profihost

Erreichbar. Verlässlich. Bezahlbar.

Profihost AG – Pressemitteilung vom 10.4.2014

Forward Secrecy: Profihost verbessert Abhörsicherheit von Webseiten

Hannover – Im Rahmen eines umfassenden Updates hat die Profihost AG die serverseitige Verschlüsselungstechnologie auf das extrem sicherere Forward Secrecy-Verfahren umgestellt. Während bei der konventionellen SSL-Verschlüsselung jeweils nur ein fester Schlüssel für die Absicherung der Datenübertragung verwendet wurde, setzt die SSL-Zusatzfunktion Forward Secrecy auf sitzungsbasierte Verschlüsselung, die immer wieder neue Schlüssel nutzt. "Konventionelle SSL-Übertragungen können aufgezeichnet und im Nachhinein dekodiert werden. Mit Forward Secrecy hat kein Angreifer eine realistische Chance auf Erfolg. Hier kommt bei jeder Datenübertragung ein komplett neuer, zufällig generierter Schlüssel zum Einsatz", führt Sebastian Bluhm, Vorstand bei der Profihost AG, aus.

Das neue Verfahren setzt auf das Folgenlosigkeitsprinzip und kommt ohne Master-Schlüssel aus. Angreifer müssten demnach statt einem einzigen Schlüssel gleich eine Vielzahl knacken, um den Datenaustausch "abzuhören". Diese Sitzungsschlüssel werden während der Übertragung ausgehandelt und direkt danach vernichtet. "Forward Secrecy verhindert somit wirkungsvoll, dass bereits abgeschlossene, aber verschlüsselt aufgezeichnete Kommunikation durch nachträgliches Bekanntwerden nur eines geheimen Schlüssels kompromittiert wird. Das Verfahren schafft damit deutlich mehr Sicherheit beim Austausch von Daten über im Internet", so der Vorstand der Profihost AG.

Die Abhörskandale rund um PRISM & Co. haben gezeigt, wie begehrt Daten nicht nur bei Kriminellen und Industriespionen, sondern auch bei ausländischen Geheimdiensten sind. Gerade für Betreiber von E-Commerce-Projekten wird es daher immer wichtiger, den Datenaustausch auf ihren Websites konsequent zu verschlüsseln, um sensible Informationen ihrer Kunden zu schützen. Bisher galt bei der Datenverschlüsselung der Einsatz von SSL-Zertifikaten als Maß aller Dinge. "Die Abhörskandale haben jedoch deutlich gemacht, dass diese allein nicht mehr das notwendige Schutzniveau gewährleisten können", so Sebastian Bluhm. Mit dem Einsatz des wenig genutzten Forward-Secrecy Verfahrens hat das hannoversche IT-Unternehmen nun einen wichtigen Schritt zu einer noch besseren Absicherung von Unternehmensdaten im Internet getan.

Weitere Informationen unter www.profihost.com

Profihost AG
Am Mittelfelde 29 · 30519 Hannover
Telefon +49 511 5151 8181
Telefax +49 511 5151 8282
info@profihost.com
www.profihost.com

Commerzbank AG
BLZ 27040080 · Konto 6511646
Swift/BIC COBADEFFXXX
IBAN DE20270400800651164600
USt.-Ident.-Nr. DE813460827
Steuer-Nr. 2325 271 05518

Vorstand Cristoph Bluhm
Sebastian Bluhm
Stefan Priebe
Vorsitzender des Aufsichtsrats
Prof. Dr. iur. Winfried Huck
Amtsgericht Hannover · HRB 202350