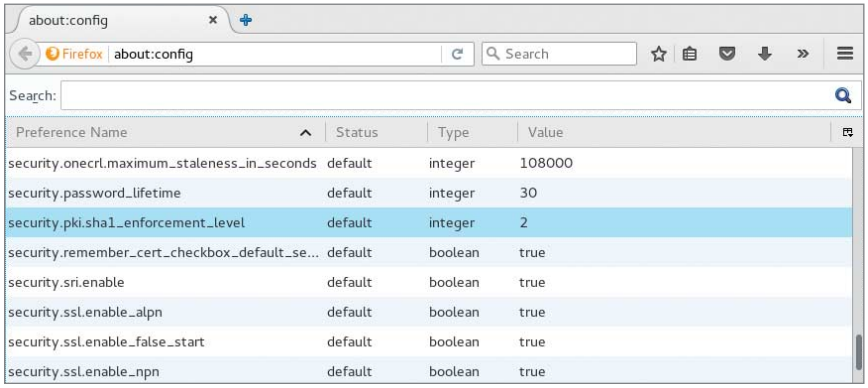
Firefox erst einmal wieder mit SHA-1

Anfang des Jahres hatte Mozilla planmäßig damit angefangen, die als unsicher geltenden SHA-1-Zertifikate für SSL/TLS-Verbindungen in Firefox zurückzuweisen. Da dies bei einigen Nutzern zu Problemen führte, machten die Entwickler diesen Schritt mit einem Update wieder rückgängig. Auslöser für den Rückzieher sind Sicherheits-Produkte, die Man-in-the-Middle-Entschlüsselung durchführen. Darunter Web-Filter und Anti-Viren-Software, die verschlüsselten Traffic aufmachen muss, um den Inhalt zu untersuchen. Viele Produkte kommen nicht damit zurecht, dass der Browser die von ihnen verteilten SHA-1-Zertifikate nicht akzeptiert. Probleme bereiten auch die Web-Zugänge einiger Router. Laut Mozilla arbeiten viele Hersteller daran, das Problem in ihren Geräten zu lösen. Bis dahin will man weiterhin SHA-1-Zertifikate erlauben. (fab@ct.de)



Wer das über SSL verteilte Firefox-Update nicht einspielen kann, kann den Wert der SHA-1-Enforcement-Variable im about:config-Dialog des Browsers manuell auf 0 setzen, um Seiten mit SHA-1-Zertifikaten aufrufen zu können.

Router-Gefahr bei Unitymedia und UPC

Kunden des deutschen Kabelnetz-Providers Unitymedia und des österreichischen Providers UPC sollten unbedingt das voreingestellte WLAN-Passwort Ihres Routers ändern – sofern nicht bereits geschehen. Ein Angreifer kann die Passwörter bei den von den Providern gestellten Routern offenbar aus dem öffentlich einsehbaren WLAN-Namen (SSID) ableiten. Ein frei zugängliches Tool spuckt nach Eingabe der SSID die möglichen Default-Passwörter aus. Voreingestellte WLAN-Passwörter entpuppen sich immer wieder als Sicherheitsproblem; man sollte sie nach Inbetriebnahme eines Routers grundsätzlich ändern – auch wenn man im aktuellen Fall nicht betroffen ist. Weiteren Schutz bringt das Abschalten von WPS. (rei@ct.de)

Triple-Seven: Sicherheitslöcher in OpenSSH

Im OpenSSH-Code schlummerten seit 2010 Schwachstellen (CVE-2016-0777 und -0778), die es bösartigen Servern erlauben, den Speicherinhalt des Clients auszulesen – inklusive der sensiblen privaten Schlüssel. Auf Grund der CVE-Nummern hat die Schwachstelle in sozialen Netzwerken den Spitznamen „Triple-Seven“ bekommen. Betroffen sind alle OpenSSH-Versionen von 5.4 bis einschließlich 7.1; das Update 7.1p2 schließt die Lücke. Außerdem gibt es Patches für OpenSSH 5.8 und 5.7.

Die Bugs befinden sich im sogenannten Roaming Support, einer OpenSSH-Funktion, die nie komplett eingeführt wurde. Zwar unterstützen die Clients die Option seit OpenSSH 5.4, im Server-Code wurde sie aber nie freigeschaltet. Mit der Roaming-Funktion sollten die beiden Enden der SSH-Verbindung ihre Kommunikation wieder aufnehmen können, wenn sie unvermittelt abreißt. Wer die Patches nicht einspielen kann, sollte die Roaming-Funktion in der SSH-Konfigurationsdatei (global oder in der Nutzer-spezifischen Datei im Home-Verzeichnis) mit folgendem Befehl komplett abschalten: `UseRoaming no`.

Angreifbar sind alle ungepatchten OpenSSH-Clients in der Standardkonfiguration. Allerdings ist ein Man-in-the-Middle-Angriff nicht möglich, das Opfer muss sich also mit einem bösartigen Server verbinden. Auch kann die Schwachstelle nur ausgenutzt werden, nachdem das Opfer sich bereits erfolgreich angemeldet hat, weshalb Linux-Distributor Red Hat die Lücke nur als „moderat“ einschätzt. Kompromittierte SSH-Server können aber immerhin bei jeder Anmeldung eines Clients dessen geheimen Schlüssel auslesen. (fab@ct.de)

Support-Ende für viele Internet-Explorer-Versionen

Microsoft leistet keinen Support für ältere Internet-Explorer-Versionen mehr. Für jede unterstützte Windows-Version gibt es Updates nur noch für die jeweils aktuellste IE-Version. Nutzer sollten spätestens jetzt auf den neuesten IE für ihr Betriebssystem umsteigen, da ihr Browser sonst keine Sicherheits-Updates mehr erhält. Da der Browser die größte Angriffsfläche bei modernen Windows-Systemen darstellt, wäre es fatal, eine veraltete Version weiterzubenutzen.

Konkret heißt das für Vista-Nutzer, dass sie sicherstellen sollten, dass sie IE 9 nutzen. Falls noch nicht geschehen, sollte bei Windows 7 und 8.1 auf IE 11 aktualisiert werden. Für die meisten Heimanwender gibt es wahrscheinlich gar nichts zu tun, da auf vielen Rechnern schon irgendwann in der Vergangenheit ein entsprechendes Update eingespielt wurde. Falls das nicht der Fall ist, hilft Windows Update dabei, das nachzuholen. Auch wer den IE gar nicht aktiv benutzt, sollte die Updates installieren, da das Programm tief in Windows verwurzelt ist.

Angreifer können das ausnutzen, indem sie dem Anwender über verschiedene Wege Links unterjubeln, die auf dem System mit IE geöffnet werden. Welches Betriebssystem ab sofort welche IE-Version noch mit Updates versorgt, hat Microsoft auf einer Support-Seite zusammengetragen. (fab@ct.de)

c't Noch unterstützte IE-Versionen: ct.de/yrgz

Sicherheits-Notizen

Abzock-Anrufer geben sich telefonisch als Dell-Techniker aus und versuchen dem Angerufenen sein Geld aus der Tasche zu ziehen.

Im Passwort-Manager der AV-Software von **Trend-Micro** wurden kritische Schwachstellen entdeckt. Abhilfe schafft ein Update auf die aktuelle Version.

Die **PHP-Updates** mit den Versionsnummern 7.0, 5.5 und 5.6 schließen mehrere Sicherheitslücken und beseitigen zahlreiche Bugs.

Die **Cisco Identity Services Engine** plagen zwei kritische Schwachstellen. Neben der Wireless-LAN-Controller-Software sind auch noch Aironet-Basisstationen der 1800-Serie verwundbar. Sicherheits-Updates stehen bereit.

Firewalls der Sicherheitsfirma **Fortinet** hatten jahrelang ein fest eingestelltes Passwort, das Admin-Zugriff auf die Geräte über SSH ermöglicht. Anfällig sind alle FortiOS-Versionen von 4.3.0 bis einschließlich 5.07 – erschienen sind diese zwischen November 2012 und Juli 2014.