



# Bericht für **www.sternwarte.at**

17. Februar 2020

## Disclaimer

Dieser Bericht stützt sich ausschließlich auf Daten, die unauthentifiziert abrufbar sind. Es wurden weder Login-Daten mittels Bruteforce ermittelt, noch per Login geschützte Daten kopiert oder verwendet.

## 1 Zusammenfassung

Tests wurden im Zeitraum von 15. Jänner 2020 bis 17. Februar 2020 vorgenommen. Ziel dieses Tests war die Ermittlung der Angriffsfläche von [www.sternwarte.at](http://www.sternwarte.at), der verwendeten Infrastruktur sowie eine Analyse der verwendeten Programme um schließlich eine Handlungsempfehlung zu formulieren. Im Rahmen des Test wurden neben dem Server der Sternwarte auch andere Services gefunden. Sofern sich diese im IP-Adressbereich in unmittelbarer Nähe befunden haben, wurden diese Server ebenfalls analysiert.

Im Folgenden werden die wichtigsten Erkenntnisse kurz dargestellt

1. Keine TLS-Verschlüsselung der Website obwohl auf der Website Formulare angeboten werden, die vertrauliche Daten abfragen. Auch der Admin-login ist unverschlüsselt und kann daher sehr einfach in einem überwachten Netzwerk abgefangen werden.
2. Unauthentifiziert einsehbare Log-Datei, die Server-Fehler ausgibt.
3. Der FTP-Server ist auf dem Standardport verfügbar und es ist mutmaßlich verwundbar auf Bruteforce-Attacken.
4. Die Webseite kann durch modifizierte URLs in der Darstellung verändert werden. Die Daten auf dem Server müssen dafür nicht verändert werden.
5. Die verwendete Software (4D Webstar 2004) wird vom Hersteller nicht mehr unterstützt. Die Tatsache, dass keine dokumentierten Sicherheitslücken existieren ist der mangelhaften Verbreitung und nicht der Qualität der Software zuzuschreiben.

## 2 Methodik

In die Untersuchungen waren folgende Personen involviert:

- Robert Führicht
- Tobias Höller
- Michael Preisach

Alle genannten sind bei SIGFLAG ([www.sigflag.at](http://www.sigflag.at)) tätig.

## 2.1 Informationsgewinnung

Ziel dieser Analyse ist Informationen über das System hinter [www.sternwarte.at](http://www.sternwarte.at) zu finden. Für die gefundenen Services sollen möglichst alle frei zugänglichen Daten gefunden und ausgewertet werden. Daraus ergeben sich dann Handlungsempfehlungen, die im Folgenden Teil des Berichts erläutert sind.

## 2.2 Verwendete Programme

- Firefox 72
- Nmap 7.80
- Dirsearch 0.3.9
- TOR Web Browser (Firefox 68)
- ftp 1.9.4
- OpenBSD netcat 1.206 Debian Patchlevel 1

## 3 Erkenntnisse

Über einen einfachen NMap-Scan können folgende Services auf dem Zielhost ermittelt werden:

Listing 1: Ergebnis des Portscans von NMap

```

1 sternwarte.at
2 Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-17 17:43 CET
3 Nmap scan report for www.sternwarte.at (85.126.106.150)
4 Host is up (0.052s latency).
5 rDNS record for 85.126.106.150: polaris.mag.eu
6 Not shown: 65513 closed ports
7 PORT      STATE SERVICE
8 19/tcp    filtered chargen
9 21/tcp    open    ftp
10 80/tcp   open    http
11 111/tcp  filtered rpcbind
12 135/tcp  filtered msrpc
13 136/tcp  filtered profile
14 137/tcp  filtered netbios-ns
15 138/tcp  filtered netbios-dgm
16 139/tcp  filtered netbios-ssn
17 407/tcp  filtered timbuktu
18 445/tcp  filtered microsoft-ds
19 554/tcp  filtered rtsp
20 593/tcp  filtered http-rpc-epmap
21 1417/tcp filtered timbuktu-srv1
22 1418/tcp filtered timbuktu-srv2
23 1419/tcp filtered timbuktu-srv3
24 1420/tcp filtered timbuktu-srv4
25 1434/tcp filtered ms-sql-m
26 1720/tcp filtered h323q931
27 2000/tcp filtered cisco-sccp
28 5060/tcp filtered sip
29 8000/tcp open   http-alt
30 8080/tcp open   http-proxy

```

<sup>31</sup>

<sup>32</sup> Nmap done: 1 IP address (1 host up) scanned in 23.82 seconds

Daraus ergibt sich folgende Service Liste für sternwarte.at

- Port 21 und 8000: FTP Server und Rumpus FTP Webinterface
- Port 80 und 8080: Webstar 4D Webserver
- Mail-Service für den Zivilschutzverband Oberösterreich (nur Clientverbindungen)
- Mailserver für sternwarte.at, der auf 2 anderen Hosts angeboten wird.

Die folgende Analyse wird in die genannten Services unterteilt.

### 3.1 Webserver

Firefox kann in den Developer Tools die Metadaten des Response Headers analysieren. Dort findet sich im Server-Tag die Information des Webservers:

Listing 2: HTTP Response Header von [www.sternwarte.at](http://www.sternwarte.at)

```
HTTP/1.1 200 OK
Server: 4D WebStar D/2004
Date: Sun, 02 Feb 2020 21:08:44 GMT
Content-Length: 12281
Last-Modified: Sun, 02 Feb 2020 21:08:44 GMT
Connection: Keep-Alive
Content-Type: text/html
```

- Installierter Server: 4D WebStar\_D/2004, vermutlich installiert auf Mac OS X

#### 3.1.1 Kein TLS

Die Webseite bietet neben statischen Inhalten auch Anmeldeformulare für Events des Vereins an. Im Sinne der §§24 ff DSGVO müssen geeignete technische Maßnahmen getroffen werden, damit persönliche Daten nicht an eine unbestimmte Zahl dritter Personen zugänglich gemacht werden kann. Daher muss eine Verschlüsselung der Kommunikation eingeführt werden, um mit diesen Bestimmungen konform zu werden.

#### Handlungsempfehlung:

Einführung von TLS1.2 oder höher für zumindest die Formularseiten, aber auch für das restliche Angebot des Vereins. Da dies aufgrund der veralteten Software nicht direkt unterstützt wird, muss entweder ein TLS-Proxy vorgeschalten werden oder die Website auf einen Server mit aktueller Software umgesiedelt werden.

#### 3.1.2 Beliebige Frames per URL laden

Die Darstellung der Webseite gliedert sich in 2 Frames, Verzeichnis und Inhaltsframe. `start.html` stellt dabei den Inhalt dar und `default.html` kümmert sich um das Verzeichnis. Nun ist es aber möglich, die Homepage mit einer beliebigen zusätzlichen URL aufzurufen:

`http://www.sternwarte.at/default.html?https://jku.at`

Das Beispiel lädt die Seite der JKU in den Hauptframe anstelle der vorgesehenen Startseite. Weiters kann auch die eigene Seite geschachtelt aufgerufen werden:

`http://www.sternwarte.at/?/?/?/`

Hier wird vier Mal `default.html` aufgerufen und in den Inhaltsframe des vorherigen Aufrufes dargestellt. Diese Schwachstelle eine Möglichkeit Drive-By-Exploits an Personen, die dieser Website vertrauen, auszuliefern.

#### Handlungsempfehlung:

`default.html` darf nur eine definierte Liste an Links entgegennehmen - die der vorhandenen Subseiten (Whitelisting).

### 3.1.3 Fehlerhafte Auslieferung spezieller Subseiten

Es gibt Subseiten, die sich in einem Unterverzeichnis auf dem Server befinden. Ein aktuelles Beispiel ist:

```
http://www.sternwarte.at/planetenweg/
```

Damit dieser Aufruf korrekt erfolgt, muss das Arbeitsverzeichnis auf dem Server gewechselt werden. Es ist aber möglich, dies zu verhindern, indem der letzte / in der URL weggelassen wird:

```
http://www.sternwarte.at/planetenweg
```

Nun können referenzierte Objekte, wie Bilder und Stylesheets nicht mehr geladen werden. Zusätzlich wird für jedes nicht fundene Objekt eine Zeile im error.log erzeugt.

Listing 3: Erzeugte Fehler durch fehlerhaften Seitenaufruf

```
1 17.02.2020 21:28:40 ON ERR CALL -120 MaG /images/nav.png 95.129.203.119 :HandlePAGE
2 17.02.2020 21:28:40 ON ERR CALL -120 MaG /images/LAG-Logo.png 95.129.203.119 :HandlePAGE
3 17.02.2020 21:28:40 ON ERR CALL -120 MaG /images/next.png 95.129.203.119 :HandlePAGE
4 17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel01.png 95.129.203.119 :HandlePAGE
5 17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel02.png 95.129.203.119 :HandlePAGE
6 17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel04.png 95.129.203.119 :HandlePAGE
7 17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel05.png 95.129.203.119 :HandlePAGE
8 17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel03.png 95.129.203.119 :HandlePAGE
9 17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel06.png 95.129.203.119 :HandlePAGE
10 17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel07.png 95.129.203.119 :HandlePAGE
11 17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel08.png 95.129.203.119 :HandlePAGE
12 17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel09.png 95.129.203.119 :HandlePAGE
13 17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel10.png 95.129.203.119 :HandlePAGE
14 17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel11.png 95.129.203.119 :HandlePAGE
15 17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel12.png 95.129.203.119 :HandlePAGE
16 17.02.2020 21:28:40 ON ERR CALL -120 MaG /images/top.png 95.129.203.119 :HandlePAGE
17 17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel03.png 95.129.203.119 :HandlePAGE
18 17.02.2020 21:28:41 ON ERR CALL -120 MaG /Images/Tafel04.png 95.129.203.119 :HandlePAGE
19 17.02.2020 21:28:41 ON ERR CALL -120 MaG /Images/Tafel05.png 95.129.203.119 :HandlePAGE
20 17.02.2020 21:28:41 ON ERR CALL -120 MaG /Images/Tafel06.png 95.129.203.119 :HandlePAGE
21 17.02.2020 21:28:41 ON ERR CALL -120 MaG /Images/Tafel07.png 95.129.203.119 :HandlePAGE
22 17.02.2020 21:28:41 ON ERR CALL -120 MaG /images/nav.png 95.129.203.119 :HandlePAGE
23 17.02.2020 21:28:41 ON ERR CALL -120 MaG /images/next.png 95.129.203.119 :HandlePAGE
24 17.02.2020 21:28:41 ON ERR CALL -120 MaG /images/LAG-Logo.png 95.129.203.119 :HandlePAGE
25 17.02.2020 21:28:41 ON ERR CALL -120 MaG /Images/Tafel01.png 95.129.203.119 :HandlePAGE
26 17.02.2020 21:28:41 ON ERR CALL -120 MaG /Images/Tafel02.png 95.129.203.119 :HandlePAGE
```

#### Handlungsempfehlung:

- Aliasing für diese Endpunkte einführen (wie es auch bei den anderen Webauftritten auf diesem Server der Fall ist). Damit wird der Browser automatisch auf den richtigen Endpunkt weiter geleitet.
- absolute Referenzen in der Seite verwenden oder immer aus dem gleichen Arbeitsverzeichnis den Webauftritt ausliefern.

### 3.1.4 Öffentlich zugängliche Dateien mit Metainformationen

Dirsearch traversiert die zugänglichen Seiten auf dem Server, indem es die URL errät. Dazu hat Dirsearch eine Liste von Verzeichnissen aller gängiger Webserver. Das Ergebnis dieser Suche:

Listing 4: Mittels DirSearch Gefundene Endpoints

```
1 > dirsearch -u www.sternwarte.at -E
2
3 |. | v0.3.9
4 (|||_) (7(|||(| )
5
6 Extensions: php, asp, aspx, jsp, js, html, do, action | HTTP method: get | \
7 Threads: 10 | Wordlist size: 8673
```

```

8
9 Error Log: /home/fuero/.dirsearch/logs/errors-20-01-19_19-32-00.log
10
11 Target: www.sternwarte.at
12
13 [19:32:00] Starting:
14 [19:32:01] 200 - 2KB - /%3f/
15 [19:32:03] 200 - 21KB - /.DS_Store
16 [19:32:13] 200 - 46KB - /log/error.log
17 [19:32:30] 500 - 294B - /ActiveDirectoryRemoteAdminScripts/
18 [19:34:27] 200 - 64KB - /favicon.ico
19 [19:35:02] 200 - 408KB - /log/error.log
20 [19:35:35] 500 - 294B - /phpMyAdmin-2.11.5.1-all-languages/
21 [19:35:35] 500 - 294B - /phpMyAdmin-2.11.7.1-all-languages-utf-8-only/
22 [19:35:35] 500 - 294B - /phpMyAdmin-2.11.7.1-all-languages/
23 [19:35:35] 500 - 294B - /phpMyAdmin-2.11.8.1-all-languages-utf-8-only/
24 [19:35:35] 500 - 294B - /phpMyAdmin-2.11.8.1-all-languages/
25 [19:35:53] 200 - 118B - /robots.txt
26 [19:36:14] 200 - 15KB - /start.html
27 [19:36:40] 500 - 294B - /WebSphereSamples.Configuration.config
28
29 Task Completed

```

Die HTTP Statuscodes zeigen, dass einige URLs mit Code 500 antworten. Bei Aufruf dieser Seiten ist zuverlässig und immer gleich. Daher ist es sehr wahrscheinlich, dass der *Internal Server Error* nur eine Verschleierungstaktik ist.

Des Weiteren findet sich in Zeile 15 der Ausgabe `.DS_Store` welches auf dem MAC zum Speichern von Metadaten der in diesem Verzeichnis abgelegten Dateien genutzt wird. Viel Aussagekräftiger ist das `error.log`, das mutmaßlich beim Blacklisting übersehen wurde. Dieses Log wird wöchentlich in der Nacht von Samstag auf Sonntag gelöscht. Es werden alle Dateiaufrufe am Server geloggt, die einen Rückgabewert ungleich 0 haben. Dieses Log bietet eine Vielzahl an Meta-Informationen, die hier nur beispielhaft aufgezählt sind:

- Wann sich der Administrator (vermutlich) eingeloggt oder ausgeloggt hat (Rückgabewert > 0)
- Dazugehöriger Pfad zum Login des Backends (wieder unverschlüsselt!)
- Welche Dateien geöffnet wurden (aber Rückgabewert = 15)
- Fehler anderer Webauftritte auf diesem Server <sup>1</sup> <sup>2</sup>
- Fehlerhaft eingegebene URLs auf diesem Server (alte Seiten auf dem Server oder Metainformationen zu den Besuchern)
- Rückgabewerte der Datenbank und der hinterlegten Skripte - Damit kann der Ordner `/4dcgi` durchsucht, bzw. dessen Inhalt aus dem Log ausgelesen werden.
- Fehler des Mailservers geben Hinweis auf die Aufgaben des selben. Mehr dazu im Kapitel zu Mailserver

Es wurden dank der Dokumentation für 4D WebStar, die noch immer online verfügbar ist<sup>3</sup>, weitere gültige Pfade gefunden:

- `/4dstats` - Abrufstatistiken
- `/4dhtmlstats` - Abrufstatistiken
- `/4dcache-clear` - Leeren des Caches
- `/4dwebtest` - Informationen über den verbundenen Client
- `/4dblank` - Leere Seite

<sup>1</sup>[www.kalendermanufaktur.at](http://www.kalendermanufaktur.at)

<sup>2</sup>[www.baer.co.at](http://www.baer.co.at)

<sup>3</sup>[http://www.island-data.com/downloads/books/4D\\_Web\\_Companion.pdf](http://www.island-data.com/downloads/books/4D_Web_Companion.pdf)

- /4dmETHOD - Kann nicht aufgerufen werden, die URL wird aber erweitert auf beispielsweise  
<http://www.sternwarte.at/4dmETHOD//%23%231997692744.0>
- /4dSSI - Verbotene Anfrage

Alle diese Seiten erzeugen keinen Log-Eintrag und sollten nicht direkt aufgerufen werden können.

Zusätzlich lassen sich die Skripts im Ordner /4dcgi, die beispielsweise für das Erfassen der Formulardaten genutzt werden, direkt per URL ausführen, ganz ohne Parameter. Durch das Log können auch per Erraten der Namen weitere Skripte gefunden werden.

#### **Handlungsempfehlung:**

Im Arbeitsverzeichnis des Webservers sollten sich nur Dateien befinden, die mit der Auslieferung der Seite direkt zu tun haben. Für Log-Dateien gibt es eigene Verzeichnisse.

#### **3.1.5 Sehr alte Version des Servers**

Der zurzeit laufende Webserver scheint zumindest gegen dokumentierte Schwachstellen geschützt zu sein, die letzten bekannten Bugs CVE 2004-0696 und CVE 2006-6131 haben keinen Erfolg gezeigt. Die Software wird aber vom Hersteller nicht mehr unterstützt. Wenn also neue Bugs auftreten, werden diese nicht mehr repariert. Daher sollte die Webseite auf einem Server betrieben werden, der von den Entwicklern noch mit Updates versorgt wird.

#### **Handlungsempfehlung:**

- Update der verwendeten Software auf aktuell gewartete Versionen.
- Regelmäßige bzw. automatische Updates (zumindest bei reinen Sicherheitsupdates)

#### **3.2 FTP-Server**

Port 21 auf dem Server war zum Zeitpunkt der ersten Untersuchung noch erreichbar. Der Server bot unverschlüsseltes FTP an und verlangte Username und Passwort. Wie schon beim Webserver kann hier der Login über das Netzwerk abgefangen werden. Das gleiche Problem hat auch der Rumpus FTP Server, der über

<http://www.sternwarte.at:8000>

erreichbar ist. Abgesehen von der unverschlüsselten Übermittlung von Login-Daten scheint dieser Service aber aktuell zu sein. Die dokumentierte Schwachstelle CVE-2019-19368<sup>4</sup> ermöglicht Cross-Site-Scripting über die URL. Die Resultierende URL

<http://www.sternwarte.at:8000/Login?!%27%3E%3CsVg/0nLoAD=alert'1'//>

blieb ohne Effekt.

#### **Handlungsempfehlung:**

- FTP ausschließlich über eine verschlüsselte Verbindung anbieten. Einerseits kann dafür Secure FTP verwendet werden, was inzwischen die meisten FTP Server anbieten. Andererseits bietet auch SSH einen File Transfer Modus an, der in den Einstellungen des SSH aktiviert werden kann.
- Passwort-Authentifizierung durch Key-Based Authentication ersetzen. FTP over SSH bietet zusätzlich die Möglichkeit, die Authentifizierung über Public/Private Keys zu machen, um Bruteforce-Attacken auf Passwörter zu unterbinden.
- Fail2Ban aktivieren. Damit können Firewall-Regeln dynamisch angepasst werden, wenn ein Client zu oft versucht, sich mit falschen Login-Daten zu authentifizieren.

<sup>4</sup>[https://github.com/harshit-shukla/CVE/blob/master/CVE-2019-19368\(Un-authenticated\).md](https://github.com/harshit-shukla/CVE/blob/master/CVE-2019-19368(Un-authenticated).md)

- WebFTP ausschließlich über TLS anbieten (gleiche Handlungsempfehlung, wie bei Webserver weiter oben).

Nachtrag: Zumindest auf dem Server, der `www.sternwarte.at` ausliefert, ist eine Firewall aktiviert worden, die Anfragen auf diesen Port droppt (keine Antwort zurückschickt). Etwa später zeigt NMap wieder, dass der Port 21 zwar offen ist, allerdings antwortet der Server nicht auf Anfragen. Es ist daher nicht ganz klar, ob hier eine Firewall eigenartige Verbindungszustände hervorruft oder der Service zurzeit nicht ordnungsgemäß läuft.

### 3.3 Mail-Server

Hier sind zwei verschiedene Services entdeckt worden, die im folgenden behandelt werden.

- Mailserver, die für die Domain `sternwarte.at` im DNS eingetragen sind
- Der SMTP-Server, der direkt auf dem Server läuft

#### 3.3.1 Mailserver, der laut DNS zuständig ist

Listing 5: Mittels DirSearch Gefundene Endpoints

```

1 > dig -t mx sternwarte.at
2
3 ; <>> DiG 9.14.10 <>> -t mx sternwarte.at
4 ;; global options: +cmd
5 ;; Got answer:
6 ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26587
7 ;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 2
8
9 ;; OPT PSEUDOSECTION:
10 ; EDNS: version: 0, flags:; udp: 4000
11 ;; QUESTION SECTION:
12 ;sternwarte.at. IN MX
13
14 ;; ANSWER SECTION:
15 sternwarte.at. 2484 IN MX 20 mizar.mag.eu.
16 sternwarte.at. 2484 IN MX 10 nihal.mag.eu.
17
18 ;; ADDITIONAL SECTION:
19 mizar.mag.eu. 2484 IN A 85.126.106.142
20
21 ;; Query time: 1 msec
22 ;; SERVER: 140.78.100.119#53(140.78.100.119)
23 ;; WHEN: Mon Feb 17 13:38:08 CET 2020
24 ;; MSG SIZE rcvd: 108

```

Im DNS stehen zwei Server als Mail-Server (MX) zur Verfügung:

- `nihal.mag.eu` (85.126.106.144)
- `mizar.mag.eu` (85.126.106.142)

Beide Hosts haben laut NMap-Bericht Port 25 für SMTP offen:

Listing 6: NMap Portscan auf `nihal.mag.eu`

```

1 > nmap -T3 -Pn -p0-65535 85.126.106.144
2 Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-17 21:12 CET
3 Nmap scan report for nihal.mag.eu (85.126.106.144)
4 Host is up (0.026s latency).
5 Not shown: 65522 closed ports
6 PORT      STATE SERVICE
7 0/tcp      filtered unknown
8 22/tcp     filtered ssh
9 25/tcp     open  smtp
10 53/tcp    filtered domain
11 80/tcp    filtered http
12 407/tcp   filtered timbuktu
13 443/tcp   filtered https

```

```

14 465/tcp filtered smtps
15 587/tcp filtered submission
16 1417/tcp filtered timbuktu-srv1
17 1418/tcp filtered timbuktu-srv2
18 1419/tcp filtered timbuktu-srv3
19 1420/tcp filtered timbuktu-srv4
20 8080/tcp filtered http-proxy
21
22 Nmap done: 1 IP address (1 host up) scanned in 28.29 seconds

```

Listing 7: NMap Portscan auf `mizar.mag.eu`

```

1 > nmap -T3 -Pn -p0-65535 85.126.106.142
2 Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-17 21:13 CET
3 Nmap scan report for mizar.mag.eu (85.126.106.142)
4 Host is up (0.029s latency).
5 Not shown: 65523 closed ports
6 PORT      STATE SERVICE
7 0/tcp      filtered unknown
8 22/tcp     filtered ssh
9 25/tcp     open  smtp
10 53/tcp    filtered domain
11 80/tcp    filtered http
12 407/tcp   filtered timbuktu
13 465/tcp   filtered smtps
14 587/tcp   filtered submission
15 1417/tcp  filtered timbuktu-srv1
16 1418/tcp  filtered timbuktu-srv2
17 1419/tcp  filtered timbuktu-srv3
18 1420/tcp  filtered timbuktu-srv4
19 8080/tcp  filtered http-proxy
20
21 Nmap done: 1 IP address (1 host up) scanned in 26.70 seconds

```

Bei der ersten Analyse dieses Services war nur eine unverschlüsselte Verbindung möglich. Inzwischen wurde auf diesen Servern STARTTLS aktiviert.

### 3.3.2 Mailserver auf `sternwarte.at`

Im Errorlog des Webservers ist am 28. Jänner ein Fehler des internen Mailservers aufgetreten:

Listing 8: Fehler des Mailservers auf `sternwarte.at`

```

1 28.01.2020 06:37:22 ZS_SendAuthEmail 10042 MaG /4dcgi/form/webuser/reg/ 134.119.236.3 SMTP
      550 - Requested action not taken: mailbox unavailable
2
3 Liebe(r) Bürger(in)!
4
5 Vielen Dank für die Anmeldung zum Zivilschutz-SMS! Aus Datenschutzgründen ist noch ein
      letzter Schritt notwendig, um zukünftig die kostenlosen Zivilschutz-SMS-Nachrichten
      Ihrer Gemeinde zu erhalten:
6
7
8 1. Klicken Sie auf folgenden Link: http://sms.zivilschutz-ooe.at/ex4D/valid/free/key=646976/
      sec=91B7C3185E86CFA3E315F82F0142028F/id=4861077/
9
10 2. Daraufhin erhalten Sie eine SMS mit dem Aktivierungslink auf Ihr Handy.
11
12 3. Nach dem Anklicken des Aktivierungslinks ist Ihre Mobiltelefon-Nummer für das Zivilschutz-
      SMS aktiviert.
13
14 4. Ab sofort erhalten Sie das Zivilschutz-SMS Ihrer Gemeinde und somit Informationen in
      Katastrophenfällen, Notfällen oder bei besonderen Ereignissen!
15
16
17 Bei Fragen wenden Sie sich bitte an das Zivilschutz-Team unter office@zivilschutz-ooe.at
      oder unter der Telefonnummer 0732 65 24 36!
18
19 Mit freundlichen Grüßen
20

```

<sup>21</sup> Josef Lindner

<sup>22</sup> Zivilschutz-Landesgeschäftsführer

Dies dokumentiert die Funktion des Services für `sms.zivilschutz-ooe.at`. Der DNS-Eintrag für diese Domain zeigt auf 85.126.106.150, was die *benachbarte* IP-Adresse zu `sternwarte.at` ist. Es ist nicht nachvollziehbar, warum diese Fehlermeldung im `error.log` der Sternwarte-Website auftritt. Am wahrscheinlichsten ist, dass hinter beiden IPs der selbe Server läuft und es keine Trennung der Services voneinander gibt.

Diese Vermischung unterschiedlicher Services darf in einem Produktivsystem nicht passieren.

#### **Handlungsempfehlung:**

- Sofern der Betrieb unterschiedlicher Domains auf einem Host erforderlich ist, sollten zumindest alle Ressourcen der verschiedenen Services auf dem Server (User, Dateien, Berechtigungen) möglichst weitgehend voneinander getrennt werden.
- Stand der Technik ist die Trennung der Webseiten auf Service-Ebene (z. B. Docker), Betriebssystem-Ebene (mittels virtueller Maschinen) oder getrennte Hardware. Letzteres wäre in diesem Fall sogar recht einfach möglich, da schon 2 unterschiedliche IPs eingerichtet sind.