Radius mit Windows Server

Server, Clients und WLAN richtig konfigurieren

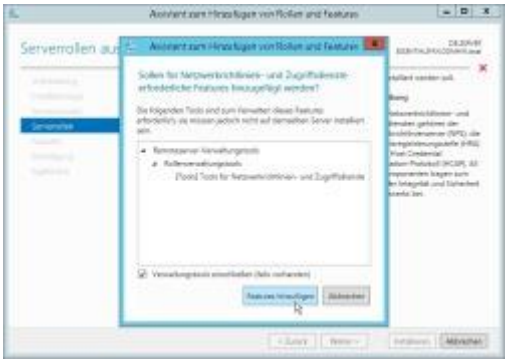
Überall, wo viele wechselnde Nutzer und Geräte Zugang zu einem Funknetzwerk benötigen, stößt WPA2 an seine Grenzen. Kommt der gemeinsame Zugangsschlüssel in die falschen Hände, steht ein Kennwortwechsel für alle an. Damit nicht Alles von einem einzigen Schlüssel abhängt, wird bei WPA2-Enterprise der Zugang für jeden Benutzer zum WLAN über individuelle Zugangsdaten (Credentials) gelöst. Bucht sich ein Benutzer mit einem Mobilgerät im WLAN ein, fragt der Access-Point einen Radius-Server (Remote Dial In User Service), ob der Nutzer überhaupt auf das Netz zugreifen darf. Der Server lässt dann entweder die Verbindung zu oder weist sie ab. Den Radius-Server liefert Microsoft in allen aktuellen Varianten des Windows Server in Form des Netzwerkrichtlinienservers (engl. Network Policy Server) mit.

Für die Inbetriebnahme benötigen Sie neben Server und Clients auch einen WPA2-Enterprise-fähigen Access Point (WLAN-Basis). Die nötigen Einrichtungsschritte haben wir für den veralteten Windows Home Server 2003 in dem Artikel "Windows-Home-Server-sicher-WLAN" gezeigt. Das Folgende zeigt die bei aktuellen Servern nötige Vorgehensweise und widmet sich der Konfiguration stationärer und mobiler Clients. Zur Veranschaulichung dient ein Heimnetzwerk mit jeweils einer Benutzergruppe für Eltern und Kinder.

Wer sich erst noch eine Version des Server-Betriebssystems von Mircosoft kaufen will, bezahlt im günstigsten Fall 40 Euro für den nur noch in Restposten verfügbaren Windows Home Server 2011. Die aktuellen Einsteiger-Server 2012 R2 Foundation und Essentials sind ab 200 Euro und 320 Euro erhältlich. Bei den großen Servern 2012 R2 Standard (574 Euro) und Datacenter (3900 Euro) kommen zum Anschaffungspreis noch Kosten für Nutzer-Client-Access-Licenses (rund 110 Euro für 5 Lizenzen) oder Geräte-Client-Access-Licenses (ab 100 Euro für 5 Lizenzen) hinzu. Jede Lizenz eines großen Servers gilt für zwei physische CPUs (Kerne werden nicht gezählt).

Server und Basis aufmöbeln

Wie Sie den Radius-Server am einfachsten installieren, hängt von der verwendeten Server-Version ab: Nutzer des Home Server 2011 können direkt mit der Konfiguration starten, Nutzer anderer Server-Versionen müssen womöglich zunächst Domänen-Dienste (Active Directory) und die Zertifizierungsstelle vollständig einrichten (siehe Kasten "Zertifikatsquerelen"). Mindestens auf dem Server braucht man nämlich ein Zertifikat. Erst dann sollten Sie die Rolle "Netzwerkrichtlinienserver" (NPS) hinzufügen.



Nur der Home Server 2011 installiert alle für die Radius-Authentifizierung benötigten Rollen einschließlich des Netzwerkrichtlinienservers von sich aus.

Der NPS greift auf dieselben Benutzerkonten zurück wie die übrigen Server-Dienste, um Benutzer zu identifizieren. Die Vergabe von Zugriffsrechten erledigt man am besten über dafür eigens eingerichtete Gruppen. Die sollten Sie spätestens jetzt für die weitere Konfiguration anlegen.

Ob Nutzer und Gruppen in einem Active Directory liegen oder in einer lokalen Nutzerdatenbank wie beim Home Server, ist dem NPS herzlich egal. Im Active Directory empfiehlt Microsoft Benutzerkonten in globalen Gruppen zusammenzufassen und diese wiederum über lokale Gruppen mit unterschiedlichen Rechten zu versorgen.

Nach der Vorarbeit müssen Sie WLAN-Basis und Server einander vorstellen: Die Basis müssen Sie etwa im Web-Interface auf ein anderes Verschlüsselungsverfahren einstellen. Es heißt "WPA2-Enterprise" oder "802.1X". Außerdem müssen Sie die IP-Adresse Ihres Windows Servers eintragen und ein Passwort definieren, das die Kommunikation zwischen WLAN-Basis und Radius-Server absichern soll.

Am Server rufen Sie die Konsole des Netzwerkrichtlinienservers auf und öffnen "RADIUS-Clients und -Server". Markieren Sie "RADIUS-Clients" und wählen in der Menüleiste die Aktion "Neu". Im Fenster "Neuer RADIUS-Client" geben Sie Ihrer WLAN-Basis einen Namen und tragen die IP-Adresse sowie das eben festgelegte Passwort ein. Nutzer von Cisco-Geräten müssen unbedingt den Hersteller unter dem Reiter "Erweitert" umstellen. Das ist notwendig, da Cisco den Radius-Standard anders verarbeitet.

Zertifikatsquerelen

Die Microsoft-eigene Radius-Implementierung setzt zumindest auf Seiten des Windows-Servers ein Zertifikat voraus, mit dem sich die Clients von seiner Vertrauenswürdigkeit überzeugen können. Will man kein offizielles Zertifikat kaufen, hilft ein selbst erzeugtes. Der Home Server 2011 und Essentials 2012 R2 generieren die nötigen Zertifikate automatisch, nicht jedoch die anderen Varianten. Auf diesen benötigen Sie eine Zertifizierungsstelle, die mit einem Active Directory verbunden ist.

Sollte Ihr Server bisher ohne laufen: Fügen Sie im Server-Manager die Rolle "Active Directory-Domänendienste" hinzu und folgen Sie den Hinweisen zur Konfiguration. Anschließend wählen Sie in der Rolle "Active Directory-Zertifikatsdienste" den Punkt "Zertifizierungsstelle" aus. Im Anschluss hilft wieder ein Assistent beim Einrichten der eigenen CA -- seine Vorgaben können Sie akzeptieren.

Bei den regulären Server-Varianten (Standard und Datacenter) müssen Sie abschließend die Zertifizierungsstelle benutzen, um das eigentliche Zertifikat zur Authentifizierung zu erstellen. Starten Sie dazu über Ausführen eine leere Management-Console (mmc.exe) und fügen Sie das Snap-In "Zertifikate" hinzu. Bearbeiten Sie die Zertifikate für das "Computerkonto".

Mit einem Rechtsklick auf "Eigene Zertifikate" können Sie ein neues Zertifikat anfordern. Die Vorgaben des Assistenten übernehmen Sie bis zum Schritt "Zertifikate anfordern". Dort wählen Sie "Domänencontrollerauthentifizierung" aus und klicken auf "Registrieren". Zwei Anmerkungen noch: Ohne Active Directory fehlen der Zertifizierungsstelle in diesem Schritt die Vorlagen. Und: Microsoft rät davon ab, die genannten Rollen auf dem selben Server zu installieren.

Ein NPS beurteilt Anmeldeversuche auf Basis von Richtlinien. Es gibt Verbindungsanforderungsrichtlinien, Netzwerkrichtlinien und Integritätsrichtlinien. Im Normalfall genügt es, für jede Gruppe eine Verbindungsanforderungs- und eine Netzwerkrichtlinie zu erstellen. Über sie kann man die Zugriffsrechte gezielt einstellen. Integritätsrichtlinien braucht man nur für den zusätzlichen Netzwerkschutz NAP (Network Access Protection).
Das Verfahren hält unsichere Clients vom Netzwerk fern, was aber nur mit Windows funktioniert.

Ein Assistent erstellt zusammengehörige Richtliniensätze. Um ihn zu starten, wählt man im NPS-Fenster im Dropdown-Menü unter der Überschrift "Standardkonfiguration" den Menüpunkt "RADIUS-Server für drahtlose oder verkabelte 802.1X Verbindungen" und klickt auf "802.1X konfigurieren". Im Einrichtungsfenster lässt sich zwischen drahtlosen und kabelgebundenen Verbindungen wählen und ein Name vergeben.

Zertifikate, warum eigentlich?

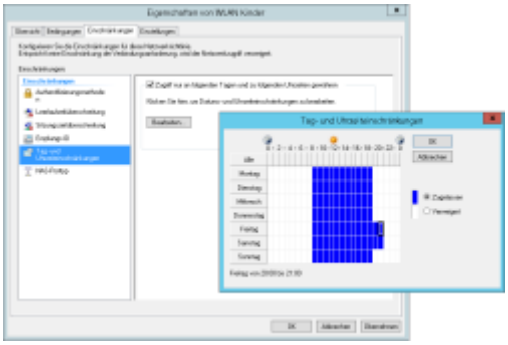
WPA2-Enterprise sieht verschiedene Verfahren zur Anmeldung vor, die auf dem Extensible Authentication Protocol (EAP) aufbauen. Die Variante PEAP stellt einen vernünftigen Kompromiss zwischen Sicherheit und Einfachheit dar. Es weist während des Anmeldevorgangs die Echtheit des Radius-Servers mithilfe eines Zertifikats aus. Das vermeidet, dass sich der Server eines Dritten als der eigene Radius-Server ausgibt und so die Login-Daten abgreift. Für höchste Sicherheit sorgt EAP-TLS. Dieses Authentifizierungsverfahren nutzt zusätzlich individuelle Zertifikate für Clients. Entsprechend muss man sowohl für den Server als auch für die Nutzer Zertifikate erstellen und verteilen.

Nach einem Klick auf "Weiter", wählen Sie ihre im vorherigen Schritt konfigurierte WLAN-Basis aus und nutzen "PEAP" als Authentifizierungsmethode im nächsten Fenster. Öffnen sie danach mit einem Druck auf "Hinzufügen" das Fenster "Gruppe auswählen" und tippen Sie die gewünschten Gruppennamen ein. Ist ihnen das zu umständlich, klicken Sie auf "Erweitert". Dort listet ein Klick auf "Jetzt Suchen" alle auf dem Server befindlichen Nutzergruppen auf. Wählen Sie die gewünschte Gruppe und bestätigen Sie mit "OK".

Jetzt braucht es nur noch zwei Klicks auf "Weiter" und einen auf "Fertigstellen". Für das gewählte Beispiel Familienserver müssten Sie diese Routine zweimal durchlaufen, damit Eltern und Kinder jeweils einen Satz unabhängig editierbarer Zugangsregeln erhalten.

Die erstellten Richtlinien lassen sich unter der gleichnamigen Kategorie im NPS-Fenster anpassen. Im Eigenschaften-Fenster der jeweiligen Richtlinie kann man beispielsweise die

Zugriffszeit einer Kindernutzergruppe einschränken. Die dazugehörige Option versteckt sich in den Eigenschaften der entsprechenden Netzwerkrichtlinie unter "Tag- und Uhrzeiteinschränkungen" im Reiter "Einschränkungen".



Auf Wunsch schränken die Netzwerkrichtlinien die Zugangszeiten ein, zum Beispiel für Kinder. Außerhalb der definierten Zeiträume ist eine Verbindung mit dem Netzwerk nicht möglich. Damit die Zugangsbeschränkungen auch greifen, müssen Sie die Richtlinien in der richtigen Reihenfolge anordnen. Wenn schon die erste Richtlinie den Zugang ermöglicht, werden alle nachfolgenden ignoriert. Haben Sie beispielsweise zwei unterschiedlich stark einschränkende Richtlinien für dieselbe Kindergruppe angelegt, sollten Sie restriktivere Zugangsregel über die schwächere stellen.

Vor dem Einsatz im Alltag sollte man die fertig konfigurierte Radius-Installation ausprobieren. Loggen Sie sich nacheinander über alle Benutzerkonten mit einem Test-Client ein und prüfen Sie, ob der Zugang funktioniert. Wie das geht, erklärt der nächste Abschnitt für verschiedene Gerätetypen- und Hersteller.

Beobachten Sie dabei das Log des Netzwerkrichtlinienservers in der Ereignisanzeige unter "Benutzerdefinierte Ansichten" im Menü "Serverrollen" bei "Netzwerkrichtlinien und Zugriffsdienste". Standardmäßig zeigt es sowohl erfolgreiche als auch abgelehnte Verbindungsversuche.

Wenn alles läuft, können Sie in der Verwaltungskonsole des Netzwerkrichtlinienservers die Protokollwut eindämmen. Sie finden die Optionen über einen Rechtsklick auf den Eintrag "NPS (lokal)" im Unterpunkt "Eigenschaften". Entfernen Sie dort im Reiter "Allgemein" beide Haken. Danach zeichnet Ihr Server nur noch Fehlermeldungen auf.

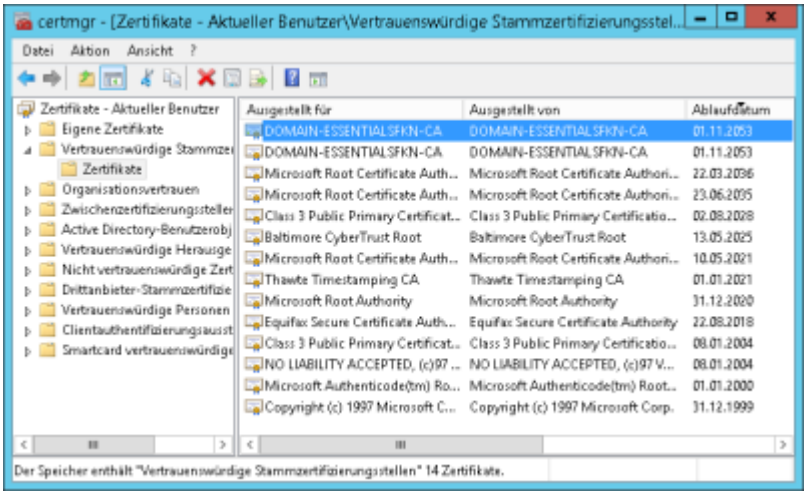
Stationär...

Wer sich unbedarft an einem Radius-gesicherten WLAN anmeldet, etwa per Doppelklick auf das Netz, kann je nach Client und Konfiguration verzweifeln: Trotz mehrfach korrekt eingegebener Credentials misslingt der Zugriff. Wer Uni-WLANs nutzt, lernt schnell, dass man sicher nur dann ins Netz kommt, wenn man akribisch der dafür gefertigten Anleitung folgt.

Das gilt leider auch für das eigene WPA2-Enterprise WLAN. Schuld daran sind vor allem die selbstsignierten Zertifikate. Die Clients trauen dem Server nicht, es sei denn, man macht sich die Mühe, auf jeden Client das Stammzertifikat zu übertragen und dort als vertrauenswürdig

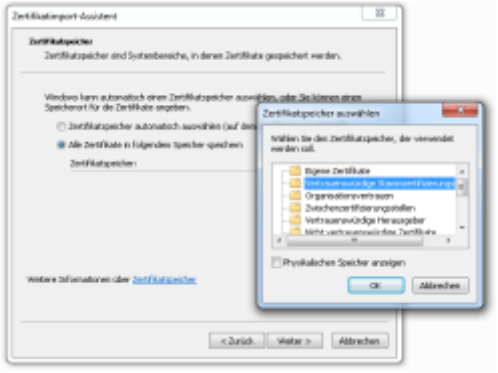
einzustufen. Und selbst das ist keine Garantie für eine erfolgreiche Anmeldung. Die folgenden Rezepte sollten in jedem Fall gelingen.

Um das Stammzertifikat Ihres Servers zu exportieren, starten Sie dort "certmgr.msc" und wählen unter "Vertrauenswürdige Stammzertifikate" den Ordner "Zertifikate". Das gesuchte Stammzertifikat trägt meist den Namen des Servers. Mit einem Rechtsklick auf "Alle Aufgaben" beim Befehl "Exportieren" kann man das Zertifikat auf eine Netzwerkfreigabe oder ein USB-Speichermedium kopieren.



Windows Home Server 2011 und der Server 2012 R2 Essentials generieren während der Installation ein Stammzertifikat. Damit die Clients dem Server bei der Radius-Verbindung trauen, muss es exportiert und auf den Clients importiert werden.

Um das Zertifikat auf Windows 7/8 zu installieren, kopieren Sie die Datei auf den PC und führen mit einem Rechtsklick darauf den Befehl "Zertifikat installieren" aus. Klicken Sie sich im "Zertifikatimport-Assistent" bis zum Fenster "Zertifikatspeicher" durch und wählen "alle Zertifikate in folgendem Speicher speichern" aus. Mit "Durchsuchen" muss dann der Speicherort "Vertrauenswürdige Stammzertifizierungsstelle" ausgewählt werden.



Bei Windows 7 und 8 bringt der Zertifikatimport-Assistent das Stammzertifikat des Radius-Servers auf den Client. Egal ob mit oder ohne Zertifikat, konfigurieren Sie bei Windows 7 die WLAN-Verbindung am besten manuell über das "Netzwerk- und Freigabecenter". Unter "Drahtlosnetzwerke verwalten" erstellen Sie manuell ein Netzwerkprofil mit dem Sicherheitstyp "WPA2-Enterprise" und dem in der WLAN-Basis eingestellten Verschlüsselungsverfahren.

Bei den Verbindungseinstellungen im Reiter "Sicherheit" wählen Sie "Microsoft: Geschütztes EAP" und klicken auf "Einstellungen". Soll eine Verbindung ohne Zertifikate etabliert werden, wählen Sie "Serverzertifikat überprüfen" ab. Andernfalls belassen Sie den Haken und wählen ihr vorher installiertes Stammzertifikat in der Liste weiter unten.

Unter der Schaltfläche "Konfigurieren" neben der Authentifizierungsmethode deaktivieren Sie die Übergabe der Windows-Anmeldedaten, wenn die nicht mit den Credentials übereinstimmen, die auch den Zugang zum Netzwerk ermöglichen. Zum Schluss stellen Sie den Authentifizierungsmodus auf "Benutzerauthentifizierung" in den "Erweiterten Einstellungen" um.

Bei Windows 8 wählt man im Netzwerkcenter "Neue Verbindung oder neues Netzwerk einrichten" und dann "Manuell mit einem Funknetzwerk verbinden". Danach verläuft die Einrichtung wie bei Windows 7.

Gängige Linux-Distributionen verbinden sich am komfortabelsten über das Programm Network Manager mit der WLAN-Basis. Für eine ungesicherte Übertragung der Credentials reicht es, sich mit PEAP, MSCHAPv2, der SSID der Basis-Station und den Credentials anzumelden. Für mehr Sicherheit importiert man das Stammzertifikat im Network Manager und wählt es beim Login aus (siehe: WLAN sichern mit Radius").

Unter Mac OS X wählen Sie ihre WLAN-Basis in den Netzwerkeinstellungen aus und verbinden sich mit Nutzernamen und Passwort. Zertifikate importieren Sie optional in der Schlüsselbundverwaltung in den Ordner "System" und stellen den Vertrauensstatus auf "Immer vertrauen".

...und mobil

Bei Android wählen Sie zunächst Ihre Radius-gesicherte WLAN-Basis über das WLAN-Widget aus. Geben Sie "PEAP" als "EAP-Methode" an und wählen MSCHAPV2 als "Phase-2-Authentifizierung". Soll die Einwahl ohne Zertifikate erfolgen, genügt es weiter unten die Credentials einzugeben. Nach einem Druck auf "Verbinden" bucht sich das Android-Device ins Funknetzwerk ein.

Um die Verbindung mit Zertifikaten zu sichern, kopieren Sie das Server-Stammzertifikat per USB in das Root-Verzeichnis des Gerätes und wählen im Menü den Punkt "Einstellungen". Suchen Sie hier das Untermenü "Sicherheit". Es verbirgt sich häufig unter dem Reiter "Optionen". Im Sicherheitsabschnitt unter dem Punkt "Berechtigungsspeicher" genügt ein Druck auf "Von USB-Speicher installieren", um das Zertifikat zu importieren. Danach reicht es aus, beim Login das Stammzertifikat unter dem Punkt "CA-Zertifikat" auszuwählen.

Windows Phone verbindet sich über "WLAN" unter "Einstellungen" mit dem gewünschten Netz und begnügt sich mit der Eingabe der Login-Daten auch ohne Zertifikat. Ein Stammzertifikat können Sie installieren, indem sie es auf das Gerät übertragen und die Datei antippen. Bejahen Sie die Frage "Zertifikat installieren?" und schon vertraut das Windows Phone Ihrem Radius-Server.

Leider lässt sich das Zertifikat nicht so leicht auf das Gerät übertragen. Microsoft empfiehlt dafür eine E-Mail, eine Website oder Skydrive. Hierbei muss man aber darauf achten, dass die Verbindung vollständig mit SSL abgesichert wird. Damit Windows Phone das Zertifikat nutzt, aktivieren Sie "Serverzertifikat überprüfen" im Login-Bildschirm der WLAN-Einstellungen.

Sonderfall: iPhone

Ihr iPhone können Sie testweise ohne Zertifikate verbinden, es fragt die Credentials ab. Falls es dabei zu einer Fehlermeldung kommt, lassen Sie sich die Details des Serverzertifikats anzeigen. Nach ihrer Bestätigung sollte die Verbindung zustande kommen.

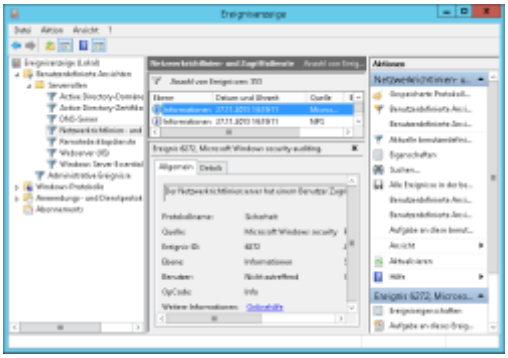
Klappt auch das nicht, hilft nur noch das iPhone-Konfigurationsprogramm. Installieren Sie die für Mac OS X und Windows kostenlos erhältliche Anwendung sowie das Server-Stammzertifikat auf einem Computer, mit dem Sie das iPhone konfigurieren wollen. Starten Sie die Anwendung und erstellen ein neues Konfigurationsprofil. Sie benennen das Profil unter "Allgemein" und wählen danach den Punkt "Zertifikate" aus. Nach einem Klick auf die Schaltfläche "Konfigurieren" müssen Sie das zuvor installierte Server-Stammzertifikat auswählen.

Bei Problemen überredet das iPhone-Konfigurationsprogramm Apples Smartphone dazu, sich mit dem WLAN zu verbinden. Konfigurieren Sie jetzt das WLAN unter der gleichnamigen Rubrik. Geben Sie hierzu die SSID des WLANs und "Firmenweiter WPA/WPA2" als Sicherheitstyp an. Weiter unten markieren Sie "PEAP" unter dem Reiter "Protokolle", geben Ihren Nutzernamen und Ihr Passwort unter "Authentifizierung" an und versehen bei "Vertrauen" ihr eben gewähltes Zertifikat mit einem Haken.

Zum Abschluss verbinden Sie Ihr iPhone mit dem Computer und wählen es im Konfigurationsprogramm aus. Unter dem Reiter "Konfigurationsprofile" installieren Sie Ihr eben erstelltes Profil. Nach einer Bestätigung auf dem iPhone verbindet sich das Smartphone von Apple automatisch mit dem WLAN.

Kleine Fehlerkunde

Schlägt die WLAN-Anmeldung trotz korrekter Credentials fehl, empfiehlt es sich zu kontrollieren, ob der Dienst des Netzwerkrichtlinienservers auch tatsächlich läuft, etwa in der Computerverwaltung. In seltenen Fällen blockiert eine Firewall die Kommunikation zwischen WLAN-Basis und Radius-Server. Die UDP-Ports 1812 und 1813 oder 1645 und 1646 für ältere Geräte sollten durchlässig sein.



Ein Blick in die Ereignisanzeige hilft häufig bei Problemen mit der Radius-Authentifizierung. Nach unseren Erfahrungen hängen die meisten Probleme jedoch mit den Zertifikaten zusammen. Hinweise liefert das NPS-Log in der Ereignisanzeige. Sie finden es unter "Benutzerdefinierte Ansichten" bei den "Serverrollen" im Abschnitt "Netzwerkrichtlinien und Zugriffsdienste".

Wird ein Login-Versuch beispielsweise durch einen angeblich falschen Nutzernamen oder ein falsches Passwort verursacht, kann genauso gut ein nicht installiertes Zertifikat die Ursache sein. In der Regel lohnt es sich, das Server-Zertifikat zu überprüfen oder gegebenenfalls erneut auszustellen.