25.08.2013

PFS - Folgenlos ist sicherer

SSL Zertifikate verlieren Ihre Schutzwirkung, wenn das Schlüsselpaar abhanden kommt. Abhilfe schafft ein neues Verfahren mit temporären Sitzungsschlüsseln. Wir erklären, was es damit auf sich hat und helfen bei der Einrichtung.

Bei der Verschlüsselung ihrer Kommunikation sollten Unternehmen künftig nicht mehr nur auf SSL alleine vertrauen. Zu diesem Ergebnis gelangt ein Symposium mittelständischer Unternehmen in Bonn auf Einladung der icertificate GmbH, einem führenden Distributor für digitale Verschlüsselung. Zwar sichern SSL Zertifikate eine Verbindung zuverlässig ab, sie können dies aber nur so lange tun, wie ihr eigenes Schlüsselpaar wirklich geheim bleibt. Gelingt es jedoch einem Dritten, an den Private Key oder gar den SSL Master-Key zu gelangen, kann er nicht nur gegenwärtige, sondern auf vergangene Kommunikationen entschlüsseln und Daten ausspähen.

Abhilfe schafft hier "PFS", was für *perfect forward secrecy* steht und Verschlüsselungsverfahren beschreibt, bei dem für jede neue Kommunikationssitzung (Session) ein neuer Schlüssel generiert wird. Hierzu tauschen die Verbindungspartner eine Reihe von Details aus, aus denen sie einen *temporären Sitzungsschlüssel* ermitteln. Dieser Schlüssel, die *Passphrase*, wird dabei nie mit übertragen oder nirgendwo abgespeichert. Nach Ende der Sitzung wird der Schlüssel vernichtet. Jede Sitzung wird somit individuell verschlüsselt, eine nachträgliche Entschlüsselung einer aufgezeichneten SSL-Sitzung ist selbst mit vorhandenem Master Key nicht möglich.

Aktuelle Webserver und Browser sind bereits in der Lage, mittels PFS zu verschlüsseln. Viele Administratoren wissen jedoch nicht um die Möglichkeiten oder den Konfigurationsweg, PFS für sich zu aktivieren. Eine ausführliche Anleitung zur Einrichtung der eigenen Hardware auf PFS gibt die icertificate GmbH in ihren Tutorials und zeigt auf, mit welchen SSL Zertifikaten die Verwendung des neuen Verfahrens am Besten umgesetzt werden kann.

HowTo

Perfect Forward Secrecy (PFS) einrichten bei Apache 2.x
Perfect Forward Secrecy (PFS) einrichten bei IIS 7.x

Link zum Originalartikel
Impressum