Wie kann ein kleines mittelständisches Unternehmen mithilfe eines Raspberry Pi alle mit dem Unternehmensnetzwerk verbunden Netzwerkgeräte monitoren?

Felix Guderley
INF-6
Matrikelnr: 84636

***Zusammenfassung*—Heutzutage empfiehlt es sich das Unternehmensnetzwerk zu monitoren. In diesem Paper wird vorallem für die Unternehmen eine Lösung beschrieben, die sich keine teueren Schutzmaßnahmen einkaufen können oder wollen. Deshalb wird dieses Projekt mit einem Budget von 40 Euro, die für die Anschaffung eines Raspberry Pi notwendig sind, umgesetzt. Auf der Hardware wird die kostenfrei nutzbare Software ARPwatch installiert, die Änderungen am Netzwerk anhand des ARP-Protokolls erkennt. Der Netzwerkverantwortliche wird per E-Mail informiert. In den Teststellungen hat sich gezeigt, dass ARPwatch die vom Hersteller angepriesenen Leistungen auch auf einem Raspberry Pi vollständig zur Verfügung stellt. Es werden sowohl neue Netzwerkgeräte als auch Änderungen an bekannten Geräten zuverlässig erkannt und der Verantwortliche informiert.**

***Index Terms*—nmap, arpON, XARP, ARPwatch, Raspberry Pi**

I. Einleitung

Heutzutage ist das Computersystem für jedes Unternehmen ein wichtiger Bestandteil. Dazu gehört auch die Sicherheit der Daten auf den Computern und der Daten, die im internen Netzwerk gesendet werden. Um dieses Ziel zu erreichen ist es notwendig Änderungen, die das Netzwerk betreffen, zu erkennen und bei Bedarf die verantwortliche Stelle im Unternehmen zu informieren. Im folgenden soll auf die Art des Monitoring eingegangen werden, die sowohl bei neu verbundenen Geräten im Netzwerk, als auch bei untypischen Änderungen der bereits verbundenen Geräte eine automatische Warnung erzeugt.

Im speziellen wird der Fokus auf kleine, mittelständische Unternehmen gelegt, die meist keine große IT-Abteilung und kein Geld für teure Netzwerküberwachungstools besitzen. Für diese Unternehmen wird in den folgenden Kapiteln eine Lösung beschrieben, die das Unternehmensnetzwerk auf neue Netzwerkgeräte scannt und falls ein unbekanntes Gerät erkannt wurde, den Netzwerkverantwortlichen im Unternehmen informiert. Das selbe soll geschehen, wenn sich eine IP- und MAC-Adressen Kombination ändert. Dabei sollen sowohl die Anschaffungskosten sowie der Unterhaltungskosten möglichst gering gehalten werden. Bei allen eingesetzten Softwarelösungen wird sich an der verbreitetsten Nutzung der Produkte orientiert, um möglichst wenig Wartungsaufwand bei Aktualisierungen zu haben. Die Analyse des Netzwerks soll von einem Endgerät durchgeführt werden. Damit kein Arbeitsplatzcomputer für dieses Projekt zweckentfremdet wird, soll die zugrunde liegende Hardware ein Raspberry Pi sein.

II. Netzwerk Scanning Tools

Als Grundlage für das Monitoring wird ein Raspberry Pi 3 B+ verwendet. Dieses besitzt genügend Leistung, um ein Standard Linux Betriebssystem auszuführen. Zur Hardware muss ein passendes Tool ausgewählt werden, welches die Analyse des Netzwerks bewerkstelligen kann. Die Voraussetzungen für dieses Tool sind zum einen, dass es sich um eine kostenfreie Software handelt und zum anderen, dass die Software auf einem Linux Betriebssystem installiert werden kann. Eine Auswahl der gängigsten Tools wird im Folgenden kurz vorgestellt.

A. Nmap

Das kostenfreie Tool nmap wird in der Netzwerktechnik häufig für Netzwerkscans verwendet. Eine Funktionalität ist die Host-Erkennung. Dabei wird

mit verschiedenen Protokollen im Netzwerk nach aktuell verbundenen Geräten gesucht. Zu jedem gefundenen Gerät werden zusätzlich zur IP-Adresse weitere Informationen wie MAC-Adresse, Betriebssystem und offene Ports erkannt. Es kann auf allen gängigen Betriebssystemen installiert und ausgeführt werden. Ein Vorteil von nmap ist, dass es sehr schnell große Netzwerksegmente analysieren kann.[1][2][3]

Nmap bietet für diesen Anwendungsfall mehr Auswertungsmöglichkeiten als notwendig. Beispielsweise ist das Erkennen des Betriebssystems und der offenen Ports für die Detektion eines neu verbundenen Netzwerkgeräts nicht notwendig. Für die weitere Analyse eines neu verbundenen, unbekannten Geräts können die durch nmap gewonnenen Informationen sehr hilfreich sein. Informationen über das Betriebssystem können zum Beispiel einen Anhaltspunkt geben, ob es sich um ein Gerät handelt, dass typischerweise in dem Unternehmen eingesetzt wird und somit die Verbindung mit dem Firmennetzwerk legitim ist.

Ein erheblicher Nachteil für den geforderten Use-Case ist, dass nmap rein für die Analyse gedacht ist und keine Funktion zur Datenspeicherung bietet. Für den Anwendungsfall muss dementsprechend zusätzlich zu diesem Tool eine eigenständige Datenbank und ein Agent, der nmap ausführt und das Ergebnis interpretiert, installiert bzw. programmiert werden. Dadurch entstehen mehrere Abhängigkeiten, die beispielsweise bei Softwareupdates berücksichtigt werden müssen.

B. ARPwatch

ARPwatch ist eine Open-Source-Software, die vor allem für die Überwachung des Ethernet-Netzwerks verwendet wird. Die Funktionsweise des Tools basiert auf dem *Address Resolution Protocol* kurz ARP. Die Funktionsweise von ARP ist wie folgt: Sobald ein Gerät mit einem anderen kommunizieren möchte, sendet dieses eine ARP-Anfrage an alle Geräte im Netzwerk. Diese Anfrage beinhaltet unter anderem die IP-Adresse des Zielgerätes. Alle Geräte vergleichen daraufhin die eigene mit der angefragten IP-Adresse und antworten nur wenn sie das entsprechende Zielgerät sind.[4] Die ARP-Anfragen von verbundenen Netzwerkgeräten werden von ARPwatch genutzt, um die Netzwerkadressen des Gerätes mitzubekommen. Die durch dieses Verfahren erhaltenen Daten werden mit der Datenbank, in der die bekannten Geräten enthalten sind, abgeglichen. Zu jedem neu entdeckten Gerät wird in der integrierten Datenbank die MAC-Adresse, die dazugehörige IP-Adresse im Netzwerk, der Gerätename und der aktuelle Zeitstempel gespeichert. Während der Laufzeit wird so eine Datenbank mit allen bekannten Geräten erstellt. Der Administrator wird informiert, sobald sich eine bekannte IP- und MAC-Adressen-Kombination ändert oder neu zur Datenbank hinzugefügt wird. Das Tool kann den Administrator beispielsweise per E-Mail über Auffälligkeiten und neue Geräte benachrichtigen. Für den E-Mail-Versand muss zusätzlich ein SMTP-Dienst auf dem System installiert sein.[5][6]

Ein Vorteil von ARPwatch ist, dass die Datenbank, die Analyse-Logik und die Benachrichtigung in der Anwendung integriert sind und nicht separat installiert werden müssen. Es wird für den E-Mail-Versand lediglich ein SMTP-Dienst auf dem Betriebssystem vorausgesetzt. Ein weiterer Vorteil von ARPwatch ist, dass zum Analysieren keine Anfragen in das Netzwerk gesendet werden müssen, da lediglich bei ARP-Anfragen zugehört wird.

C. XARP

XARP analysiert den ARP-Cache des Computers. Dabei werden alle aktuellen ARP-Einträge mit den in der Datenbank bekannten IP- und MAC-Adressen-Kombinationen abgeglichen. Noch unbekannte IP-MAC-Adressen werden automatisch in einer integrierten Datenbank gespeichert. Wenn sich eine Kombination aus IP- und MAC-Adresse ändert, wird je nach Version der Anwender an seinem Computer oder der Administrator per E-Mail gewarnt. Mit diesem Tool muss jedes Endsystem separat ausgestattet werden, da im ARP-Cache jeweils nur die Geräte enthalten sind, mit denen das Gerät kommuniziert.[7][8] Eine Alarmierung per E-Mail ist nur in der Pro-Version des Tools möglich, diese ist kostenpflichtig und beginnt bei einem Preis ab 13,69 Euro pro Endsystem.[9]

Das Projekt soll das gesamte Netzwerk von nur einem Endgerät aus überwachen. Um dies auch mit XARP umsetzen zu können, muss zusätzlich ein Agent erstellt werden, der zyklisch versucht eine Verbindung mit allen Geräten im Netzwerk aufzunehmen. Dabei sind einfache Anfragen von allen IP-Adressen im aktuellen Subnetz ausreichend, weil beim Verbindungsaufbau mit einem anderen Gerät das ARP-Protokoll ausgeführt wird und dadurch der ARP-Cache des Endsystems aktualisiert wird. Diese Lösung erhöht jedoch den Netzwerk-Datenverkehr und benötigt ein weiteres Tool beispielsweise nmap, das dafür ausgelegt ist möglichst schnell

und effizient Anfragen, an alle möglichen IP-Adressen im Subnetz, senden zu können (siehe Kapitel II-A). Ein weiterer Nachteil des Tools ist, dass es nur in der Pro-Version E-Mail-Benachrichtigungen senden kann. Die Verwendung der kostenfreien Version ist daher nicht ausreichend, weil keine andere Form der Benachrichtigung an eine zentrale Stelle angeboten wird.

D. arpON

ArpOn ist ein vollständig kostenfreies Tool zum Überwachen des ARP-Cache des Computers. Ähnlich wie XARP muss arpON auf jedem Endgerät installiert sein und greift dort auf den ARP-Cache des Computers zu. Als zusätzliche Funktionalität kann arpON die Verbindung sofort abbrechen, falls ein ARP-Spoofing Angriff vermutet wird. Es besteht jedoch keine Möglichkeit eine E-Mail-Benachrichtigung zu versenden. Dabei ist zu beachten, dass arpON nur für Linux-Systeme entwickelt wurde.[8][10] Die meisten Unternehmen, vor allem im Mittelstand, verwenden als Betriebssystem Microsoft Windows.[11] Dementsprechend ist eine Installation auf jedem Endgerät nicht möglich.

Für diese Anwendung kann, wie bei XARP (siehe Kapitel II-C) beschrieben, ein Agent genutzt werden. Dieser versucht zyklisch einen Verbindungsaufbau mit allen Geräten um so den ARP-Cache des Endsystems zu aktualisieren. Problematisch ist jedoch, dass ArpON auf die Erkennung von ARP-Angriffen ausgelegt ist und keinerlei E-Mail-Benachrichtigung zur Verfügung stellt.

III. Konzeptionierung des Netzwerk-Monitoring Tools

Das Projekt wird, wie in den vergangen Kapiteln erwähnt, mit einem Raspberry Pi 3 B+ umgesetzt und ist für knapp 40 Euro erhältlich.[12] Das Raspberry Pi besitzt mit einer Gigabit-Ethernet-Schnittstelle, einem Gigabyte Arbeitsspeicher und einem Broadcom Cortex-A53 Prozessor alle nötigen Voraussetzungen zum Betreiben eines Linux Betriebssystems. Das Raspberry Pi zählt zu den Mini-Computern und kann mit lediglich 5 Volt und 2,5 Ampere betrieben werden.[13]

Ein wesentlicher Vorteil von Linux ist, dass es kostenfrei genutzt werden kann. Der Hersteller des Raspberry Pi empfiehlt die Verwendung des Raspberry-Pi-Betriebssystem, dem sogenannten Raspbian, welches auf einer Debian Linux Distribution basiert und für die Verwendung auf dieser Hardware angepasst wurde.[14][15] Der Herstellerstandard soll, wie in der Einleitung beschrieben, nach Möglichkeit verwendet werden, dementsprechend wird als Betriebssystem Raspbian eingesetzt.

In der Vorstellung möglicher Anwendungen (siehe Kapitel II), ist nmap das einzige Tool, das auf Geräteerreichbarkeit und Port-Scanning auslegt ist. Da für die Verwendung jedoch noch weitere Tools installiert oder programmiert werden müssen, konnte nmap relativ einfach ausgeschlossen werden. ARPwatch und arpON sind jeweils kostenfreie Tools, wohingegen XARP für die Verwendung mit E-Mail-Versand eine Lizenz benötigt. Alle drei Tools analysieren die Veränderungen anhand des ARP-Protokolls. Bei XARP und arpON empfiehlt der Hersteller jeweils, dass diese auf jedem Endsystemen installiert werden und sind sind vorallem für den Schutz von ARP-Angriffen entwickelt. In diesem Projekt soll jedoch von einem Endgerät - dem Raspberry Pi - erkannt werden, wenn sich ein noch unbekanntes Gerät mit dem Netzwerk verbindet oder wenn sich zu einer bekannten IP-Adresse ein Gerät mit anderer MAC-Adresse meldet. ARPwatch hingegen hört beim ARP-Verkehr im Netzwerk zu und benötigt dementsprechend keinen Agenten, der Anfragen in das Netzwerk sendet. Aus den zuvor genannten Gründen soll für die Umsetzung des Projekts ARPwatch eingesetzt werden. Wie erwähnt, wird zu ARPwatch zusätzlich ein E-Mail-Dienst auf dem Betriebssystem benötigt. Ein leichtgewichtiger Mailing-Dienst ist sSMTP, der ausschließlich für das Versenden von E-Mails gedacht ist.[16][17] Nachdem lediglich E-Mails gesendet werden müssen, ist sSMTP für dieses Projekt sehr gut geeignet.

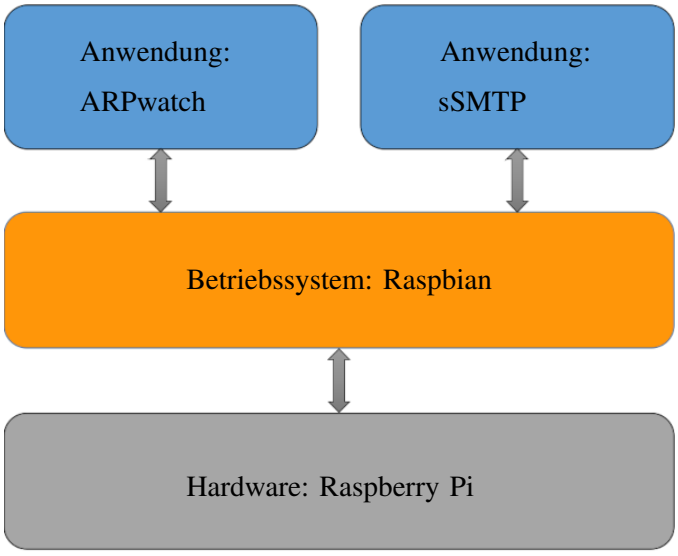

Abbildung 1: Hardware und Software Zielarchitektur.

In Abbildung 1 wird der Aufbau mit den ausgewählten

Tools grafisch dargestellt. Dabei ist die Hardware-Ebene in der Ansicht unten aufgetragen. Je weiter oben ein Tool angeordnet ist, desto Hardware unabhängiger ist dieses.

IV. Umsetzung

A. Installation Raspbian

Auf ein handelsübliches Raspberry Pi 3 B+ wurde mithilfe des NOOBS Betriebssystem-Installationsprogramm das Betriebssystem Raspbian aufgesetzt. Im Anschluss an die Installation muss auf neue Updates geprüft werden und falls welche vorhanden sind, müssen diese eingespielt werden.

Mit dem in Listing 1 beschriebenen Befehl werden die Update-Paketlisten neu eingelesen.[18]

```
$ sudo apt-get update
```

Listing 1: Update-Befehl um die Paketlisten vor dem Update neu einzulesen.

Auf Grundlage der aktualisierten Paketlisten werden, mit dem in Listing 2 beschriebenen Befehl, die Updates auf dem System installiert.[19]

```
$ sudo apt-get upgrade
```

Listing 2: Upgrade-Befehl um alle verfügbaren Updates zu installieren.

Nachdem das Betriebssystem auf dem aktuellen Stand ist, kann mit der Softwareinstallation und Konfiguration begonnen werden.

B. Installation von sSMTP

Wie in Kapitel III beschrieben, ist ARPwatch nicht in der Lage E-Mails ohne einen zusätzlichen, auf dem Betriebssystem installierten, Dienst zu versenden. Mit dem Befehl in Listing 3 wird sowohl der sSMTP-Dienst installiert, als auch das mailutils Paket, welches zum Verarbeiten von E-Mails benötigt wird.[20]

```
$ sudo apt install ssmtp mailutils
```

Listing 3: Befehl zum Installieren des sSMTP-E-Mail-Dienstes und des mailutils Paket.

In der Konfigurationsdatei */etc/ssmtp/ssmtp.conf* kann der E-Mail-Dienst konfiguriert werden.[21] Die angepasste Konfigurationsdatei ist in Listing 4 dargestellt. Die Variable *root* beinhaltet dabei die E-Mail-Adresse, über welche standardmäßig die E-Mails gesendet werden. Im *mailhub* sind die Webadresse und der Port des Mail-Providers hinterlegt. Als *hostname* wird der Gerätenamen des sendenden Geräts angegeben, standardmäßig wird *localhost* verwendet. Wenn eine Unterscheidung beispielsweise zwischen E-Mails von verschiedenen Geräten gewünscht ist, muss der Name entsprechend angepasst werden. *AuthUser* und *AuthPass* werden benötigt, damit sich das Tool am E-Mail-Server anmelden kann. Zuletzt wird definiert, dass eine verschlüsselte Verbindung zum E-Mail-Server aufgebaut werden soll.[22]

```
root=xxxx_pi@gmx.de
mailhub=mail.gmx.net:587
hostname=localhost
AuthUser=xxxx_pi@gmx.de
AuthPass=xxxxxxxxxxxx
UseSTARTTLS=YES
```

Listing 4: Konfigurations-Datei des sSMTP E-Mail-Dienstes.

Anschließend muss in der Datei */etc/ssmtp/revaliases* dem jeweiligen Betriebssystemnutzer eine Mailadresse zugeordnet werden. In diesem Projekt soll ARPwatch als *root*-Benutzer ausgeführt werden, dementsprechend wurde, wie in Listing 5 dargestellt, die E-Mail-Adresse mit den Serverinformationen bei dem Benutzer hinterlegt.

```
root:xxxx_pi@gmx.de:mail.gmx.net:587
```

Listing 5: Konfiguration der Aliasse in der ssmtp.conf.

Mit dem Befehl, der in Listing 6 abgebildet ist, soll eine Testmail vom Raspberry Pi an *meineMail@gmx.de* gesendet werden.

```
$ echo Raspberry-Pi Testmail | sudo
  ↪ mail -s "Teste␣ssmtp"
  ↪ meineMail@gmx.de
```

Listing 6: Befehl zum Senden einer Testmail über das Terminal.

Beim ersten Ausführen des Befehls, konnte jedoch keine Mail versendet werden, da dieser auf der Kommandozeile lediglich mit einem nichtssagenden Fehler beendet wurde. Die Meldung lautet: «*mail: Nachricht kann nicht gesendet werden: Prozess wurde mit einem von Null verschiedenen Status beendet*». Um den Fehler zu beheben wurde die Logdatei unter */var/log/mail.err* eingesehen.

```
pi@raspberrypi:~ $ tail /var/log/mail.err
Jun 18 10:40:10 raspberrypi sSMTP[1149]: 550 Sender address is not allowed.
Jun 18 10:40:26 raspberrypi sSMTP[1178]: 550 Sender address is not allowed.
Jun 18 10:42:09 raspberrypi sSMTP[1224]: 550 Sender address is not allowed.
```

Abbildung 2: Fehlermeldungen von sSMTP in der Logdatei.

Diese enthält, wie in Abbildung 2 dargestellt, weiterführende Informationen und Fehlercodes, die auf der Website des E-Mail-Providers nachgeschlagen

werden können. Aufgrund der Fehlerinformationen wurde die Konfigurationsdatei angepasst, damit nun in E-Mails keine Überschreibung des «*gesendet von*» Feldes mehr möglich ist (siehe Listing 7, letzte Zeile). Daraufhin funktioniert das versenden der Testmail ohne Probleme.

```
root=xxxx_pi@gmx.de
mailhub=mail.gmx.net:587
hostname=localhost
AuthUser=xxxx_pi@gmx.de
AuthPass=xxxxxxxxxxxx
UseSTARTTLS=YES
FromLineOverride=NO
```

Listing 7: Geänderte Konfigurations-Datei des sSMTP E-Mail-Dienstes.

C. Installation von ARPwatch

Nachdem sSMTP installiert ist, kann nun ARPwatch mit dem in Listing 8 beschriebenen Befehl installiert werden.

```
$ sudo apt-get install arpwatch
```

Listing 8: Befehl zum Installieren von ARPwatch.

Bevor ARPwatch verwendet werden kann, muss zwingend die Datei */var/lib/arpwatch/arp.dat* mit dem Befehl aus Listing 9 erstellt werden, da diese nicht automatisch bei der Installation erstellt wird. Falls ARPwatch nicht mit Root-Rechten ausgeführt wird, benötigt der entsprechende User auf die Datei Lese- und Schreibrechte.[23]

```
$ sudo touch /var/lib/arpwatch/arp.dat
```

Listing 9: Befehl zum Erstellen einer neuen leeren Datei.

In der Literatur finden sich Anleitungen, wie ARPwatch zu konfigurieren ist. Dabei soll unter anderem der E-Mail-Empfänger in einer Konfigurationsdatei unter */etc/arpwatch.conf* für jedes Netzwerkinterface separat hinterlegt werden können.[16] In einer weiteren Konfigurationsdatei besteht die Möglichkeit, den allgemeinen E-Mail-Empfänger für alle Netzwerkinterfaces zu hinterlegen. Zusätzlich kann die Absenderadresse eingestellt werden.[24] Mit den beschriebenen Konfigurationsdateien lässt sich ARPwatch auf dem Raspberry Pi zwar starten, jedoch scheitert der E-Mail-Versand.

Aus den Loginformationen in Abbildung 3 des sSMTP-Dienstes wird ersichtlich, dass ARPwatch versucht E-Mails unter einer anderen als der registrierten E-Mail-Adresse zu versenden. Der Anbieter des E-Mail-Dienstes verhindert das Senden der Nachrichten.[25] Durch verändern der Konfigurationsdateien und Versuchen ARPwatch mit einer bzw. keiner Konfigurationsdatei zu starten wurde ermittelt, dass ARPwatch beim Einlesen von Konfigurationsdateien unvorhersehbare Aktionen an der Absender E-Mail-Adresse vornimmt. Um dieses Problem zu lösen, ist auf die beiden zuvor beschriebenen Dateien zu verzichten. Anschließend ist es ausreichend, wenn ARPwatch beim Programmstart lediglich die Empfänger E-Mail-Adresse mitgegeben wird.

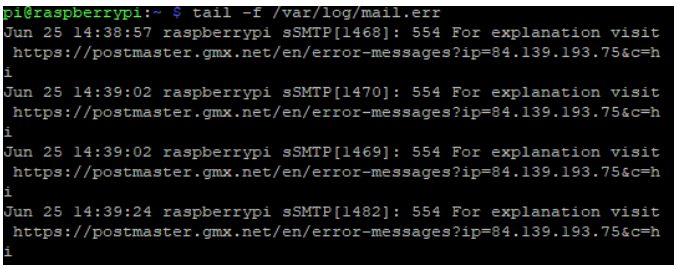

Abbildung 3: Fehlermeldungen in der sSMTP-Logdatei beim Senden von ARPwatch Benachrichtigungen.

Die einfachste Methode für den Programmaufruf ist in Listing 10 beschrieben. Damit wird ARPwatch gestartet und sendet ohne Probleme E-Mails an die angegebene E-Mail-Adresse.

```
$ sudo arpwatch -m email.
    ↪ nwadmin@meinunternehmen.de
```

Listing 10: Befehl zum Starten von ARPwatch.

Damit ARPwatch nach jedem Neustart des Betriebssystems erneut ausgeführt wird, muss der in Listing 10 beschriebene Befehl zum Autostart hinzugefügt werden. Dafür wird dieser in die Datei */etc/rc.local* geschrieben. Beim Starten wird dann diese Datei mit Root-Rechten ausgeführt, dadurch kann es zu keinen Zugriffsproblemen auf die in Listing 9 beschriebenen Dateien kommen.[26]

V. Tests und Ergebnisse

Das fertig installierte Raspberry Pi wird zuerst mit einfachen Testkonstellationen getestet. Dabei werden verschiedene Geräte sowohl über WLAN als auch über LAN mit dem Netzwerk verbunden. Verwendete Geräte waren unter anderem Desktop-Computer, Laptops, Smartphones, Tablets, SmartTV und Netzwerkdrucker mit Linux, Windows und herstellereigenen Betriebssystemen. ARPwatch hat die Geräte sofort erkennen können, sobald diese eine Netzwerkverbindung

aufgebaut haben. In Abbildung 4 ist der Inhalt einer E-Mail abgebildet, die bei Detektion eines neuen Netzwerkgerätes an die angegebene Ziel E-Mail-Adresse gesendet wird. Der Netzwerkadministrator erhält somit Informationen über den Gerätenamen, die MAC- und IP-Adresse des Endgerätes sowie Zeitstempel und falls bekannt, den Hersteller des Netzwerkinterfaces.

```
        hostname: [redacted]
      ip address: [redacted]
       interface: eth0
ethernet address: d6:7b:95:ef:8f:7f
 ethernet vendor: <unknown>
       timestamp: Saturday, June 27, 2020 10:28:50 +0200
```

Abbildung 4: Inhalt der Hinweis-E-Mail von ARPwatch, dass ein neues Gerät im Netzwerk erkannt wurde.

Um zu testen, ob ebenfalls MAC-Adressen-Änderungen erkannt werden, wird das kostenfreie Tool «MAC Address Changer» von NoVirusThanks verwendet. Dieses ermöglicht einem Windows 10 Rechner seine MAC-Adresse zu ändern.[27] Auch in diesem Fall funktioniert ARPwatch ohne Probleme, erkennt die neuen MAC-Adressen und warnt per E-Mail bezüglich der Änderung. In Abbildung 5 ist aufgeführt, wie der Inhalt einer E-Mail aussieht, wenn ARPwatch eine Änderung der MAC-Adresse erkennt. In dieser sind die geänderten Werte, wie MAC-Adresse und Zeitstempel, gegenübergestellt und das Delta zwischen den Zeitstempeln berechnet.

```
           hostname: [redacted]
         ip address: [redacted]
          interface: eth0
   ethernet address: ac:ed:5c:ae:e5:0c
    ethernet vendor: Intel Corporate
old ethernet address: d6:7b:95:ef:8f:7f
 old ethernet vendor: <unknown>
          timestamp: Saturday, June 27, 2020 10:30:05 +0200
 previous timestamp: Saturday, June 27, 2020 10:28:49 +0200
              delta: 1 minute
```

Abbildung 5: Inhalt der Warnhinweis-E-Mail von ARPwatch, dass ein bereits bekanntes Gerät seine MAC-Adresse geändert hat.

Zu beachten ist bei der Software jedoch, dass die Geräte nur erkannt werden, sobald eine ARP-Anfrage in das Netzwerk gesendet wird.[23] Dementsprechend werden bei der ersten Inbetriebnahme der Anwendung nicht alle, mit dem Netzwerk verbundenen, Geräte auf einmal gefunden. In mehreren Tests hat sich jedoch gezeigt, dass die meisten verbundenen Geräten nach etwa 12 Stunden gefunden wurden.

Zusätzlich zur Funktionalität wurde noch die Prozessorauslastung des Raspberry Pi im Betrieb ermittelt. Dafür wird das in Linux integrierte Tool vmstat verwendet, womit die Auslastung des gesamtem Betriebssystem ermittelt wird.[28] Über 24 Stunden hinweg wurde jeweils nach 60 Sekunden ein Mittelwert gespeichert. In Abbildung 6 wird ersichtlich, dass die Auslastung über den gemessen Zeitraum durchgehend sehr gering war. Die mittlere Prozessorauslastung beträgt $0,023\%$.

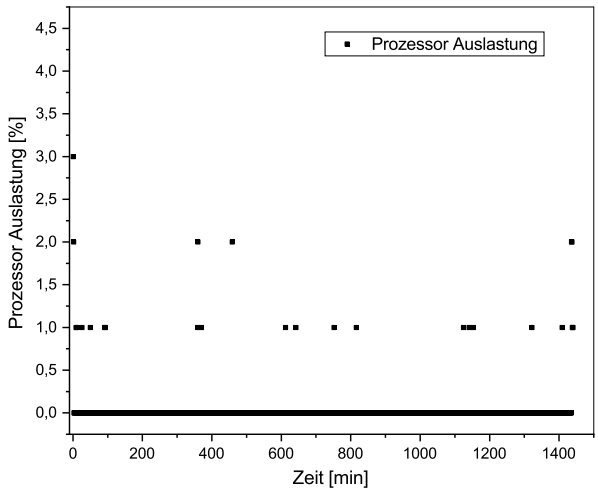

Abbildung 6: Auswertung der Prozessorauslastung des Raspberry Pi über 24 Stunden.

Als Testergebnis kann festgehalten werden, dass ARPwatch sehr zuverlässig funktioniert und wenig Rechenleistung benötigt. Dabei konnte das kostenfreie Tool relativ einfach auf einem Raspberry Pi installiert werden. Der Release Zyklus von ARPwatch ist nicht auf der Herstellerwebsite angegeben. Da zwischen den letzten beiden Vollversionen, Version 2 (Mitte 2006) und Version 3 (Ende 2019), knapp 13,5 Jahre lagen, kann von einem relativ langem Release Zyklus ausgegangen werden.[29] Das erfüllt den in der Einleitung geforderten niedrigen Wartungs- und Pflegeaufwand der Software. Durch ARPwatch hat jedes Unternehmen den Mehrwert, dass alle Netzwerkgeräte mit dem Unternehmensnetzwerk bekannt sind. Sofern das Gerät nicht von der administrativen Abteilung aufgebaut wurde, kann von einem unbefugten Einbruchsversuch ausgegangen werden und die entsprechenden Schutzmaßnahmen ergriffen werden.

VI. Ausblick

Das Raspberry Pi ist mit der aktuellen Konfiguration bei weitem nicht vollständig ausgelastet (siehe Kapitel V). Es können zukünftig weitere Anwendungsfälle abgebildet werden.

Die Verfügbarkeit der Geräte im Netzwerk kann, wie in Kapitel II-A beschrieben, mit der Anwendung nmap überwacht werden. Dabei ist der Unterschied zu diesem Projekt, dass beispielsweise nur der bzw. die Server im Unternehmensnetzwerk beobachtet werden muss und nicht das gesamte Subnetz. Bei dieser Gelegenheit, können alle Netzwerk Ports des Servers überprüft werden, um eventuelle Verwundbarkeiten automatisiert zu erkennen.

Falls das Unternehmen in einem Gegend mit schlechter oder inkonstanter Internetverbindung angesiedelt ist, kann beispielsweise mit nmap die Verfügbarkeit eines bekannten Webservers dokumentiert werden. Die Verfügbarkeit ist in den meisten Fällen auf die eigene Internetverfügbarkeit zurückzuführen, da Webserver normalerweise immer erreichbar sind. Das Protokoll kann bei unzureichender Internetverfügbarkeit als Nachweis beim Internetprovider mit der Aufforderung zur Mängelbeseitigung vorgelegt werden.

Unabhängig davon, ob das Unternehmen einen gekühlten Server- bzw. Netzwerkschrank besitzt oder lediglich einen Server-/Netzwerkschrank ohne Kühlung, kann mit einem Raspberry Pi sehr einfach die Temperatur in diesem überwacht werden. Dadurch könnte der IT-Verantwortliche beispielsweise in einem heißen Sommer oder bei Ausfall einer aktiven Kühleinheit informiert werden, bevor die Geräte überhitzen. Falls keine aktive Kühleinheit vorhanden ist, kann die Information über die Temperaturentwicklung als Kaufentscheidung für eine Kühlung zugrunde gelegt werden.

VII. Fazit

In dieser Arbeit wurde erläutert, wie ein kleines mittelständisches Unternehmen mithilfe eines Raspberry Pi alle mit dem Unternehmensnetzwerk verbundenen Netzwerkgeräte monitoren kann. ARPwatch hat mit seiner integrierten Speichermöglichkeit und dem integrierten E-Mail-Versand lediglich auf einen E-Mail-Dienst des Betriebssystems zurückgreifen müssen. Die weitere Funktionalität wird von ARPwatch selbstständig gemanagt. Dabei muss die Anwendung nicht selbst aktiv nach neuen Geräten suchen, sondern hört bei ARP-Anfragen von anderen Geräten zu und verarbeitet diese. Dadurch entsteht beim Entdecken der Geräte kein zusätzlicher Netzwerkdatenverkehr. In den Tests hat sich gezeigt, dass ARPwatch die Änderungen im Netzwerk zuverlässig mitbekommt. Ebenfalls hat ARPwatch in den Testfällen Änderungen an den MAC-Adressen stets erkannt und die entsprechende E-Mail versendet. Die in diesem Projekt verwendete Software ist vollständig kostenfrei nutzbar, daher sind nur Kosten für die Anschaffung des Raspberry Pi angefallen. Mit den Gesamtkosten von knapp 40 Euro wird das in der Einleitung beschriebene Kostenziel erreicht. Damit kann festgehalten werden, dass die Verwendung von ARPwatch auf einem Raspberry Pi eine zuverlässige, sowie kostengünstige Lösung ist die jedes bisher nicht geschützte Unternehmensnetzwerk verbessern kann.

Literatur

[1] Gordon Lyon, *Host-Erkennung*. Adresse: https://nmap.org/man/de/man-host-discovery.html (besucht am 07. 07. 2020).

[2] M. Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan und Ata-ur-rehman, „Penetration Testing Active Reconnaissance Phase – Optimized Port Scanning With Nmap Tool“, in *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, 2019, S. 1–6. DOI: 10.1109/ICOMET.2019.8673520.

[3] Im Sun-young, S.-H. Shin, K. Y. Ryu und B.-h. Roh, „Performance evaluation of network scanning tools with operation of firewall“, in *ICUFN 2016*, Piscataway, NJ: IEEE, 2016, S. 876–881, ISBN: 978-1-4673-9991-3. DOI: 10.1109/ICUFN.2016.7537162.

[4] David C. Plummer, „RFC 826 - An Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware“, *RFC*, 1982. Adresse: https://tools.ietf.org/html/rfc826 (besucht am 30. 06. 2020).

[5] Sudhakar und R. K. Aggarwal, „A survey on comparative analysis of tools for the detection of ARP poisoning“, in *2nd International Conference on Telecommunication and Networks - TEL-NET 2017*, B. Shukla, Hrsg., Piscataway, NJ: IEEE, 2017, S. 1–6, ISBN: 978-1-5090-6710-7. DOI: 10.1109/TEL-NET.2017.8343546.

[6] V. Prevelakis und W. Adi, „LS-ARP: A lightweight and secure ARP“, in *2017 Seventh International Conference on Emerging Security Technologies (EST)*, 2017, S. 204–208. DOI: 10.1109/EST.2017.8090424.

[7] Z. Balogh, S. Koprda und J. Francisti, „LAN security analysis and design“, S. 1–6, DOI: 10.1109/ICAICT.2018.8746912.

[8] S. Jacobs, *OVERVIEW OF CURRENT AND FUTURE NETWORKS*.
Adresse: https://ieeexplore-ieee-org.thi.idm.oclc.org/document/6671231,.

[9] Christoph Mayer,
XArp | Advanced ARP spoofing detection.
Adresse: http://www.xarp.net/#solution (besucht am 07. 06. 2020).

[10] Andrea Di Pasquale,
ArpON / Code / [0bf234] /README.
Adresse: https://sourceforge.net/p/arpon/code/ci/master/tree/README (besucht am 07. 06. 2020).

[11] Statista GmbH, *Betriebssysteme - Marktanteile in Deutschland bis 2020 | Statista*,
Statista GmbH, Hrsg.
Adresse: https://de.statista.com/statistik/daten/studie/158102/umfrage/marktanteile-von-betriebssystemen-in-deutschland-seit-2009/#professional (besucht am 07. 06. 2020).

[12] reichelt elektronik GmbH & Co. KG,
RASPBERRY PI 3B+ - Raspberry Pi 3 B+, 4x 1,4 GHz, 1 GB RAM, WLAN, BT,
reichelt elektronik GmbH & Co. KG, Hrsg.
Adresse: https://www.reichelt.de/raspberry-pi-3-b-4x-1-4-ghz-1-gb-ram-wlan-bt-raspberry-pi-3b-p217696.html?PROVID=2788 (besucht am 28. 06. 2020).

[13] Raspberry Pi Org,
Buy a Raspberry Pi 3 Model B+ – Raspberry Pi.
Adresse:
https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/ (besucht am 05. 06. 2020).

[14] ——, *Raspberry Pi OS - Raspberry Pi Documentation*. Adresse: https://www.raspberrypi.org/documentation/raspbian/ (besucht am 05. 06. 2020).

[15] ——, *NOOBS - Raspberry Pi Documentation*.
Adresse: https://www.raspberrypi.org/documentation/installation/noobs.md (besucht am 05. 06. 2020).

[16] Ben Stienstra,
raspberry_pi_arp_watcher [Ben Stienstra],
Polaire, Hrsg. Adresse: https://wiki.polaire.nl/doku.php?id=raspberry_pi_arp_watcher (besucht am 30. 06. 2020).

[17] P. Siering, „Minimal-Mailer“, *Heise*, 2018-05-25.
Adresse: https://www.heise.de/select/ct/2018/12/1528000378377701 (besucht am 12. 06. 2020).

[18] ubuntu Deutschland e. V.,
apt-get › apt › Wiki › ubuntuusers.de,
ubuntu Deutschland e. V., Hrsg.
Adresse: https://wiki.ubuntuusers.de/apt/apt-get/#apt-get-update (besucht am 12. 06. 2020).

[19] ——, *apt-get › apt › Wiki › ubuntuusers.de*,
ubuntu Deutschland e. V., Hrsg.
Adresse: https://wiki.ubuntuusers.de/apt/apt-get/#apt-get-upgrade (besucht am 12. 06. 2020).

[20] Sergey Poznyakoff, *Mailutils*. Adresse:
https://mailutils.org/ (besucht am 01. 07. 2020).

[21] Matt Ryan, Hugo Haas, Christoph Lameter, Dave Collier-Brown, *ssmtp(8): send message using smtp - Linux man page*.
Adresse: https://linux.die.net/man/8/ssmtp (besucht am 12. 06. 2020).

[22] Reuben Thomas, *ssmtp.conf(5): ssmtp config file - Linux man page*.
Adresse: https://linux.die.net/man/5/ssmtp.conf (besucht am 12. 06. 2020).

[23] Craig Leres, *arpwatch(8) - Linux man page*.
Adresse: https://linux.die.net/man/8/arpwatch (besucht am 12. 06. 2020).

[24] Sohail, *How To Monitor Ethernet Activity In Linux Using Arpwatch - LinuxAndUbuntu*,
Linuxandubuntu, Hrsg., 2019. Adresse:
http://www.linuxandubuntu.com/home/how-to-monitor-ethernet-activity-in-linux-using-arpwatch (besucht am 26. 06. 2020).

[25] 1&1 Mail & Media GmbH, *Wieso erhalte ich beim SMTP-Versand die Fehlermeldung Ünauthorized sender address"? - GMX Hilfe*,
1&1 Mail & Media GmbH, Hrsg. Adresse:
https://postmaster.gmx.net/de/fehlermeldungen (besucht am 26. 06. 2020).

[26] Raspberry Pi Org,
rc.local - Raspberry Pi Documentation,
Raspberry Pi Org, Hrsg. Adresse:
https://www.raspberrypi.org/documentation/linux/usage/rc-local.md (besucht am 26. 06. 2020).

[27] NoVirusThank Company Srl,
Change (Spoof) MAC Address with MAC Address Changer | NoVirusThanks,
NoVirusThank Company Srl, Hrsg. Adresse:
https://www.novirusthanks.org/products/mac-address-changer/ (besucht am 27. 06. 2020).

[28] Henry Ware, *vmstat(8): Report virtual memory statistics - Linux man page*.
Adresse: https://linux.die.net/man/8/vmstat (besucht am 08. 07. 2020).

[29] Lawrence Berkeley National Laboratory,
Index of /downloads/arpwatch,
Lawrence Berkeley National Laboratory, Hrsg.
Adresse: https://ee.lbl.gov/downloads/arpwatch/ (besucht am 01. 07. 2020).