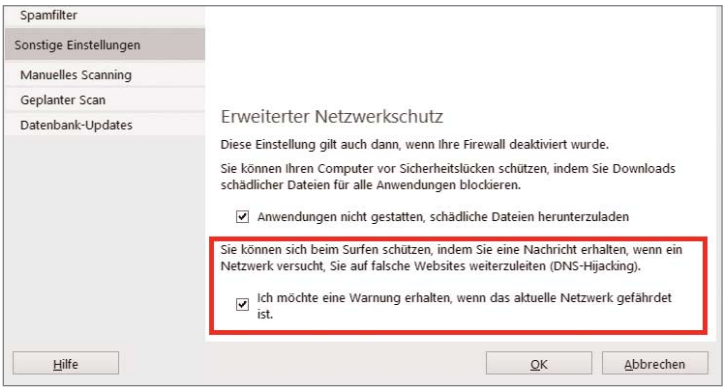
F-Secure Internet Security 2016 mit Schutz vor Router-Hacks



Die neue Version von F-Secure Internet Security soll Angriffe auf Router erkennen und Nutzer warnen.

F-Secure erweitert seine Internet-Security-Software um einen Network Checker. Dieser überprüft Netzwerkeinstellungen und DNS-Einträge, um Angriffe auf Router zu erkennen.

Dieses Jahr machte ein Exploit-Kit die Runde, das gezielt Lücken in 50 Router-Modellen unterschiedlicher Hersteller ausnutzte. Die Attacke verändert die Adresse des DNS-Servers. Anschließend erfolgt die Namensauflösung der URLs durch einen von den Angreifern kontrollierten PC, der den Datenverkehr etwa gezielt auf Phishing-Seiten umleitet.

Der Network Checker überprüft die Einstellungen in vordefinierten Intervallen. Bei potenziellen Problemen warnt er den Benutzer und zeigt ihm, wie er diese beispielsweise durch eine Aktualisierung der Router-Firmware beheben kann.

F-Secure Internet Security 2016 soll am 16. September erscheinen. Bestandskunden erhalten die neuen Funktionen über die reguläre Update-Funktion; eine Installation der 2016-Version soll nicht nötig sein. Der Preis liegt wie gehabt bei 35 Euro für einen und 50 Euro für drei PCs. Die Verlängerung des jährlichen Abos kostet 30 beziehungsweise 40 Euro. (rme@ct.de)

Der Ashley-Madison-Hack und seine Folgen

Eine Hacker-Gruppe namens Impact Team hat Daten von Nutzern des Seitensprung-Portals Ashley Madison veröffentlicht. Darunter befinden sich auch Firmen-Interna wie das E-Mail-Archiv des Chefs der Muttergesellschaft Avid Live Media (ALV). Die Hacker waren im Juli in das Computersystem eingedrungen und kopierten dabei 36 GByte Daten. Dem Security-Blogger Brian Krebs zufolge haben schon erste Erpressungsversuche stattgefunden. Außerdem gebe es zwei bislang unbestätigte Suizid-Fälle. In Kanada und den USA wurde das Seitensprung-Portal bereits von mehreren Nutzern verklagt. Die Hacker berufen sich auf moralische Gründe; angeblich wollten sie betrügerische Geschäfte aufdecken. Dabei setzten sie auf erpresserische Methoden und stellten ALV kurz nach dem Einbruch in das Computer-System ein Ultimatum. Darin forderten die Hacker, Ashley Madison offline zu nehmen, um die Veröffentlichung der erbeuteten Daten zu verhindern. (des@ct.de)

BSI will sichere E-Mail-Anbieter kennzeichnen

Das Bundesamt für Sicherheit und Informationstechnik (BSI) will den E-Mail-Versand sicherer machen. Dafür hat es den Entwurf der technischen Richtlinie „Sicherer E-Mail-Transport“ definiert, die ein am Verfahren teilnehmender E-Mail-Anbieter erfüllen muss. Zu den Anforderungen gehören gesicherte DNS-Abfragen, obligatorische Transport-Verschlüsselung, sichere Kryptografie und vertrauenswürdige Zertifikate.

Das Sicherheitskonzept muss der Anbieter selbst erstellen und umsetzen. In Zukunft soll dieser von einer unabhängigen, nicht näher beschriebenen Stelle ein Zertifikat erhalten. Die E-Mail-Anbieter GMX und Web.de bereiten sich augenscheinlich schon darauf vor: Jüngst führten sie Ende-zu-Ende-Verschlüsselung via PGP ein und wollen künftig auch auf die in den BSI-Anforderungen verankerten Sicherheits-Standards DANE und DNSSEC setzen (siehe c’t 19/15, S. 40). (des@ct.de)

NSA erforscht Post-Quanten-Kryptografie

Die National Security Agency (NSA) hat die Spezifikationen von Post-Quanten-Kryptoalgorithmen angekündigt. Sie reagiert damit auf die bevorstehende Umsetzung von Quantencomputern. Mit diesen lassen sich die mathematischen Grundprobleme von asymmetrischen Verfahren wie DSA und RSA in recht kurzer Zeit knacken. Davon sind auch Krypto-Verfahren wie ECDSA betroffen, die auf elliptischen Kurven basieren. Für symmetrische Verfahren wie AES stellen Quantencomputer hingegen keine Bedrohung dar.

Firmen wie etwa Google und Microsoft schrauben zwar bereits an den Computern der Zukunft; die Entwicklung steckt aber noch in den Kinderschuhen. Allerdings weiß niemand, was die NSA in ihren Kellern stehen hat, denn die arbeitet ebenfalls an Quantencomputern zum Knacken von Kryptoalgorithmen. Das bereitet dem Rest der Welt zunehmend Sorgen. Die NSA empfiehlt, dass Institutionen, die noch nicht auf als sicher geltende kryptografische Verfahren setzen, jetzt nicht mehr umzusteigen brauchen und lieber auf Post-Quanten-Kryptografie warten sollen. Die Einführung neuer Verfahren ist jedoch ein langwieriger Prozess und kann durchaus zehn Jahre oder länger dauern. Bis dahin soll man also dem Willen der NSA zufolge auf schwache Verschlüsselung setzen. (des@ct.de)

Sicherheits-Notizen

Den Nachfolger der Verschlüsselungs-Software **Boxcryptor** gibt es für Windows 10 nur in einer kostenpflichtigen Abo-Version für 36 oder 72 Euro im Jahr. Der Vorgänger funktioniert mit Windows 10 nur eingeschränkt.

Besitzer von **iOS-Geräten** sollten die Version 8.4.1 des mobilen Betriebssystems einspielen. Diese schließt eine Lücke, über die eine präparierte, vom Nutzer vermeintlich geschlossene App im Hintergrund weiter Daten abfischen kann.

Über eine Lücke in der Youtube-App von **Nintendos 3DS** kann man eigenen Code ausführen und etwa Homebrew-Programme starten. Nintendo hat bislang kein Update angekündigt.

Über eine neue Schwachstelle im Mediaserver von **Android** können Angreifer Geräte abermals in eine Wanze verwandeln. Wie bei den Stagefright-Lücken ist auch hier nicht bekannt, wann die Hersteller Updates ausliefern.