FritzBox fremdgesteuert

Durch eine Schwachstelle in den MyFritz-Fernwartungs-Apps für die FritzBoxen hätten Angreifer dauerhaft die Kontrolle über die AVM-Router übernehmen können. Die für Android und iOS erhältlichen Apps kommunizierten zwar über HTTPS verschlüsselt mit den FritzBoxen, allerdings überprüften sie das ihnen vorgesetzte Zertifikat nicht ausreichend.

Es gelang heise Security, den Datenverkehr der Apps zu entschlüsseln und daraus die Session-ID des Nutzers zu extrahieren. Mit dieser kann man sich an der FritzBox des Opfers anmelden und sich sogar dauerhaften Zugriff verschaffen. Voraussetzung für den Angriff ist, dass der Datenschnüffler den Traffic des Opfers über sich umleiten kann. Das funktioniert etwa, wenn beide das gleiche Netz nutzen – zum Beispiel einen öffentlichen Hotspot.

heise Security hatte AVM im Vorfeld über die Sicherheitslücke informiert. Daraufhin veröffentlichte der Router-Hersteller innerhalb von drei Monaten abgesicherte Versionen seiner MyFritz-Apps. Wer die Apps nutzt, sollte sie über den App Store respektive Google Play umgehend auf den aktuellen Stand bringen.(rei)

Synology-NAS jetzt patchen!

Eine Schadsoftware namens SynoLocker hat es gezielt auf die Netzwerkspeicher von Synology abgesehen: Sie nutzt eine Lücke in älteren Firmware-Versionen, um in das NAS-System einzudringen und verschlüsselt alle Dateien, die sie darauf finden kann.

Wer wieder auf seine Dateien zugreifen will, soll ein Lösegeld von über 200 Euro zahlen. Bislang ist kein Weg bekannt, die Verschlüsselung zu knacken – die Virenschreiber haben sich keine Fehler erlaubt. Es gibt zwar ein Tool von F-Secure, das die betroffenen Dateien entschlüsselt, es benötigt jedoch den passenden Krypto-Schlüssel, den es bei den Erpressern freizukaufen gilt.

Wer ein Synology-NAS betreibt, sollte unbedingt sicherstellen, dass darauf die aktuelle Firmware (DiskStation-Manager-Software, DSM) läuft. Darüber hinaus sollte man regelmäßig ein Backup der auf dem NAS gespeicherten Dateien durchführen. Falls ein Schädling wie SynoLocker einen neuen Weg findet, das System zu infizieren, kommt man dann fast schadlos davon. (rei)

c't NAS-Update: ct.de/yn66

Firefox blockiert böse Zertifikats-Zwillinge

Ab der nächsten Version 32 soll auch Firefox das sogenannte „Public Key Pinning“ beherrschen, um vor missbräuchlich ausgestellten Zertifikaten vertrauenswürdiger Herausgeber zu warnen. Damit wandelt Mozilla in den Spuren von Google, dessen Chrome-Browser das Pinning bereits seit Längerem beherrscht.

Zertifikatsherausgeber (Certificate Authorities, CAs) können grundsätzlich gültige Zertifikate für jede beliebige Domain wie etwa Google.com ausstellen. Eigentlich müssen sie dabei überprüfen, ob das Zertifikat vom legitimen Besitzer der Domain beantragt wurde. Es kam jedoch schon mehrfach vor, dass diese Überprüfung nicht stattgefunden hat – teilweise unter ungeklärten Umständen.

Befindet sich die betroffene CA auf der Liste der vertrauenswürdigen Herausgeber des Browsers, kann das fatale Folgen haben: Gelingt es einem Angreifer, den Traffic seines Opfers umzuleiten, kann er sich unbemerkt in dessen verschlüsselten Datenverkehr einklinken, ihn mitlesen und manipulieren. Beim Public Key Pinning gibt es eine Liste, in der verzeichnet ist, welcher Herausgeber Zertifikate für eine bestimmte Domain ausstellen darf. Wurde das Zertifikat von einer anderen CA ausgestellt, bewertet es der Browser als ungültig. Die Liste wird vom Browser-Hersteller vorgegeben.

Mozilla plant offenbar, nach und nach die Liste von Google Chrome zu übernehmen. Den Anfang machen mit Version 32 diverse Twitter-Domains sowie die Domains von Mozillas Addon-Verzeichnis und Content Delivery Network. Mit Version 33 folgen die Google-Domains sowie weitere von Twitter und mit Version 34 schließlich auch Dropbox, TOR und accounts.firefox.com.

Künftig soll Firefox darüber hinaus die „Public Key Pinning Extension for HTTP“ unterstützen. Dann können Webseitenbetreiber über den HTTP-Header festlegen, welche CAs sie üblicherweise benutzen. Entdeckt der Browser beim nächsten Besuch ein Zertifikat, das von einer anderen CA stammt, schlägt er Alarm. (rei)

Microsoft patcht

Microsoft hat das problembehaftete Sicherheits-Update KB2982791 aus dem Patch-Paket MS14-045 für Windows überarbeitet und als KB2993651 veröffentlicht. Das Unternehmen hatte es ursprünglich an seinem August-Patchday herausgegeben, musste es jedoch kurz darauf wieder zurückziehen. Das Update führte bei einigen Nutzern zu Fehlern wie Bluescreens und einer fehlerhaften Darstellung von Schriften.

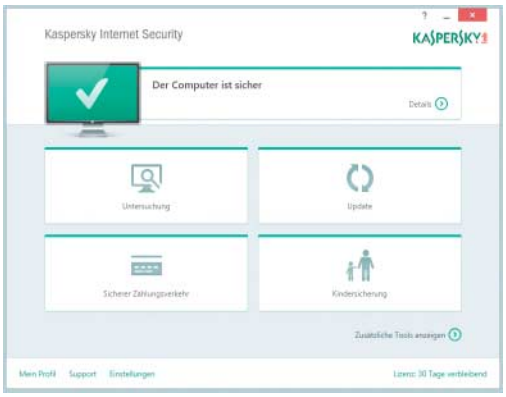
Der Hersteller rät, den alten Patch vor der Installation des neuen zu entfernen, auch wenn dies nicht zwingend erforderlich sei. Die korrigierte Fassung wird bereits über Windows Update verteilt. Das Sicherheitsupdate betrifft alle noch unterstützten Windows-Versionen. Über die gestopften Lücken kann sich ein Angreifer, der bereits Code zur Ausführung gebracht hat, höhere Rechte verschaffen. (rei)

Kaspersky 2015 will Krypto-Trojaner ausbremsen

Die 2015er-Generation von Kaspersky Lab soll besser vor Verschlüsselungs-Trojanern schützen, die das digitale Hab und Gut des Nutzers in Geiselhaft nehmen. Laut Hersteller prüft der Wächter mittels eines heuristischen Verfahrens, ob ein Prozess bösartiger Natur ist, wenn er auf die persönlichen Dokumente des Anwenders zugreift.

Schlägt die Heuristik an, legt Kaspersky 2015 zunächst Schattenkopien der betroffenen Dateien an und gibt die Dokumente danach zum Verändern frei. Das soll vermeiden, dass zu Unrecht verdächtigte – also erwünschte – Software an ihrer Arbeit gehindert wird. Nach Beseitigung der Ransomware sollen sich die verschlüsselten Dateien mit den unverschlüsselten Sicherungskopien überschreiben lassen.

Als weitere Neuerung hat Kaspersky einen Webcam-Schutz eingebaut, der den unberechtigten Zugriff auf Videogeräte durch Hacker oder Spähsoftware unterbinden soll. Damit will der Hersteller die allgegenwärtigen Klebestreifen auf Notebook-Webcams überflüssig machen. Ob ein Software-Modul den gleichen hundertprozentigen Schutz bietet wie ein Stück Klebeband, bleibt abzuwarten – zumindest hat eine wirklich blindgemachten Kamera eine beruhigendere Wirkung.



Unter der kantigen Haube von Kasperskys 2015er-Generation steckt unter anderem ein verbesserter Schutz vor Krypto-Trojanern und Webcam-Spionen.

Kaspersky Anti-Virus 2015 läuft auf Windows ab XP mit Service Pack 3. Für ein Gerät und ein Jahr kostet es 30 Euro. Für die größere Version Internet Security werden 40 Euro fällig. Sie bringt zusätzlich zu den Malware-Schutzfunktionen noch Extras wie Kindersicherung und Online-Banking-Schutz mit. Lizenzen für drei Geräte kosten jeweils 20 Euro mehr. (jss)

© Copyright by Heise Zeitschriften Verlag
Persönliches PDF für alle Leser der c't aus 30625 Hannover