

TC Sicherheitsinformationen

SSL CERTIFICATES

Sicherheit im Internet geht alle an

Eines ist sicher: Erfolgreiches Online-Business basiert vor allem auf Vertrauen. Mit Secure Sockets Layer – kurz SSL – und einem passenden Zertifikat für Ihren Server geben Sie Ihren Kunden und Geschäftspartnern das, was wichtig ist: Sicherheit und Vertrauen.

Aber auch der Nutzer muss seinen Teil dazu beitragen, sich sicher im Internet zu bewegen. Das Web hat sich in den letzten zehn Jahren von der Anzeige einfacher Textseiten zu einer umfangreichen interaktiven Anwendung entwickelt. Viele alte Browser können diese neuen Inhalte nicht mehr richtig darstellen. Aber schlimmer noch, sie weisen erhebliche Sicherheitslücken auf. Neben betrügerischen Websites sind auch Würmer, Viren oder Trojaner bekannte Risiken, vor denen man sich schützen kann. So gehört zu einem sicheren Zugang zum Internet neben aktueller Virensoftware auch ein Computer mit aktuellem Betriebssystem und aktuellem Browser. Ein regelmäßiges Update veralteter Systeme ist deshalb dringend notwendig, da ansonsten bekannte Sicherheitslücken die Integrität von Daten, Systemen und Netzwerken gefährden.

Publikationen der letzten Zeit bestätigen dies eindrucksvoll, wie diese kleine Sammlung belegt:

www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Sicherheitsluecke_IE_150110.html

» Kritische Sicherheitslücke im Internet Explorer - BSI empfiehlt die vorübergehende Nutzung alternativer Browser; Bonn, 15.01.2010 ... «

www.sicher-im-netz.de/wir_ueber_uns/329_1652.aspx

» Internetnutzer sollten darauf achten, möglichst die neueste Version eines Browsers zu verwenden. Gerade in den letzten Versionen wurden die Sicherheitsarchitekturen der Browser grundlegend überarbeitet und auf die neuesten Angriffsmethoden angepasst... «

www.heise.de/security/dienste/Browsercheck-2107.html

» Durch diese große Bandbreite an Funktionen und die damit einhergehende Komplexität der Browser schleichen sich immer wieder Programmierfehler ein... «

Regelmäßige kostenlose Warn- und Informationsdienste bietet beispielsweise das Bürger-CERT des BSI:

www.buerger-cert.de

Sicherheit von Root-Zertifikaten

Veraltete Betriebssystem- oder Browserversionen unterstützen außerdem die Prüfung vieler SSL-Zertifikate nicht und verwirren mit entsprechenden Fehlermeldungen die Benutzer oder gaukeln ihnen eine falsche Sicherheit vor. In der Regel verfügen veraltete Browser- bzw. Betriebssysteme nicht über die aktuellen Root-Zertifikate, die notwendig sind, um die Echtheit eines SSL-Zertifikats zu prüfen. Anders als moderne Systeme verfügen Altsysteme nicht über automatische Update-Fähigkeiten, so dass fehlende Root-Zertifikate nicht mehr nachgeladen werden. Diese Root-Zertifikate können in der Regel manuell von den Webseiten der SSL-Anbieter nachgeladen werden (bei TC TrustCenter etwa unter: www.trustcenter.de/infocenter/root_certificates.htm), doch dieses Vorgehen sollte nur in Ausnahmefällen genutzt werden. Aus übergeordneten Sicherheitsgründen ist in diesen Fällen immer der Upgrade auf aktuelle Browser-Versionen wie etwa MS IE 8 oder Firefox 3.6 vorzuziehen. Was nutzt ein geprüftes SSL-Zertifikat beim Online-Banking, wenn der PC ansonsten alle Chancen für Angriffe bietet?

Verschärft wird die Situation für Nutzer alter Systeme dadurch, dass viele Zertifikatsanbieter ihre Root-Zertifikate bald erneuern, um höhere Sicherheitsanforderungen an die Schlüssellängen zu erfüllen. So verwendet auch TC TrustCenter mit Beginn des Jahres Root-Zertifikate mit erweiterter Schlüssellänge.

TC Sicherheitsinformationen

SSL CERTIFICATES

Grund hierfür sind die aktuellen Einschätzungen der Sicherheit von Schlüssellängen und Kryptoalgorithmen durch anerkannte Institutionen wie dem National Institute of Standards and Technology (NIST), dem European Telecommunications Standards Institute (ETSI) oder dem Bundesamt für Sicherheit in der Informationstechnik (BSI).

Die Verwendung von sogenannten Zwischen-CA Zertifikaten (auch Sub- oder Intermediate-CA Zertifikat genannt) ist ein weiterer Mechanismus, um die Sicherheit von Zertifikaten zu stärken. Dabei werden die Server- bzw. Client-Zertifikate nicht direkt von der Root-CA signiert, sondern von einem dazwischen geschalteten, separaten CA-Zertifikat. TC TrustCenter hat dies bei der Umstellung auf die neue Rootgeneration berücksichtigt und stellt Server- und Client-Zertifikate seit dem 11.12.2009 nur noch unterhalb einer SubCA aus. Als Nebeneffekt verringert dieses Modell die Größe der Sperrlisten (CRLs), was zu einem beschleunigten Validierungsprozess bei CRL-basierten Verfahren führt. Installationshinweise für Zwischen-CA Zertifikate von TC TrustCenter finden Sie hier: www.trustcenter.de/installation_instruction_for_intermediate_ca_certificate_ll.htm

Die führenden Browserhersteller Microsoft und Mozilla haben dementsprechend ihre Anforderung für die Vorinstallation der Root-Zertifikate in die Zertifikatsspeicher der Browser verschärft, so dass die Umstellung auf erweiterte Schlüssellängen und die Verwendung Sub-CA-Zertifikaten bald von vielen Anbietern vorgenommen werden wird. Damit haben veraltete Browser- bzw. Betriebssysteme nur noch geringe Chancen. Hier hilft nur ein Upgrade auf aktuelle und sichere Browser.

Sichere Browser-Software

Microsoft Internet Explorer 7.0+

www.update.microsoft.com/windowsupdate/v6/default.aspx?ln=de

Mozilla Firefox 3.0+

www.mozilla.com/de

Google Chrome 4.0+

www.opera.com/download/get.pl?id=32656&thanks=true=true

Opera 10+

www.opera.com/download

Safari 3.0+

www.apple.com/safari

Browserhersteller wie Microsoft, Mozilla (Firefox) und Apple bieten regelmäßig aktualisierte Updates an. Wenn nicht eine automatisierte Update-Funktion verwendet wird, empfiehlt sich ein regelmäßiger Besuch der Update-Webseiten der Hersteller, um die aktuellen Updates herunterzuladen und zu installieren. Beim Internet-Explorer werden die Aktualisierungen (Updates) als Bestandteil der ohnehin empfehlenswerten Windows-Update-Funktion gesteuert.

Einen derartigen Service des Betriebssystems gibt es für Firefox nicht. Deshalb besitzt er eine eigene Update-Funktion (Extras/Einstellungen/Erweitert/Update), die so eingestellt werden kann und sollte, dass sich der Browser automatisch aktualisiert.

In Unternehmensnetzwerken wird die Aktualisierung der eingesetzten Software meist über automatische Softwareverteilung oder die Aufforderung zum manuellen Update realisiert. Hier sind die IT-Verantwortlichen gefordert, die notwendigen Sicherheitsanforderungen im Patch-Management zu berücksichtigen.

Zum Auffinden veralteter Software auf Windows-Systemen eignet sich der Update-Checker von Secunia:

www.heise.de/security/dienste/Update-Check-843063.html

Für Privatpersonen bietet das Deutsche Sicherheitsnetz e. V. (Desine, www.desine.de) kostenlose Browser-Beratung und direkte Hilfe per Telefon und Fernwartung an: www.desine.de/presse/20100125-kostenloser-browserschutz.pdf

Schlüssellängen für Server- und Client-Zertifikate

Aber nicht nur für Root- und CA-Zertifikate gelten zukünftig strengere Anforderungen:

So fordert das CA/Browser Forum, ein freiwilliger Zusammenschluss führender Zertifizierungsstellen (CAs) und Internet-Browser-Software-Anbieter, in den im Jahr 2007 veröffentlichten Leitlinien für Extended Validation (EV)-Zertifikate, dass Zertifikate, die über den 31. Dezembers 2010 hinaus gültig sind, eine Schlüssellänge von mindestens 2048 Bit aufweisen müssen. Deshalb ist bei Extended Validation (EV) Zertifikaten (z.B. TC Extended Trust SSL) die Schlüssellänge 2048 Bit bereits heute zwingend.

Das National Institute of Standards and Technology (NIST) empfiehlt generell die Schlüssellängen bis Ende 2010 auf 2048 Bit anzuheben: http://csrc.nist.gov/publications/drafts/800-131/draft-800-131_transition-paper.pdf

Das Windows® Root Certificate Program von Microsoft (<http://technet.microsoft.com/en-us/library/cc751157.aspx>) verbietet den eingetragenen Zertifizierungsstellen ab dem 01.01.2011 die Ausstellung von Zertifikaten mit 1024 Bit unterhalb einer öffentlichen Root gänzlich.

Aus Sicherheitsgründen empfiehlt TC TrustCenter bereits heute eine Schlüssellänge von 2048 Bit zu verwenden.

Unsere Empfehlung für Online-Anbieter: Klären Sie Ihre Kunden auf!

Einige Anbieter von Online-Diensten, die mit ihren Kunden vertrauliche Daten austauschen (Banken, Shops mit Bezahlungsfunktion etc.), informieren ihre Kunden im eigenen Interesse direkt auf ihrer Webseite über Sicherheitsrisiken und Schutzmöglichkeiten. Zusätzlich wird die Aufklärung von vielen Kunden als Zeichen eines vertrauenswürdigen Kundenservices gewertet.

Sicherheitsempfehlungen und Tipps für ein sicheres Bewegen im Internet gibt auch das BSI:

Für Behörden und Unternehmen:

www.bsi.bund.de/cln_174/DE/Themen/InternetSicherheit/internetsicherheit_node.html

Für Bürger:

www.bsi-fuer-buerger.de/cln_165/BSIFB/DE/Home/home_node.html