nwe

Sicherheitskonzept und Sicherheitsprüfung

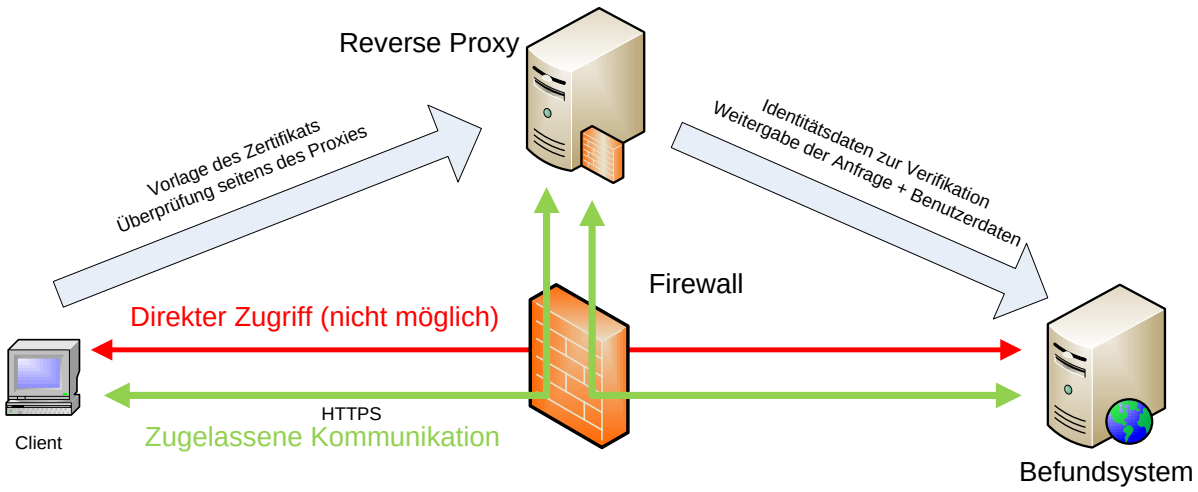
Internetanbindung Befundserver MVZ Labor PD Dr. Volkmann und Kollegen GbR

Einführung

Die Firma MVZ Labor PD Dr. Volkmann und Kollegen GbR, nachstehend als Labor Dr. Volkmann bezeichnet, betreibt eine Plattform zum Abruf von Patientenbefunden. Die Zugänglichkeit zu diesem System wurde bisher überwiegend durch VPN Verbindungen realisiert. Dies ist jedoch durch die erwartete erhöhte Nachfrage nach diesem Dienst keine ausreichend skalierbare Lösung mehr, weshalb eine alternative, aber ebenso sichere Lösung angestrebt wird.

Generelles Konzept

Da es grob fahrlässig wäre, den sogenannten Befundserver direkt ans Internet anzubinden, und ihn so einer Vielzahl von Angriffsmöglichkeiten auszusetzen, wurde ein Sicherheitskonzept erstellt, welches für die Sicherheit der vertraulichen Daten im Rahmen des Datenschutzes sorgt. Die Anbindung des Systems erfolgt über ein sogenanntes Reverse Proxy System über das HTTPS Protokoll, mit einer Serverzertifikatsstärke von 2048bit (RSA Verschlüsselung). Zudem existiert eine vorgeschaltete Firewall, welche Direktzugriffe auf den Befundserver unterbindet, und nur Zugriffe auf den HTTPS Port des Reverse Proxy Systems zulässt. Die Verschlüsselung der Verbindung (https), garantiert den Datenschutz während des Transfers vom Reverse Proxy zum Client im Internet. Abhörangriffe auf der Strecke sind daher praktisch unmöglich. Als weitere Sicherheitsbarriere kommen X509 Zertifikate mit privatem Schlüssel zum Einsatz, welche wenn einmal im Client installiert, diesem den Zugriff auf das Reverse Proxy System erlauben. Sollte der Client bei Aufruf der Seite nicht über ein gültiges Zertifikat verfügen, wird er vom Reverse Proxy System bereits in dieser Stufe zurückgewiesen. Die Zertifikate werden beim Import in den Windows Certificate Store durch Labor Dr. Volkmann als nicht exportierbar markiert, wodurch dem Diebstahl von Zertifikaten nach erfolgter Installation vorgebeugt wird. Hierfür ist es erforderlich, dass nur Clients eingesetzt werden, die den Windows Certificate Store benutzen. Andere Produkte, wie z.B. Mozilla Firefox unterstützen diesen Schutzmechanismus nicht, und können nicht eingesetzt werden. Die grundsätzliche Kommunikation spielt sich nur zwischen Client und Reverse Proxy, beziehungsweise Reverse Proxy und Befundsystem ab. Der Client hat niemals direkten Zugriff auf den Befundserver, um potentielle Angriffe zu unterbinden. Als letzte Barriere werden durch das Befundsystem empfangene Identitätsdaten aus dem Zertifikat des Clients (welche durch den Reverse Proxy nach erfolgreicher Prüfung weitergegeben wurden) mit dem Benutzerstamm abgeglichen. Der Benutzer braucht also zusätzlich zu seinem Benutzernamen und Passwort auch noch ein gültiges Zertifikat, welches ihm zudem in der Datenbank zugeordnet sein muss.



Sicherheitsebene HTTPS Verschlüsselung

HTTPS steht für HyperText Transfer Protocol Secure und wurde als Verfahren entwickelt um Daten im World Wide Web abhörsicher zu übertragen. Es funktioniert wie unverschlüsseltes http im Rahmen einer zusätzlichen Schicht zwischen http und TCP. Die eigentliche Verschlüsselung des http Verkehrs erfolgt dann via SSL/TLS.

Ohne eine Verschlüsselung wie sie HTTPS bietet, sind Web-Daten für jeden der Zugang zum entsprechenden Netz hat im Klartext lesbar.

Bei HTTPS erfolgt dazu im Gegensatz unter Verwendung des SSL-Handshake-Protokolls eine geschützte Identifikation und Authentifizierung der Kommunikationspartner. Anschließend wird dann mit einer asymmetrischen Verschlüsselung oder des Diffie-Hellman-Schlüsselaustauschs ein gemeinsamer symmetrischer Sitzungsschlüssel ausgetauscht. Der so generierte Schlüssel wird dann im weiteren Verlauf zur Verschlüsselung der Nutzdaten verwendet.

In diesem speziellen Konzept kommen zusätzlich signierte Clientzertifikate nach X-509.3 zum Einsatz, welche eine Authentifizierung des Clients gegenüber dem Server ermöglichen, und damit eine weitere Sicherheitsstufe darstellen.

In der Regel einigen sich die gängigen Clients mit dem Server auf eine RC4 (bis 128bit) oder eine AES Verschlüsselung. Die bei SSL eingesetzten Verschlüsselungsverfahren werden unabhängig von ihrem Einsatzzweck regelmäßig überprüft, und gelten als mathematisch sicher. Das heißt sie lassen sich theoretisch mit den heute bekannten Techniken nicht brechen. Die Zuverlässigkeit wird regelmäßig zum Beispiel durch Wettbewerbe unter Kryptologen überprüft.

Sicherheitsebene x509 Zertifikate

Als zusätzliche Sicherheitsebene zur verschlüsselten Datenübertragung via HTTPS kommen elektronische Ausweise in Form von x509 Zertifikaten nach dem X-509.3 Standard zum Einsatz. Diese Zertifikate werden von einer internen Zertifizierungsstelle signiert, und erhalten damit die Gültigkeit zum Verbindungsaufbau mit dem System. Durch die Signierung ist es nicht möglich, sich selbst einen Ausweis mit den gleichen Identitätsdaten auszustellen, da diese vom Server aufgrund der fehlenden Signierung zurückgewiesen werden würden. Um den Diebstahl von solchen elektronischen Ausweisen unmöglich zu machen, werden die Zertifikate beim Installieren in den Windows Certificate Store als nicht exportierbar markiert. Von daher ist es nicht möglich im Rahmen dieses Konzeptes Clientprodukte zu verwenden, die den Windows Certififcate Store nicht benutzen (z.B. Mozilla Firefox). Es ist demnach bei Benutzung des Windows Certificate Store praktisch nicht möglich die Zertifikate aus dem Client zu entwenden um sie dann gegebenenfalls auf einem nicht autorisierten System erneut zu installieren und sich damit unberechtigten Zugriff zu verschaffen.

Sicherheitsebene Identitätsprüfung der Applikation

Die Identitätsdaten des Zertifikats werden seitens der Applikation als ergänzende Sicherheitsmaßnahme bei der Benutzerauthentifizierung verwendet. So reichen dem Benutzer zur Anmeldung am System nicht alleine sein Benutzername und Passwort – er muss zusätzlich noch über gültige Identitätsdaten aus dem Zertifikat verfügen, welche seinem Benutzer zugeordnet sind, um Zugang zu erhalten.

Zusätzliche Empfehlung

Generell ist das beschrieben Konzept als sicher zu bezeichnen. Auf der Zertifikatsebene wäre theoretisch noch eine weitere Sicherheitsstufe möglich, welche jedoch mit der Installation von Software auf dem Client verbunden wäre. Die Zertifikatsdaten sowie die dazugehörigen privaten Schlüssel könnten auf Smartcards (e.g. eToken von Aladdin) hinterlegt werden, der private Schlüssel wird somit nicht im System abgelegt. Hierfür muss auf dem Client zusätzlich entsprechende Treibersoftware installiert werden, und jeder Nutzer benötigt effektiv ein solches Token, welches zusätzliche Kosten bei der Implementation verursacht. Selbst bei Verlust des Tokens ist es nicht möglich ohne ein entsprechendes Passwort an die enthaltenen Daten zu kommen.

Prüfprotokoll

Serverzertifikat

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, ST=BW, L=Karlsruhe, O=MVZ Labor Volkmann, OU=HTTP Forward Proxy, CN=MVZ Labor Volkmann
CA/emailAddress=.
        Validity
            Not Before: Jul 26 11:58:47 2013 GMT
            Not After : Jul  2 11:58:47 2113 GMT
        Subject: C=DE, ST=BW, L=Karlsruhe, O=MVZ Labor Volkmann, OU=HTTP Forward Proxy,
CN=dfue.labka1978.de/emailAddress=.
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                            Modulus (2048 bit):
                            <gekürzt>
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Server
            Netscape Comment:
                Easy-RSA Generated Server Certificate
            X509v3 Subject Key Identifier:
                FD:E4:5A:9E:3A:4A:D8:E8:A2:0A:2C:4F:2F:E6:5B:67:6B:B9:88:7D
            X509v3 Authority Key Identifier:
                keyid:E3:9C:35:9B:F8:0D:A7:BF:63:78:06:18:75:06:8D:2C:81:6D:04:4A
                DirName:/C=DE/ST=BW/L=Karlsruhe/O=MVZ Labor Volkmann/OU=HTTP Forward Proxy/CN=MVZ Labor Volkmann
CA/emailAddress=.
                serial:8C:96:F3:30:40:2C:64:2B

            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Digital Signature, Key Encipherment
    Signature Algorithm: sha1WithRSAEncryption
                            <gekürzt>
```

Beispielzertifikat Client

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 203 (0xcb)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=DE, ST=BW, L=Karlsruhe, O=MVZ Labor Volkmann, OU=HTTP Forward Proxy, CN=MVZ Labor Volkmann CA/emailAddress=.
    Validity
      Not Before: Sep 30 13:32:24 2013 GMT
      Not After : Sep 28 13:32:24 2023 GMT
    Subject: C=DE, ST=BW, L=Karlsruhe, O=MVZ Labor Volkmann, OU=HTTP Forward Proxy, CN=ARZT3329/emailAddress=.
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
        <gekürzt>
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      Netscape Comment:
        Easy-RSA Generated Certificate
      X509v3 Subject Key Identifier:
        C1:DC:E6:D3:F6:64:29:1A:88:16:47:DB:82:7A:39:FB:13:37:5E:A4
      X509v3 Authority Key Identifier:
        keyid:E3:9C:35:9B:F8:0D:A7:BF:63:78:06:18:75:06:8D:2C:81:6D:04:4A
        DirName:/C=DE/ST=BW/L=Karlsruhe/O=MVZ Labor Volkmann/OU=HTTP Forward Proxy/CN=MVZ Labor Volkmann CA/emailAddress=.
        serial:8C:96:F3:30:40:2C:64:2B

      X509v3 Extended Key Usage:
        TLS Web Client Authentication
      X509v3 Key Usage:
        Digital Signature
  Signature Algorithm: sha1WithRSAEncryption
                <gekürzt>

Zugriffstests

Im Rahmen des Zugriffstests sind die gewünschten Ergebnisse in **grün** dargestellt, potentiell ungewünschte Ergebnisse wurden **rot** markiert und mit einem Kommentar versehen.

Zugriff ohne gültiges Zertifikat	fehlgeschlagen
Zugriff mit selbstausgestelltem Zertifikat	fehlgeschlagen
Zugriff mit exportiertem Zertifikat (ohne Private Key)	fehlgeschlagen
Zugriff mit gültigem Zertifikat	erfolgreich

Clienttests

Exportierbarkeit Windows Certificate Store	bei korrekter Installation* nicht möglich
Exportierbarkeit Mozilla Firefox	möglich, Nutzung nicht empfohlen!!!

*Bei der Installation von den Zertifikaten in den Windows Certificate Store ist unbedingt darauf zu achten, dass die Zertifikate als nicht exportierbar markiert sind, daher sollte die Installation beim Endbenutzer auch nur durch Administratoren des Labor Dr. Volkmann vorgenommen werden.

Firewalling

Direktzugriff auf das Befundsystem	nicht möglich
Zugriff auf das Reverse Proxy System	möglich