

Schwache Web-Server-Zertifikate gefährden Online-Shopping

 Zu schwache Web-Server-Zertifikate könnten von Hackern dechiffriert werden. Hiervor warnt ein Bericht in der bekannten Fachzeitschrift c't des Heise-Verlags: "Erschreckend viele https-Zertifikate nutzen schwache Schlüssel und lassen sich demnach einfach fälschen."

Prüfen Sie Ihr Zertifikat jetzt und reagieren Sie rechtzeitig.

Hier die Meldung zum Thema, die alle Shopbetreiber lesen sollten, sofern Sie ein eigenes SSL-Zertifikat einsetzen:

Beim Online-Shopping sollen https-Verbindungen dafür sorgen, dass der Kunde sicher sein kann, auf der richtigen Seite gelandet zu sein und seine Daten nur verschlüsselt an den Server zu schicken. Durch einen Fehler des Paketbetreuers erzeugten jedoch Debian-Systeme über anderthalb Jahre schwache OpenSSL-Schlüssel. Kommen diese als Zertifikat von https-Sites zum Einsatz, können Kriminelle nicht nur den verschlüsselten Verkehr einfach dechiffrieren, sondern auch gefälschte https-Sites unter dem Namen des Shops aufsetzen.

Bei einer Untersuchung von über 4.300 gültigen Zertifikaten, die im Browser keine Warnung erzeugten, fand c't, dass etwa jedes dreißigste einen solchen schwachen Schlüssel nutzt. Darunter fanden sich auch Online-Shops, die zum Beispiel zur Eingabe von Kreditkartennummern auffordern. Hochgerechnet auf die über 800.000 SSL-Sites, die Netcraft in seiner letzten SSL-Untersuchung registrierte, ergibt das rund 25.000 schwache Zertifikate.

Damit ein Zertifikat vom Browser ohne Warnung akzeptiert wird, muss eine Zertifizierungsstelle (Certification Authority, CA) die Identität des Eigentümers beglaubigen. Alle von c't befragten CAs erklärten, man könne bei ihnen schwache Zertifikate kostenlos widerrufen und durch neue ersetzen lassen.

*Doch offenbar machen von dieser Möglichkeit bislang nur wenige Zertifikatseigner Gebrauch. So zeigt etwa die Widerrufsliste von Verisign, dass in den vergangenen Wochen nicht mehr Widerrufe erstellt wurden als gewöhnlich. Das mag daran liegen, dass die internationalen CAs anders als die deutschen ihre Kunden nicht aktiv benachrichtigen. Wer unsicher ist, kann das Zertifikat seiner Website mit einem **Tool von heise Netze** testen.*

Doch selbst ein Widerruf der schwachen Zertifikate schafft das Problem nicht aus der Welt. Denn die meisten aktuellen Browser überprüfen die Widerrufslisten in ihrer Standardkonfiguration nicht. Die Certification Revocation Lists werden schnell so groß, dass der Download zu lange dauert und die Serverkapazitäten der CAs nicht ausreichen. Das Online Certificate Status Protocol (OCSP), wie es Internet Explorer 7 unter Vista und Firefox 3 nutzen, ermöglicht den Test einzelner Zertifikate. Allerdings unterstützen das viele CAs noch nicht. Von den gefundenen, schwachen Zertifikaten enthielten weniger als 20 Prozent eine OCSP-URL. Das bedeutet, dass viele der schwachen Zertifikate von vielen Browsern auch nach ihrem Widerruf ohne Warnung akzeptiert werden, bis sie regulär ablaufen.