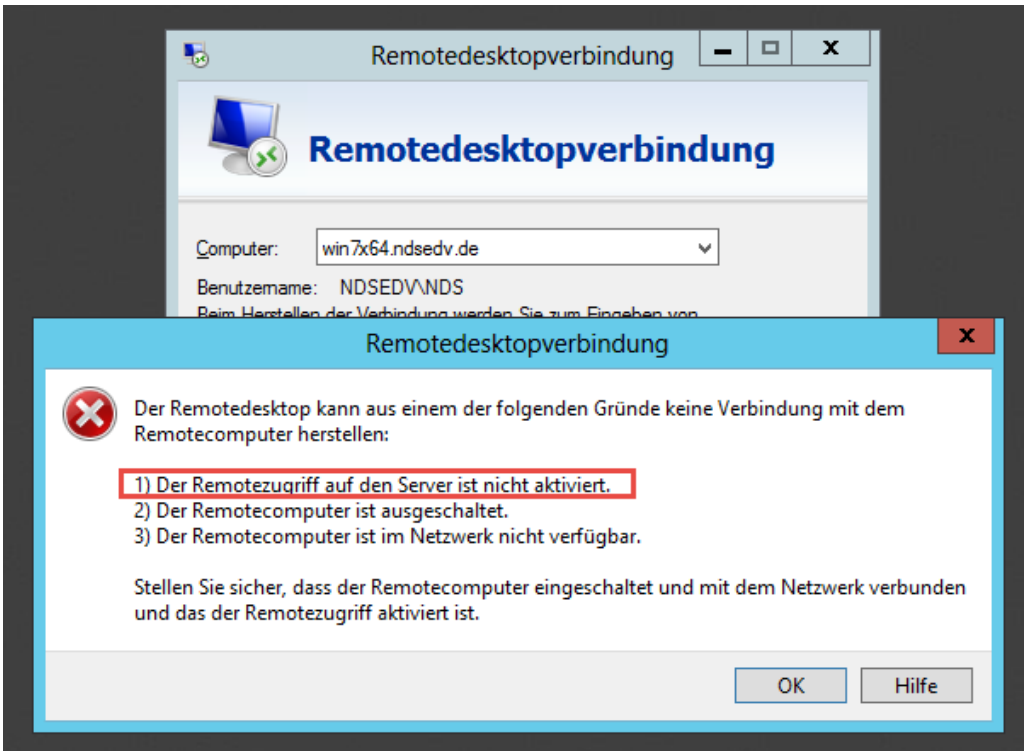
To disable the TLS 1.2 protocol, create an **Enabled** entry in the appropriate subkey. This entry does not exist in the registry by default. After you have created the entry, change the DWORD value to 0. To enable the protocol, change the DWORD value to 1.

TLS 1.2 subkey table

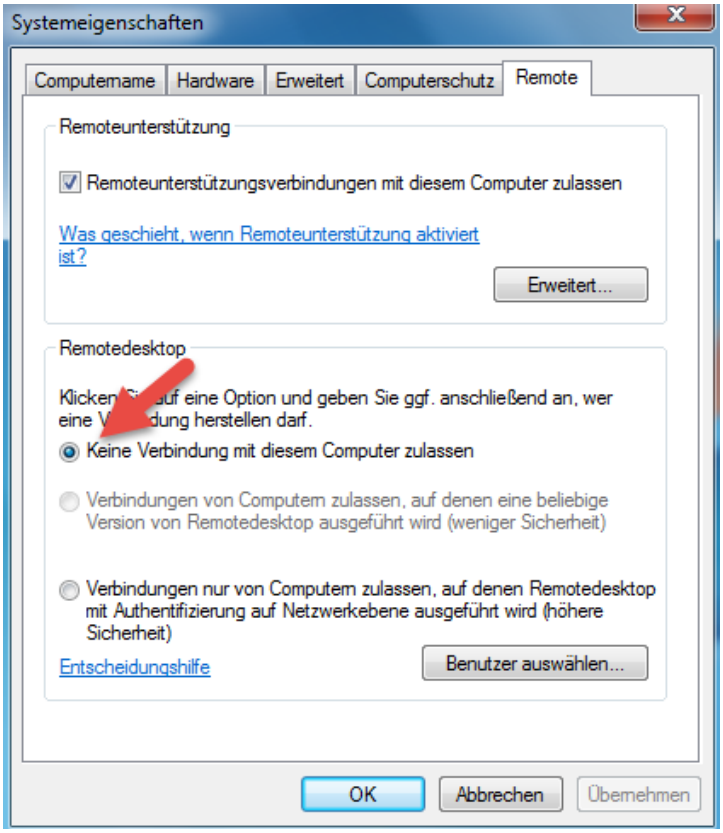
Subkey	Description	Default
Client	Controls the use of TLS 1.2 on the client.	Enabled
Server	Controls the use of TLS 1.2 on the server.	Enabled
DisabledByDefault	Flag to disable TLS 1.2 by default.	Enabled

Troubleshooting:

Kein RDP Verbindung möglich.

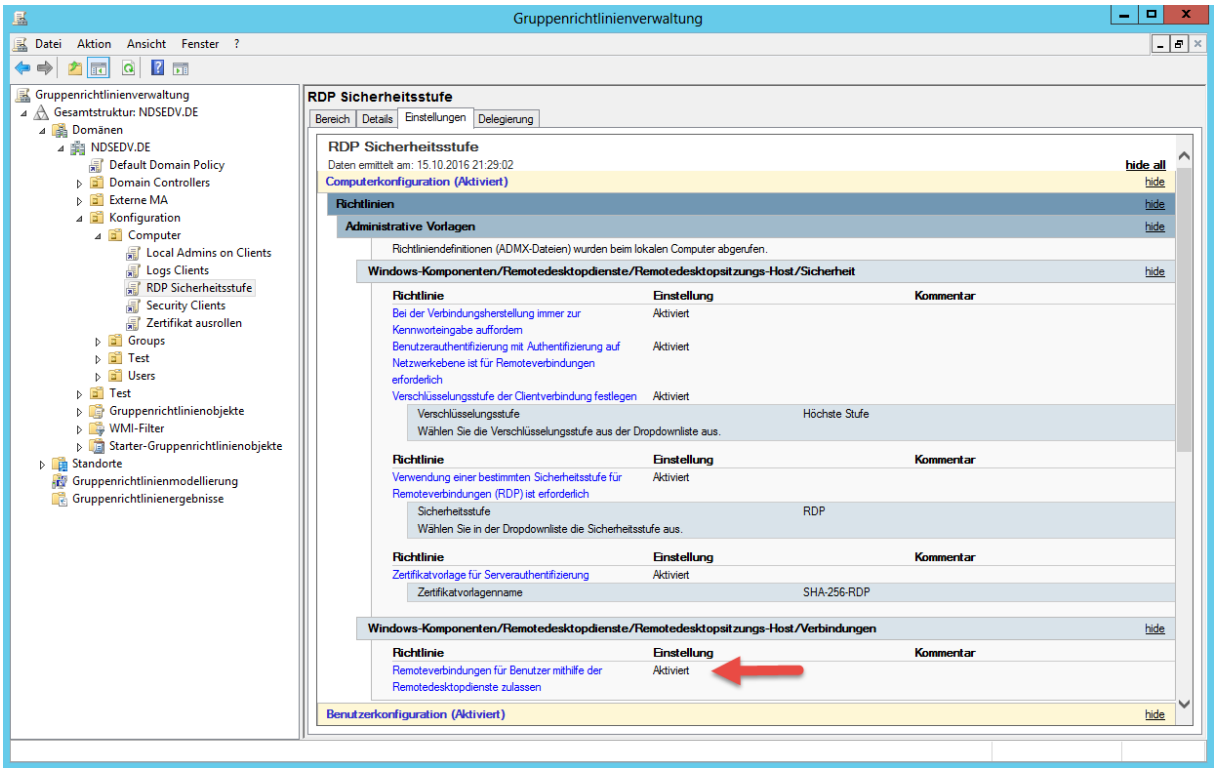


Ursache:

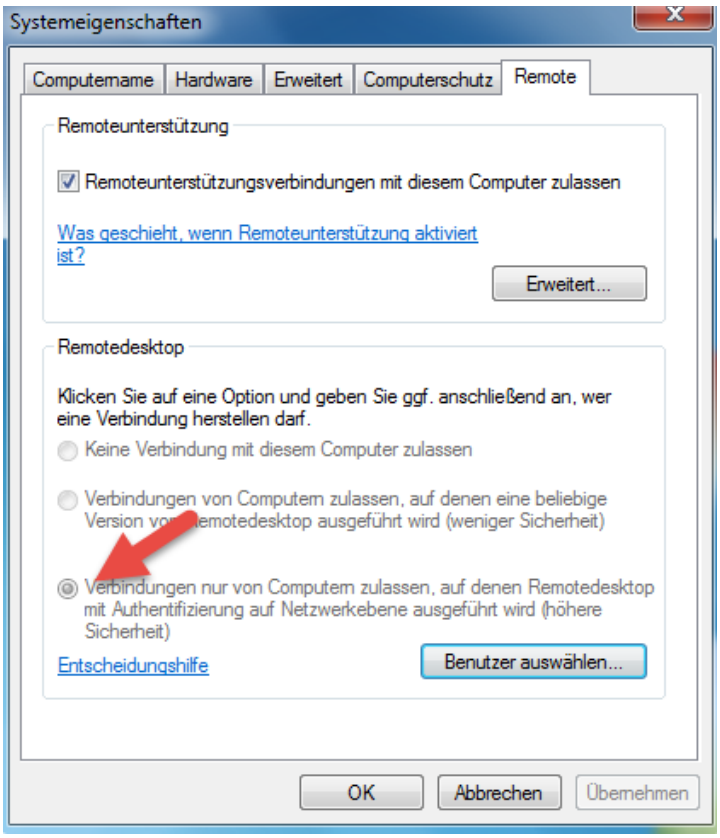


RDP & IIS Hardening auf TLS1.2

Lösung:



Ergebnis:



RDP & IIS Hardening auf TLS1.2

Falls keine Authentifizierung über Netzwerkeben unterstützt wird, ist zu prüfen ob der Schlüssel vorhanden ist.