Für alle, die sich für eine kleine

externe Firewall

für zuhause

interessiern

Andreas Horn
Ingenieur für Industrielle Elektronik (FS)

Heilbad Heiligenstadt, 31. Oktober 2023

Inhaltsverzeichnis

1 Einleitung

Diese Serie richtet sich an Nutzer kleiner Netzwerke, z.B. zuhause. Es tauchen ja immer wieder Argumente auf wie: **Ich habe doch nichts zu verbergen** oder **An mir haben die doch sowieso kein Interesse**. Das stimmt aber nicht! Siehe hierzu auch:

„Befallen vom Überwachungsvirus“ - Deutschlandfunk, 04.01.2015
„Überwachungsstaat“ - Youtube Video, 28.07.2013
„Du bist Terrorist“0 - Youtube Video, 18.05.2009

Zuallererst muss man fragen, wer sind denn **„die“**?

- Interesse haben z.B. alle, die etwas verkaufen wollen - Werbung müllt das Postfach zu und wichtige Post wird dabei nicht oder nicht rechtzeitig entdeckt. Das kann durchaus unangenehme Konsequenzen haben.
- Verbrecher haben auch ein Interesse daran, fremde Rechner zu kapern. Bankverbindungen und Passwörter zu erbeuten, in fremdem Namen einzukaufen, den Rechner als Spamversender oder als Kryptominer zu missbrauchen. Das sind nur einige Möglichkeiten.
- Geheimdienste haben u.U. auch ein Interesse daran, fremde Rechner zu übernehmen. Das muss nicht nur zur Überwachung sein, es kann auch dazu dienen, falsche Fährten zu legen oder mir etwas unterzuschieben.

Außerdem ist interessant nachzuvollziehen, welches Gerät sich wie im Internet bewegt und z.B. nach Hause telefoniert. Mein Fernseher macht das nämlich ab und an ... Und dümmer wird man durch diese Kenntnisse keinesfalls.

2 Desktop Firewall

Sehr häufig werden Desktop Firewalls angepriesen, die auch Personal Firewall genannt werden. Von so etwas halte ich gar nichts! Sie laufen auf demselben Betriebssystem wie die Anwendungen, und ist das Betriebssystem angegriffen, können von dort aus alle Abwehrmechanismen der Desktop-Firewall ausgehebelt werden - und dazu können auch noch die Angriffe verborgen werden, ich kriege also von einer Kompromittierung unter Umständen nur dann etwas mit, wenn ich von einem sauberen System (DVD, Stick) boote. Mit UEFI-Boards ist die Situation noch schlimmer geworden.

3 Router als Firewall

Seit geraumer Zeit wurde wieder von Angriffen auf Router berichtet. Nutzt man nur dessen (rudimentäre) Firewall-Funktionen, ist nach einem gelungenen Angriff darauf das gesamte Netzwerk dahinter „offen wie ein Scheunentor“. Ob ein Router durch ein Firmwareupdate wirklich wieder sauber ist, kann nicht immer garantiert werden. Es kommt darauf an, ob beim Aufspielen einer neuen Software wirklich alles überschrieben wird. Außerdem sind auch bei nicht gehacktem Router genügend Möglichkeiten vorhanden, z.B. NAT zu überwinden. Ein vollständiges logging machen solche Router in der Regel auch nicht.

4 Hardware-Firewall

Die Harware-Firewall wird auch externe oder Netzwerk-Firewall genannt. Sie ist vom Rechner unabhängige Hardware und wird zwischen das interne Netzwerk und den Router (externes Netzwerk) gehängt. Es läuft nur das darauf, was für die Funktion des Netzwerks unbedingt nötig ist - es gibt also auch keine zusätzliche Software darauf, die ihre Sicherheitslücken mitbringt. Wer meint, dass die externe Firewall auch als Netzwerkspeicher (NAS) verwenden zu können, kann das durchaus tun, mir wäre das aber zu unsicher, zumal dann sicherlich nicht nur der Firewall-Admin auf die externen Firewall Zugriff haben dürfte.

Ich habe einen „Raspberry Pi 2 Modell B“testweise versucht als Firewall einzusetzen, da das eine extrem günstige Variante gewesen wäre. Zweiter Netzwerkport war ein USB-Netzwerkadapter. Als Software hatte ich ipfire verwendet. Der RasPi in der verwendeten Version ist aber mit der Außenanbindung des Netzwerks völlig überfordert, das Surfen macht dann keinen Spaß mehr... Andere Einplatinenrechner habe ich nicht getestet. Andere Firewall-Software mit in der Regel größerem Ressourcenverbrauch ist damit auch nicht sinnvoll.

Nach reichlichem Einlesen auf diversen Internetseiten habe ich mich dann entschlossen, ein Board von PC Engines anzuschaffen. Die Wahl fiel auf die APU2C4. PC Engines verkauft nicht an Privatpersonen und verweist z.B. auf

Varia Store und APU-board (= NRG-Systems)

Was wird benötigt (die Links sind Beispiele, durch googlen findet man auch weitere):

- APU2C4 board
- mSATA SSD mindestens 16 GB
- eines dieser Gehäuse (mit 2 bzw. in einem Fall 6 Durchbrüchen für Antennen)
- Netzteil
- Nullmodemkabel
- Seriell-USB-Adapter
- Schablone (optional)

Am Besten kauft man sich ein Bundle mit SSD und ergänzt es mit dem erforderlichen Zubehör (Nullmodemkabel, Seriell-USB-Adapter, Schablone). Die SSD-Größe ist im Bundle wählbar und sollte mindestens 16 GB haben.

Die Montage erfolgt wie bei PC Engines gezeigt, das Blech dient in Verbindung mit dem Gehäuse als Kühlkörper.

Falls die optionale Schablone im Gerät verbleiben soll, müssen beide aufgelöteten Gewinde abgetrennt werden.

Ich habe versucht, die APU2C4 mit 2 Antennen als AP zu betreiben, das ging nicht lange, dann war der Compex WLE600VX kaputt. Außerdem muss man sich bei nur einem Modul entscheiden, ob man 2.4 oder 5 GHz verwenden will, beides gleichzeitig geht nur mit 2 Modulen. Hier wäre dann das Gehäuse mit 6 Durchbrüchen für Antennen angebracht. Auch ein Bundle mit APU4B4 und externem AP ist möglich.

5 Firewall Software

Die Sophos XG Firewall Home Edition ist eine tolle Firewall mit vielen Features, die man sonst so nicht findet. Leider ist eine APU2C4 zu schwach, um damit eine vernünftige Performance zu erhalten.

Ich entschied mich also für die mir bereits bekannte IpFire. Sie läuft bei mir auf einer APU2C4 jetzt bereits mehrere Jahre. In IpFire kann die Oberfläche (genauso wie bei der Sophos XG Firewall Home Edition) auf deutsch umgestellt werden. Sie hat eine sehr hilfsbereite deutsche CommunityCommunity und deutsche Anleitungen sind im Internet ebenfalls gut zu finden. Wer nicht selber installieren will, kann z.B. hier fertig mit ipfire konfigurierte Geräte kaufen.

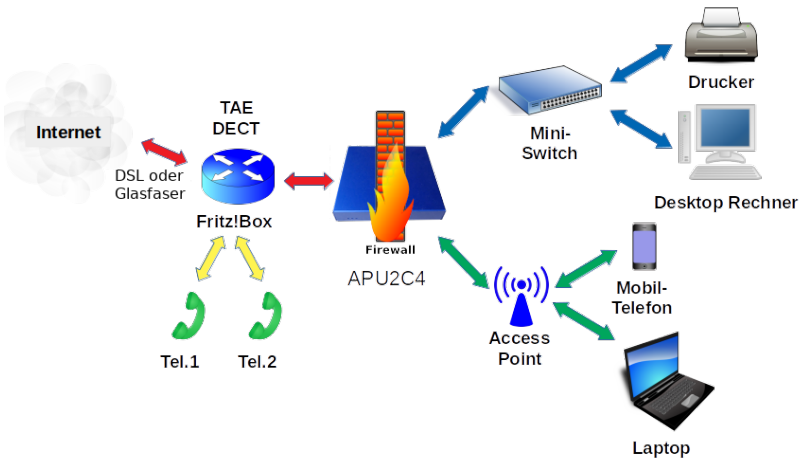
Hilfreich ist auch das script *dns_blocklist.sh*, das die (Basis-)Funktionalität von Pi-Hole nachbildet. Hierbei wird das DNS verbogen,damit „besondere“Seiten ausgeblendet werden. Schön ist, dass die dabei ausgeblendeten Webseiten durch eine aktive Community ständig aktualisiert werden und das script pflegt die Aktualisierung automatisch ein. Testen kann man die Wirkung hier.

Sehr hilfreich für mich waren die Anleitungen von Mike Kuketz zu IpFire. Herzlichen Dank!

6 WLAN

Wie bereits oben berichtet, hat leider der WLAN-Modul nach kurzer Zeit seinen Geist aufgegeben, vermutlich thermischer Tod wegen dem lüfterlosen Gehäuse. Ich habe deshalb einen externen AP an den 3. Port der APU angehängt. Da ich eine **D**e**M**ilitarisierte**Z**one nicht brauche, ist das bei mir nicht weiter schlimm. Im Bedarfsfall gibt es ja noch die APU4B4 mit 4 x 1 GB Ports, damit kann ein externer AP und eine DMZ angeschlossen werden.

7 Gesamtbild



8 Konfiguration

Die Konfiguration der einzelnen Komponenten sollta man keinesfalls auf den Standardvorgaben belassen. Es wäre die klassische Möglichkeit zum Angriff, wenn grundlegende Einstellungen (IP-Bereich, Passwörter, ...) dem Angreifer schon bekannt sind. Deshalb sollte z.B. der IPv4-Adressebereich und die Netzmaske der Fritz!Box geändert werden. Der verwendete IP-Bereich sollte dann auch nicht bei x.x.x.1 beginnen (IPv4-Adressrechner vom Heiseverlag), damit ist schon mal eine größere Anzahl von Versuchen nötig und viele scripte stranden. Wer sich dann aber diese Konfigurationsänderung per push mail unverschlüsselt zusenden lässt, sollte sich fragen, ob er diesen Aufwand überhaupt machen will...

9 Logging

Die Auswertung händisch vorzunehmen ist ein mühsames Geschäft. Eine Tabellenkalkulation (LibreOffice Calc) ist da sehr hilfreich. Aber es ist schon erstaunlich, was man da so alles findet! Leider ist das über das Webfrontend verfügbare neueste Logfile immer nur vom Vortag. Aktueller geht es wohl nur per ssh direkt von der Firewall.

Allerdings verlangt die Auswertung der Logfiles eine gewisse Regelmäßigkeit.