Datenschutz newsbox

Ausgabe 3 2015

DATAKONTEXT

FREAK bedroht IT-Sicherheit

War es im Jahre 2014 unter anderem der sog. Heartbleed-Bug, der durch einen schwerwiegenden Programmfehler in älteren Versionen der Open-Source-Bibliothek OpenSSL dazu führte, dass über verschlüsselte TLS-Verbindungen private Daten von Clients und Servern ausgelesen werden konnten, ist es in diesen Tagen eine Schwachstelle im SSL bzw. TLS-Protokoll, der die Verantwortlichen für die IT-Sicherheit beschäftigt.

Bei der sog. Freak Sicherheitslücke liegt der Fokus auf der Verwendung der sog. Cipher Suiten bei verschlüsselten Verbindungen. Bei dem Aufbau einer verschlüsselten Verbindung müssen zwischen Klient und Server die verwendeten Verschlüsselungsverfahren ausgehandelt werden. Dabei haben der Server und der Klient jeweils eine Liste der von ihnen unterstützen Verschlüsselungsverfahren. Der Klient macht eine Vorschlag und der Server akzeptiert diesen Vorschlag oder sagt "beherrsche ich nicht, wir müssen was anderes nehmen". Können die beiden sich nicht auf eine Cipher Suite einigen, kommt keine Verbindung zu Stande. Es müssen das Protokoll (SSL, TLS) und vier Algorithmen vereinbart werden: das Schlüsselaustauschverfahren (RSA, DH) das Authentifizierungsverfahren (RSA, DSA, ECDSA) das Verschlüsselungsalgorithmus inkl. Schlüssellänge (keine, RC4, DES, 3DES, IDEA, AES die verwendete Hashfunktion (MD5, SHA1, SHA2).

Was muss ein Administrator tun, um seinen Server so zu konfigurieren, damit nur sichere Cipher Suiten verwendet werden?
Die derzeit beste verfügbare Anleitung ist ein umfangreiches PDF-Dokument "Applied Crypto Hardening" von bettercrypto.org. Erfahrene Praktiker aus europäischen Certs und Hochschulen haben für die gängigsten Webserver (Apache, lighttpd, nginx und MS IIS) die sichere Konfiguration der Cipher Suiten beschrieben. Alle Beispiele können direkt per Copy & Paste übernommen werden. Darüber hinaus wird die Krypto-Konfiguration von SSH, Mail Server, VPNs, PGP, Instant Messaging Systemen Datenbanken und anderen Systemen beschrieben. Obwohl das Dokument noch den Status "draft" hat, gibt es derzeit wohl keine bessere Anleitung.

Wer jetzt seine eigenen SSL/TLS fähigen Server überprüfen möchte, dem sei der Kommandozeilen SSL-Scanner SSLyze ans Herz gelegt. Das in Python geschriebene Programm ist für Windows, OS X und Linux verfügbar.

Mehr Infos zu FREAK und dem Thema IT-Sicherheit finden Sie im IT-Sicherheitsblog.