**BigBrotherAward 2019 Kategorie Technik – Laudator: Frank Rosengart**

Der BigBrotherAward 2019 in der Kategorie Technik geht an

das „Technical Committee CYBER“ des Europäischen Instituts für Telekommunikationsnormen (ETSI), vertreten durch den Chairman Alex Leadbeater,

für seine Bemühung, das „Enterprise Transport Security“-Protokoll (ETS) als Teil des neuen technischen Standards für die Verschlüsselung im Internet festzulegen und damit abgesicherte Verbindungen mit einer Sollbruchstelle auszustatten.

Aber von Anfang an:

Verschlüsselte Verbindungen, z.B. beim Online-Banking oder beim Internet-Einkauf, sind mittlerweile Standard. Wir erkennen sie an zwei Zeichen: Erstens wird im Browser ein Schloss-Symbol in der Adressleiste vom Browser eingeblendet, und vor der Adresse steht ein „https“. Der Kommunikationskanal zwischen Browser und Server ist nun mittels „Transport Layer Security“, kurz TLS, gesichert. Das bisher dafür genutzte Protokoll TLS in der Version 1.2 ist gut zehn Jahre alt, und im Laufe der Zeit wurden Angriffsmöglichkeiten entdeckt, mit denen Kriminelle oder auch staatliche Stellen die Verschlüsselung knacken können. Es muss ein neuer Standard her.

Seit über zwei Jahren setzen sich internationale Gremien wie die „Internet Engineering Task Force“, kurz IETF, mit Kryptographie-Experten zusammen und überlegen, wie eine solche Verschlüsselung ausgestaltet sein muss, damit sie für die nächsten Jahre als sicher gelten kann. Heraus kam die Version 1.3 der Transport Layer Security, kurz TLS. In den meisten Browsern ist eine vorläufige Version davon schon integriert. So weit, so gut, so sicher. Wenn da nicht das ETSI wäre.

Denn noch während der Beratungen über TLS 1.3 meldeten sich unter anderem Vertreter der Finanzindustrie zu Wort und wandten ein, dass sie strenge Compliance-Auflagen hätten, die es erforderlich machen, auch verschlüsselte Kommunikation, z.B. von Finanzberatern mit ihren Kunden, zu protokollieren - zum Beispiel um nachweisen zu können, dass sie gesetzestreu arbeiten. Sie behaupteten, sie bräuchten einen Nachschlüssel, um trotz Verschlüsselung für Dritte selbst alles lesen zu können. Dabei handelt es sich zwar um Daten, die sie auch auf ihren Servern im Klartext lesen könnten, aber für eine IT-Abteilung ist es einfacher, solche Daten an einem zentralen Punkt abzugreifen.

Diese Idee für einen Nachschlüssel fanden natürlich auch die europäischen Geheimdienste brillant. Allen voran der britische GCHQ, der über Mitglieder des National Cyber Security Centres

im „Technical Committee CYBER“ beim Europäischen Institut für Telekommunikationsnormen (ETSI), unserem Preisträger, vertreten ist.

Das IETF hingegen hatte sich mit dem Standard TLS 1.3 ausdrücklich gegen den Nachschlüssel entschieden. Dessen ungeachtet ging das ETSI mit dem Kopf durch die Wand und entwickelte eine spezielle Version von TLS, das sogenannte Enterprise-TLS, kurz ETS.

ETS hat nun diesen Nachschlüssel. Es ist eine Verschlüsselung mit Sollbruchstelle. Während beim stärkeren TLS 1.3. ein Server und ein Browser regelmäßig neue Schlüssel technisch miteinander aushandeln, wird bei ETS ein fester Schlüssel beim Server-Betreiber hinterlegt. Das mag für Banken noch legitim sein, da es dort in der Regel um ihre „eigenen“ Kommunikationsinhalte geht.

Der Haken beim ETS-Standard ist aber, dass staatliche Stellen die Server-Betreiber verpflichten können, einen solchen festen Schlüssel einzustellen und diesen herauszurücken, um damit sämtliche Kommunikation mit Internetseiten im Nachhinein entschlüsseln zu können, zum Beispiel versendete Nachrichten. Falls dieser Nachschlüssel Kriminellen in die Hände fällt, können die zum Beispiel auch Passwörter und andere sensible Informationen abgreifen.

Eine besondere Gemeinheit ist außerdem, dass dieser „kaputte“ Verschlüsselungsstandard für Browser und damit die Nutzer.innen nicht vom „echten“ zu unterscheiden ist. Es wird weiterhin das Schlüsselsymbol angezeigt; und der Browser hat technisch kaum eine Möglichkeit zu erkennen, ob ein fester Verbindungsschlüssel hinterlegt ist.

Die Mitglieder unseres Preisträgers, des „Technical Committees CYBER“, haben damit trotz aller Warnungen der IETF und anderer Experten einen zweiten Standard geschaffen, der wohl auch in der Praxis verwendet werden wird. Aber wer ihn verwendet, bringt damit Nutzerinnen und Nutzer in die erhebliche Gefahr, dass ihre vermeintlich sichere Kommunikation ohne ihr Wissen ausspioniert werden kann.

Daher raten wir allen Entwicklern und technisch Verantwortlichen, einen großen Bogen um ETS zu machen und das deutlich sicherere TLS 1.3-Protokoll zu verwenden. Fatalerweise haben technisch nicht versierte Nutzerinnen und Nutzer kaum eine Möglichkeit, darauf Einfluss zu nehmen. Dieser zweite, unsichere ETS-Standard schafft eine verheerende Situation für die Online-Sicherheit. Da können wir nur ironisch „Danke für gar nichts“ sagen.

Herzlichen Glückwunsch zum BigBrotherAward 2019, Technical Committee CYBER des ETSI!