PRESSEMITTEILUNG

"NSA knackt Verschlüsselung im Internet"

TeleTrusT – Bundesverband IT-Sicherheit e.V.: 50 % der schutzwürdigen Internetkommunikation nutzt unsichere Verschlüsselungsalgorithmen

Einfallstor für Entschlüsselung / Anwender sollten sichere Algorithmen wählen

Berlin, 06.09.2013 – TeleTrusT fordert Anwender auf, Server so zu konfigurieren, dass nur anerkannt sichere Verschlüsselungsalgorithmen zur Anwendung kommen.

Nach Erkenntnissen des TeleTrusT - Bundesverband IT-Sicherheit e.V. wird bei 2% der gesamten Internetkommunikation SSL genutzt, bei 0,5 % IPsec. Diese Angaben beruhen auf Erhebungen des Institutes für Internetsicherheit if(is). Prozentual erscheint dies wenig, ist aber bezogen auf das gesamte Internet eine beachtliche Größe, zumal man annehmen kann, dass es sich bei diesen 2% um besonders schutzwürdige Datenübermittlung handelt.

Prof. Dr. Pohlmann, TeleTrusT-Vorsitzender und Direktor des Institutes: "Bei SSL-Kommunikation wird serverseitig automatisiert ein Profil ausgewählt, das Verschlüsselungsalgorithmen nutzt, z.B. RC4 oder DES-Varianten, von denen man annehmen kann, dass z.B. die NSA in der Lage ist, sie zu entschlüsseln".

Alternativ ist beispielsweise 'AES 256 Bit' in Gebrauch, was nach derzeitigem Kenntnisstand nicht entschlüsselt werden kann.

Man muss vor diesem Hintergrund fragen, warum bei der Hälfte der schutzwürdigen Internetkommunikation möglicherweise unsichere Algorithmen verwendet werden. Ebenso muss man konstatieren, dass öffentlich verfügbare SSL-Technologie Schwachstellen aufweist, die z.B. von der NSA für Angriffe genutzt werden könnte.

TeleTrusT fordert Anwender in Deutschland in ihrem eigenen Interesse auf, Server so zu konfigurieren, dass nur anerkannt sichere Verschlüsselungsalgorithmen zur Anwendung kommen und stets die aktuellsten verfügbaren Software-Updates implementiert werden.

TeleTrusT – Bundesverband IT-Sicherheit e.V., Dr. Holger Mühlbauer, Geschäftsführer, Chausseestraße 17, 10115 Berlin, Tel.: +49 30 /40054310, holger.muehlbauer@teletrust.de
www.teletrust.de