WLAN-Router im Sicherheits-Check

Firmware-Analyse findet zahlreiche Lücken

Wie sicher sind Router? Spannende Frage, aber nur schwer zu beantworten. Daher haben wir uns mit der Firma IoT Inspector zusammengeschlossen und mit automatisierten Tests neun aktuelle WLAN-Router durchleuchtet

VON JÖRG GEIGER

Alles fing mit einem Brainstorming im CHIP-Testlabor an. Die Ingenieure brüteten über der Frage, wie man die Tests von WLAN-Routern weiter verbessern könnte. Derzeit haben wir zwar mehr als genug Daten in der Bestenliste, um eine fundierte Kaufempfehlung zu geben. Die spannende Frage ist jedoch, ob man die Sicherheit nicht auch testen könnte, schließlich ist sie für WLAN-Router ein besonders wichtiges Feature.

Die Antwort darauf ist kompliziert. Grundsätzlich sind Sicherheitstests von WLAN-Routern kein Ding der Unmöglichkeit, aber sie brauchen sehr viel Zeit und fachliche Expertise. Das Prozedere sieht so aus, dass sich ein Sicherheitsexperte das jeweilige Gerät vornimmt und verschiedene Tests durchführt, um einen Router auf Schwachstellen zu überprüfen.

Wichtige Fragen bei diesem Pentesting sind etwa, ob ein Angriff aus dem Internet gelingt, wie Attacken im Heimnetz funktionieren und welche Schutzfunktionen eingebaut sind, sollte ein Angreifer direkt auf die Hardware zugreifen können. Professionelle Pentester veranschlagen pro Gerät rund 14 bis 21 Tage Testzeit.

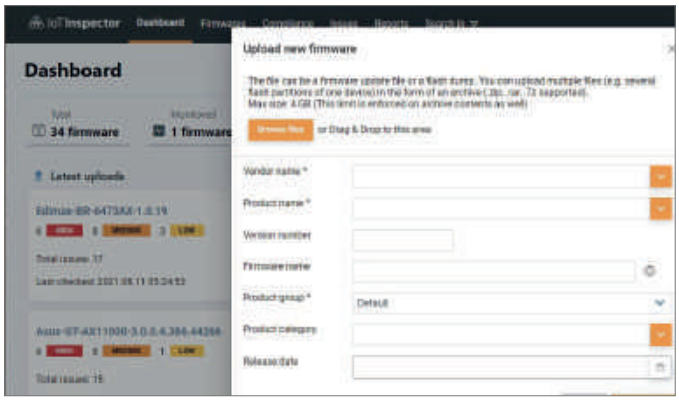
Sicherheitstest in 15 Minuten

Pentests sind mit drei Wochen Dauer lang und teuer. Man muss auch bedenken, dass die Sicherheitstests nach Firmware-Updates größtenteils zu wiederholen sind. Außerdem kann es passieren, dass allzu invasive Methoden den WLAN-Router unbrauchbar machen. Da wir im Testlabor mit neuen Geräten arbeiten, die uns für einen begrenzten Zeitraum bereitgestellt werden, dürfte ein solcher Test die Hersteller nicht begeistern. Umso interessanter finden wir den automatisierten Sicherheitstest der Firma IoT Inspector, der in wenigen Minuten ein Resultat ausspuckt.

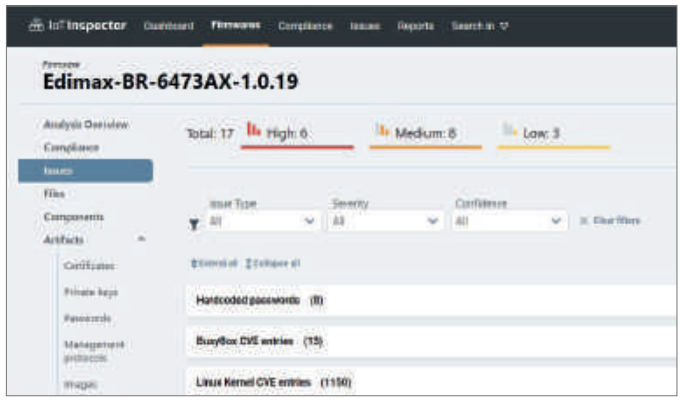
Wir wollen keinen falschen Eindruck erwecken. Pentester ist immer noch ein sicherer Job, denn eine Automatik kann nach aktuellem technischem Stand den handwerklichen Test in seiner Tiefe nicht ersetzen. In der IT gilt aber nicht zu Unrecht der Grundsatz: Was sich automatisieren lässt, soll man auch automatisieren. Ein Durchlauf mit IoT Inspector ist immer interessant, weil er bekannte Schwachstellen findet und dabei über 5.000 Lücken aus der CVE-Datenbank überprüft, einer öffentlichen Liste von Schwachstellen.

Software[1] zu diesem Beitrag finden Sie auf der **virtuellen CHIP-DVD**

[1]E-Paper-Leser können die virtuelle DVD unter **chip-kiosk.de/produkte** nachbestellen



Sicherheitstest per Firmware-Upload
Die Sicherheitsanalyse bei IoT Inspector findet komplett ohne Gerät statt, Nutzer laden einfach die Firmware zum Anbieter hoch



Gefundene Risiken in WLAN-Routern
Nach der Firmware-Analyse erzeugt IoT Inspector einen übersichtlichen Report mit vielen Details zu den gefundenen Lücken

Bei den von uns in Auftrag gegebenen neun WLAN-Routern konnten wir so in wenigen Minuten 226 potenzielle Sicherheitslücken aufspüren. Wichtig ist, dieses Ergebnis korrekt einzuordnen: Die Automatik weist nur auf bestimmte Probleme hin wie veraltete Software oder gefundene Passwort-Hashes. Dabei können sich auch Fehlalarme einschleichen, wenn zum Beispiel der IoT Inspector vor einer veralteten Dienste-Version auf dem Router warnt. Unter Umständen wird das betroffene Modul im Standardmodus nicht ausgeführt oder es sind bestimmte Vorbedingungen nicht erfüllt, um die gemeldete Sicherheitslücke ausnutzen zu können.

Nachdem der IoT Inspector seinen Durchlauf beendet hat, gibt er einen umfangreichen Report aus, der die Testmethode beschreibt und alle gefundenen Schwachstellen auflistet. Diesen Report haben wir den Herstellern der WLAN-Router mit der Bitte um Stellungnahme vorgelegt, denn zu diesen Schwachstellen gibt es aktuell keine Patches. Wir räumten den Firmen 30 Tage Zeit ein, um zumindest auf die als „hoch“ und „mittel“ klassifizierten Risiken zu reagieren. Je nach Router hat der IoT Inspector sieben bis 22 dieser schwereren Probleme entdeckt. Da unsere Anfrage zudem mitten in die Ferienzeit fiel, verlängerten wir die Frist bei Bedarf um bis zu drei Wochen.

Umfangreiche Firmware-Analyse

Der Vorteil der automatischen Firmware-Analyse ist, dass man für den Test an die Hardware eigentlich gar nicht ran muss. Es reicht eine Firmware-Datei, die viele Hersteller ohnehin bereitstellen. Manchmal müssen die Experten aber im ersten Schritt die vorhandene Firmware noch aus dem WLAN-Router extrahieren.

Das können sie auf verschiedenen Wegen bewerkstelligen. Eine gängige Methode ist, den Update-Prozess zu überwachen und dabei die Firmware-Datei abzugreifen. Manchmal ist das knifflig, etwa bei den verschlüsselten Images von D-Link. Hier hat IoT Inspector eine eigene Methode entwickelt, um an die nötigen Schlüssel zu gelangen. Liegt das Firmware-Image vor, landet es auf der Cloud-Plattform von **iot-inspector.com**. Dort wird das Image in einem ersten Schritt entpackt.

Danach startet der IoT Inspector die automatische Analyse mit der Firmware-Komposition: Er klassifiziert die einzelnen Teile der Software, welches Dateisystem es gibt, welche Dateitypen, Skripte, Binaries oder Zertifikate vorliegen. Auf diese Bestandteile wendet er verschiedene Tests an. Er überprüft neben dem Betriebssystem, welche Drittanbieter-Komponenten zum Einsatz kommen und ob die Firmware durch Standardpasswörter angreifbar ist. Er sucht nach undokumentierten Anmeldeinformationen, denn die werden häufig von Botnetzwerken ausgenutzt. Er fahndet

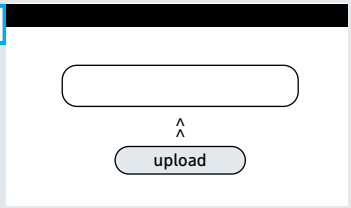
	Asus ROG Rapture GT-AX11000	AVM FritzBox 7530 AX	AVM FritzBox 7590 AX	D-Link DIR-X5460	Edimax BR-6473AX	Linksys Velop MR9600	Netgear Nighthawk AX12	Synology RT-2600ac	TP-Link Archer AX6000
Hersteller	Asus	AVM	AVM	D-Link	Edimax	Linksys	Netgear	Synology	TP-Link
Firmware-Version	3.0.0.4.386. 44266	7.27	7.27	1.10B10	1.0.19	1.0.4.205530	1.0.4.120	SRM 1.2.5	V1-210223
Sicherheitslücken gesamt	25	20	18	26	25	21	29	30	32
hohes Risiko	6	3	2	7	7	10	8	10	11
mittleres Risiko	9	6	5	6	9	9	8	9	11
geringes Risiko	1	1	1	2	1	1	3	3	1
Risiko durch auslesbare Informationen	9	10	10	11	8	1	10	8	9
Hersteller hat reagiert	●	○	○	●	●	●	●	●	●

FOTO: HERSTELLER

● ja ○ nein

So läuft der automatisierte Router-Test ab

1

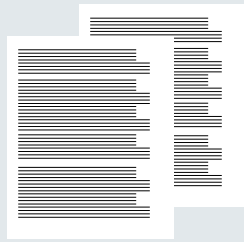


Upload: Der Dienst arbeitet Cloud-basiert. Über eine Webseite laden Sie die Router-Firmware hoch. Archive, Dateisysteme und komprimierte Daten werden automatisch entpackt

2

Analyse: Die Suche nach Schwachstellen unterteilt sich in die statische und die dynamische Prüfung, bei der nach Standard-Passwörtern, bekannten Lücken und Backdoors gesucht wird

3



Report: IoT Inspector erzeugt einen ausführlichen Report mit Details zur untersuchten Firmware und den aufgefundenen Lücken. Für einen Router umfasst er rund 300 Seiten

nach anfälligen Service-Konfigurationen und macht einen Abgleich mit den Einträgen in der öffentlich zugänglichen CVE-Datenbank.

Die CVE unterscheidet verschiedene Risikostufen: „hoch“, „mittel“, „niedrig“ und „Information“. Letztere stellt an sich keine Lücke dar, doch die Informationssammlung können Angreifer durchaus zur Vorbereitung von weiteren Attacken verwenden. Rund 15 bis 30 Minuten dauert ein Durchlauf. Damit die künftigen Tests schneller gehen, kann der IoT Inspector für bereits analysierte Firmware-Versionen ein Monitoring aktivieren. Neu entdeckte Sicherheitslücken präsentiert er dann als kleine Update-Häppchen.

Neun WLAN-Router im Test

Wir haben neun WLAN-Router aus der CHIP-Bestenliste über IoT Inspector analysiert. Das Ergebnis des Tests sehen Sie in der Tabelle auf Seite 63. Wichtig dabei: Nicht jedes gefundene Problem stellt eine echte Sicherheitslücke dar, denn durch die Analyse allein wird nicht geklärt, ob und wie Angreifer die Lücke auch ausnutzen können. Gefunden haben wir in allen WLAN-Routern Schwachstellen. Geht man allein nach der Anzahl, schneiden AVMs Fritzboxen mit 18 bzw. 20 potenziellen Risiken am besten ab, Synology und TP-Link kommen auf 30 bzw. 32 Risiken.

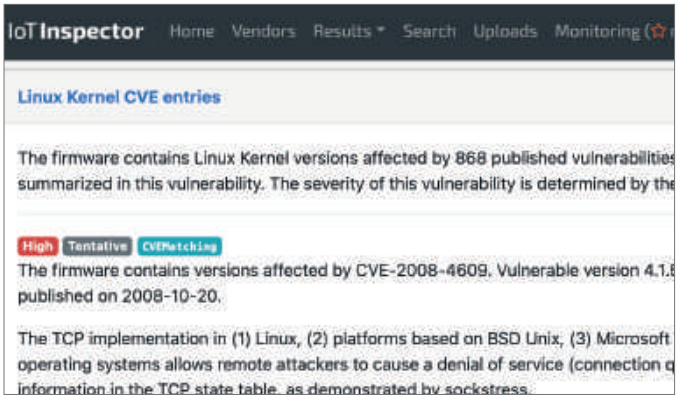
Bei der Einstufung der Risiken machen sich die Fritzboxen mit nur zwei bzw. drei als hoch eingeschätzten Problemen am besten, bis zu elf sind es bei der Konkurrenz. Alle Sicherheitslücken können wir nicht auflisten, aber es gibt eine Reihe von typischen Problemen.

Veraltete Kernel: Der Linux-Kernel kann viel und wird ständig weiterentwickelt, aber auch auf Schwachstellen abgesucht. Dementsprechend viele Sicherheitslücken entdeckt der IoT Inspector, wenn Hersteller auf veraltete Kernel-Versionen setzen. Da die Integration eines neuen Kernels in die Firmware aufwändig ist, ist kein Hersteller hier auf dem neuesten Stand.

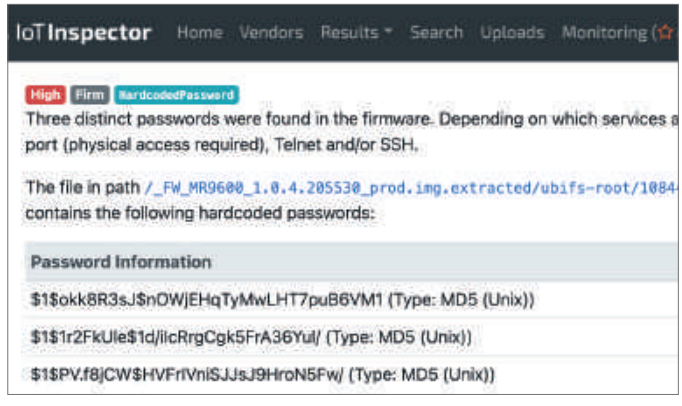
Veraltete Software: Gleiches wie für den Kernel gilt auch für die eingebaute Software. Zum Beispiel gibt es Standard-Tools wie BusyBox, die sich auf so gut wie jedem Linux-Router finden. Sie bündeln wichtige Funktionen und sind nur schwer wegzudenken. Wenn diese Software veraltet ist, bietet auch sie eine Angriffsfläche.

Anfällige Dienste: WLAN-Router stellen zahlreiche Dienste bereit. Neben dem Routing selbst sind das Multimedia-Funktionen, VPNs und mehr. Die dafür verwendete Software muss aktuell sein und sollte keine Fehlkonfigurationen aufweisen.

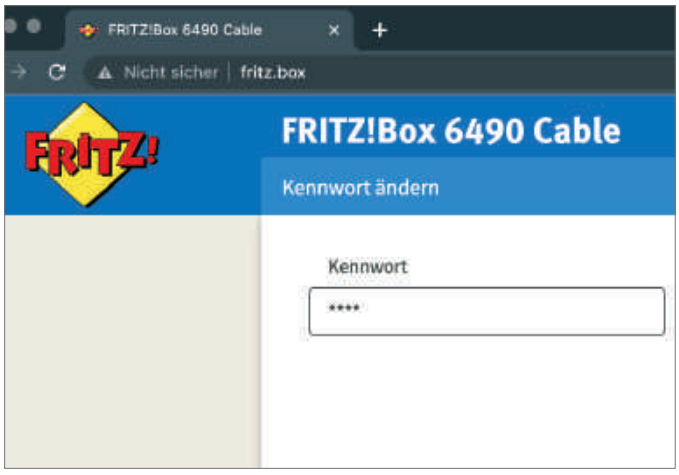
Unsichere Kommunikation: Bei der WLAN-Verschlüsselung leisten die Router-Hersteller gute Arbeit, aber das ist nicht die einzige Kommunikation, die ein Router anbietet. Oft hat er Schnittstellen, die besser abgesichert sein könnten, oder



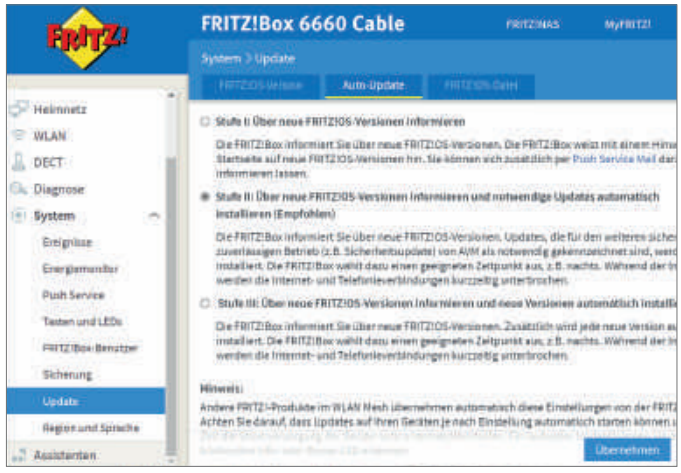
Veraltete Linux-Kernel
Die Integration eines neuen Kernels in die Router-Firmware ist aufwändig, deshalb stecken überall veraltete Versionen drin



Passwort admin
Schwache, fest vergebene Passwörter wie „admin“, die sich auch noch im Klartext auslesen lassen, untergraben die Sicherheit



Tipp 1: Standard-Passwörter ändern
Standard-Passwörter, etwa für den Zugriff auf die Admin-Oberfläche oder für das WLAN sollten Sie auf jeden Fall ändern



Tipp 2: Automatische Updates einschalten
Eine Update-Automatik ist komfortabel, um den WLAN-Router auf dem aktuellen Stand zu halten. Unbedingt einschalten!

er nutzt unsichere Protokolle wie Telnet, die noch nicht vollständig durch sichere Alternativen wie SSH abgelöst sind.

Unsichere Zertifikate: Sicherheitszertifikate sorgen für eine vertrauenswürdige Kommunikation. Aber wenn sich die Zertifikate einfach auslesen oder gar fälschen lassen, schwächen sie die Vertraulichkeit.

Feste Passwörter: Passwörter dienen der Sicherheit und ein Passwort ist besser als kein Passwort. Doch auf manchen Routern finden sich voreingestellte Passwörter im Klartext. Das ist ein klares No-Go.

So reagieren die Hersteller

Die meisten Hersteller haben unsere Kritik sportlich aufgenommen und sich schnell mit der Analyse befasst. Zumindest einen Teil der gemeldeten Probleme haben sie mittlerweile über Firmware-Updates behoben. AVM hat sich zwar auch gemeldet, war aber nicht besonders glücklich über die Vorgehensweise. Es kommt wohl öfter vor, dass Fritzboxen mit automatischen Firmware-Checks analysiert werden und die Ergebnisse mit angeblichen Sicherheitslücken beschäftigen die Mitarbeiter von AVM recht lange.

Aktuell ist der Stand so, dass AVM von automatisierten Tests nicht viel hält, weil sie viele Fehlalarme produzieren können. Auf gezielte Nachfragen zum veralteten Linux-Kernel ließ AVM verlauten, dass „nicht das Alter des Kernels zählt, sondern, ob er Schwachstellen enthält, die für die Anwendung innerhalb des Routers Relevanz haben“. Die restlichen Hersteller schickten uns konkretes Feedback:

Asus: Asus hat jeden einzelnen Punkt der Analyse untersucht und uns eine ausführliche Antwort präsentiert. Die veraltete BusyBox-Version hat Asus gepatcht, ebenso gibt es Updates für „curl“ und den Webserver. Bei den angemahnten Passwort-Problemen handelte es sich um Temp-Dateien, die der Prozess beim Beenden entfernt. Sie stellen kein Risiko dar.

D-Link: Kurz und knackig bedankte sich D-Link für die Hinweise und veröffentlichte ein Firmware-Update, das die angesprochenen Probleme fixt.

Edimax: Allzu viel Zeit scheint man bei Edimax nicht in die Überprüfung der Probleme gesteckt zu haben, trotzdem gab es am Ende ein Firmware-Update, mit dem ein Teil der Lücken behoben wurden.

FOTO: WEINWURM GMBH

„Unser Schnelltest zeigt, wie genau es IoT-Hersteller mit der Sicherheit nehmen.“

Florian Lukavsky
CTO, IoT Inspector

Linksys: Linksys hat zu allen als „hoch“ bzw. „mittel“ klassifizierten Problemen Stellung bezogen. Default-Passwörter will man künftig vermeiden, für die restlichen Probleme gibt es ein Firmware-Update.

Netgear: Bei Netgear war man fleißig und hat alle Probleme unter die Lupe genommen. Einige der als „hoch“ eingestuften Sachverhalte sieht Netgear als weniger problematisch an. Updates gibt es für DNSmasq und iPerf, weitere gemeldete Probleme will man zunächst beobachten.

Synology: Synology geht die von uns genannten Probleme mit einem großen Update für den Linux-Kernel an. BusyBox und PHP erhalten ein Update auf neue Versionen und bei den Zertifikaten will Synology demnächst aufräumen. Davon profitieren übrigens nicht nur die Router, sondern auch andere Synology-Geräte.

TP-Link: Durch Updates von BusyBox, CURL und DNSmasq schafft TP-Link viele Probleme aus dem Weg. Einen neuen Kernel gibt es nicht, aber geplant sind über 50 Fixes für das Betriebssystem.

Sicherheitstipps für Ihren Router

Durch unsere Aktion haben die Hersteller schon eine Menge Sicherheitslücken geschlossen. Doch viele WLAN-Router sind weiterhin nicht fehlerlos. Daher hält Florian Lukavsky, CTO von IoT Inspector, ein paar Maßnahmen für dringend geboten: Standard-Passwörter unbedingt ändern, Auto-Updates für die Firmware einschalten und die stärkste Verschlüsselung für das Funknetz wählen. Klemmt man dann noch unnötige Router-Funktionen ab, ist man schon einmal grundlegend gegen Angriffe geschützt. redaktion@chip.de