Bericht für *www.sternwarte.at*

20. Februar 2020

Disclaimer

Dieser Bericht stützt sich ausschließlich auf Daten, die frei 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 19. Februar 2020 vorgenommen. Ziel dieses Tests war die Ermittlung der Angriffsoberfläche von `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 (`fuerob@gmail.com`)
- Tobias Höller
- Michael Preisach (`michael@preisach.at`)

Alle genannten sind bei SIGFLAG (`www.sigflag.at`) tätig.

2.1. Informationsgewinnung

Ziel dieser Analyse war, Informationen über das System hinter `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
- DiG 9.14.10
- testssl.sh 3.0

2.3. 3 Kategorien der Informationssicherheit

Jede Schwachstelle wird in der folgenden Analyse in die drei Kategorien der Informationssicherheit eingeordnet. Diese Kategorien sind:

1. Vertraulichkeit/Confidentiality (C) – Ein Service muss den Zugriff auf Daten auf das notwendige beschränken. Das bedeutet, dass die Daten dieses Services nur von den autorisierten Benutzern gelesen werden darf. Ein Service darf seine Daten nur an autorisierte Benutzer weitergeben. Unautorisierte Dritte müssen zuverlässig vom Zugriff auf diese Daten ferngehalten werden. Dies gilt auch für die Übertragung zum Benutzer und Speicherung der Daten abseits vom System (z. B. Für ein Backup)
2. Integrität/Integrity (I) – Der Service muss sicherstellen, dass die Daten unverändert und vollständig vorgehalten werden. Es muss also verhindert werden, dass die Daten von nicht autorisierten Benutzen oder durch unerwartetes Verhalten des Services modifiziert werden können.
3. Verfügbarkeit/Availability (A) – Der Service muss verfügbar sein, wenn dieser benötigt wird. In diesem Fall sind vor Allem Maßnahmen gegen Denial-of-Service (DoS) Angriffe zu berücksichtigen.

3. Erkenntnisse

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

Listing 1: Ergebnis des Portscans von NMap

```
> nmap -T3 -Pn -p0-65535 sternwarte.at
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-17 17:43 CET
Nmap scan report for www.sternwarte.at (85.126.106.150)
Host is up (0.052s latency).
rDNS record for 85.126.106.150: polaris.mag.eu
Not shown: 65513 closed ports
PORT   STATE  SERVICE
19/tcp filtered chargen
21/tcp open   ftp
80/tcp open   http
111/tcp filtered rpcbind
135/tcp filtered msrpc
136/tcp filtered profile
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
407/tcp filtered timbuktu
445/tcp filtered microsoft-ds
554/tcp filtered rtsp
593/tcp filtered http-rpc-epmap
1417/tcp filtered timbuktu-srv1
1418/tcp filtered timbuktu-srv2
1419/tcp filtered timbuktu-srv3
1420/tcp filtered timbuktu-srv4
1434/tcp filtered ms-sql-m
1720/tcp filtered h323q931
2000/tcp filtered cisco-sccp
5060/tcp filtered sip
8000/tcp open http-alt
8080/tcp open http-proxy

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

Im Laufe der Untersuchungen wurden noch weitere Services gefunden:

- Mail-Service für den Zivilschutzverband Oberösterreich (nur Clientverbindungen)
- Mailserver für `sternwarte.at`, der auf 2 anderen Hosts angeboten wird.

Im folgenden werden die genannten Services analysiert. Mit den angegebenen Handlungsempfehlungen ist es möglich die ausgeführten Probleme umfassend zu lösen.

3.1. Webserver

Firefox kann in den Developer Tools die Metadaten des Serverantwort analysieren. Im Server-Tag finden sich die Information des Webservers:

Listing 2: HTTP Response Header von `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.
Weiters wird die Unterstützung von TLS Versionen vor TLS1.2 noch im Laufe des Jahres 2020 von den Browserherstellern abgeschaltet.

Informationssicherheit:

- Confidentiality: Daten können bei Übertragung in beide Richtungen beliebig eingesehen werden.
- Integrity: Daten und Inhalte können in beide Richtungen beliebig verändert werden, es findet keine Integritätsprüfung an den Daten statt.
- Availability: Einem Angreifer ist es möglich ein unverschlüsseltes Passwort beim Login abzufangen und damit den kompletten Webauftritt bzw. den Server zu übernehmen.

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,
- ein Reverse-Proxy TLS terminieren oder
- 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 stellt eine Möglichkeit dar, Drive-By-Exploits an Personen, die dieser Website vertrauen, auszuliefern.

Informationssicherheit:

- Confidentiality: Benutzer könnten auf gefälschten Webseiten vertrauliche Daten weiter geben.
- Integrity: Die eingegebenen Daten auf den gefälschten Webseiten werden wahrscheinlich nicht den Weg in die korrekte Datenbank finden.
- Availability: Durch das Laden von Inhalten anderer Seiten kann recht zuverlässig. verhindert werden, dass die vorgesehenen Inhalte tatsächlich angezeigt werden.

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 gefundene Objekt eine Zeile im error.log erzeugt.

Listing 3: Erzeugte Fehler durch fehlerhaften Seitenaufruf

```
17.02.2020 21:28:40 ON ERR CALL -120 MaG /images/nav.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:40 ON ERR CALL -120 MaG /images/LAG-Logo.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:40 ON ERR CALL -120 MaG /images/next.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel01.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel02.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel04.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel05.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel03.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel06.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel07.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel08.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel09.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel10.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel11.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel12.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:40 ON ERR CALL -120 MaG /images/top.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:40 ON ERR CALL -120 MaG /Images/Tafel03.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:41 ON ERR CALL -120 MaG /Images/Tafel04.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:41 ON ERR CALL -120 MaG /Images/Tafel05.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:41 ON ERR CALL -120 MaG /Images/Tafel06.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:41 ON ERR CALL -120 MaG /Images/Tafel07.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:41 ON ERR CALL -120 MaG /images/nav.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:41 ON ERR CALL -120 MaG /images/next.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:41 ON ERR CALL -120 MaG /images/LAG-Logo.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:41 ON ERR CALL -120 MaG /Images/Tafel01.png 95.129.203.119 :HandlePAGE
17.02.2020 21:28:41 ON ERR CALL -120 MaG /Images/Tafel02.png 95.129.203.119 :HandlePAGE
```

Informationssicherheit:

- Confidentiality: Keine Auswirkungen.
- Integrity: Die Integrität der ausgelieferten Webseite ist nicht gegeben.
- Availability: Die ausgelieferte Webseite ist unvollständig und daher eingeschränkt bis gar nicht benutzbar.

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 weitergeleitet.
- 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  (||| _) (/(|| (| )
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 dieser zuverlässig und immer gleich.
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 protokolliert, 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 [1] [2]
- 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[3], weitere gültige Pfade gefunden:

- `/4dstats` - Abrufstatistiken

[1] `www.kalendermanufaktur.at`
[2] `www.baer.co.at`
[3] `http://www.island-data.com/downloads/books/4D_Web_Companion.pdf`

- `/4dhtmlstats` - Abrufstatistiken
- `/4dcacheclear` - Leeren des Caches
- `/4dwebtest` - Informationen über den verbundenen Client
- `/4dblank` - Leere Seite
- `/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.

Informationssicherheit:

- Confidentiality: Informationen über den Server, dessen Benutzer und anderer Webseiten werden ohne autorisierung frei gegeben.
- Integrity: Unsicher, da nicht klar ist, ob die CGI-Skripte Datenbanken verändern oder nicht.
- Availability: Keine Auswirkung.

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.
Ist die Trennung von Log-Dateien und den auszuliefernden Webinhalten nicht möglich, muss entweder das Blacklisting um die entsprechenden Endpunkte erweitert werden oder ein vorgeschaltener Webproxy diese Aufgabe übernehmen.

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 einer Version des Produkts (4D) betrieben werden, die von den Entwicklern noch mit Updates versorgt wird.

Informationssicherheit:

- Confidentiality: Die verwendete Software ist nicht mehr in der Lage, die Daten vertraulich zu halten.
- Integrity: Undokumentierte Schwachstellen können jederzeit Daten kompromittieren.
- Availability: Die gleichen Schwachstellen können auch die Verfügbarkeit des Servers stören.

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*[4] ermöglicht Cross-Site-Scripting über die URL. Die resultierende URL

`http://www.sternwarte.at:8000/Login?!%27%3E%3CsVg/OnLoAD=alert‘1‘//`

blieb ohne Effekt.

Informationssicherheit:

- Confidentiality: Die übermittlung der Daten zwischen Server und Client sind nicht geschützt. Das gilt für das Rumpus Webinterface als auch für den FTP-Port.
- Integrity: Die Daten können während der Übertragung beliebig verändert werden.
- Availability: Wenn der Angreifer das unverschlüsselte Passwort bei der Übertragung abfängt, kann dieser wahrscheinlich den Webauftritt beliebig verändern.

Handlungsempfehlung:
Es gibt mittlerweile eine große Zahl an Argumenten, FTP nicht mehr zu verwenden. Der folgende Link fasst die Argumente anschaulich zusammen:

`http://mywiki.wooledge.org/FtpMustDie`

Die moderne Alternative zu FTP ist SFTP, also FTP over SSH. SFTP kann alle Funktionen von bisherigen FTP übernehmen und sollte daher ersatzlos zum Einsatz kommen. Folgende Punkte sind zusätzlich zu beachten:

- 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.
- WebFTP (Rumpus) 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). Etwas 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

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

3.3.1. Mailserver, der laut DNS zuständig ist

Listing 5: Mail Extension DNS Eintrag für `sternwarte.at`

```
> dig -t mx sternwarte.at

; <<>> DiG 9.14.10 <<>> -t mx sternwarte.at
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26587
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;sternwarte.at.   IN MX

;; ANSWER SECTION:
sternwarte.at.  2484 IN MX 20 mizar.mag.eu.
sternwarte.at.  2484 IN MX 10 nihal.mag.eu.

;; ADDITIONAL SECTION:
mizar.mag.eu.  2484 IN A 85.126.106.142

;; Query time: 1 msec
;; SERVER: 140.78.100.119#53(140.78.100.119)
;; WHEN: Mon Feb 17 13:38:08 CET 2020
;; 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`

```
> nmap -T3 -Pn -p0-65535 85.126.106.144
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-17 21:12 CET
Nmap scan report for nihal.mag.eu (85.126.106.144)
Host is up (0.026s latency).
Not shown: 65522 closed ports
PORT   STATE  SERVICE
0/tcp  filtered unknown
22/tcp filtered ssh
25/tcp open   smtp
53/tcp filtered domain
80/tcp filtered http
407/tcp filtered timbuktu
443/tcp filtered https
465/tcp filtered smtps
587/tcp filtered submission
1417/tcp filtered timbuktu-srv1
1418/tcp filtered timbuktu-srv2
1419/tcp filtered timbuktu-srv3
1420/tcp filtered timbuktu-srv4
8080/tcp filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 28.29 seconds
```

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

```
> nmap -T3 -Pn -p0-65535 85.126.106.142
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-17 21:13 CET
Nmap scan report for mizar.mag.eu (85.126.106.142)
Host is up (0.029s latency).
Not shown: 65523 closed ports
PORT   STATE  SERVICE
0/tcp  filtered unknown
22/tcp filtered ssh
25/tcp open   smtp
```

```
53/tcp filtered domain
80/tcp filtered http
407/tcp filtered timbuktu
465/tcp filtered smtps
587/tcp filtered submission
1417/tcp filtered timbuktu-srv1
1418/tcp filtered timbuktu-srv2
1419/tcp filtered timbuktu-srv3
1420/tcp filtered timbuktu-srv4
8080/tcp filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 26.70 seconds
```

Bei der ersten Analyse dieses Services war nur eine unverschlüsselte Verbinudung möglich. Inzwischen wurde auf diesen Servern STARTTLS aktiviert. Eine Analyse mit TestSSL zeigt (siehe Anhang), dass der Server SSLv3 anbietet. Dieses Protokoll wird schon seit längerem als unsicher gesehen. Für TLS 1.0 und 1.1 gilt das schon beim Webserver Beschriebene.

Informationssicherheit:

- Confidentiality: SSLv3 kann die Vertraulichkeit der Daten bei Übertragung nicht mehr gewährleisten. Bei den älterene TLS Versionen ist dies auch nur bedingt der Fall.
- Integrity: Wie bei der unverschlüsselten Übertragung kann auch hier die Integrität der Daten nur mit funktiostüchtiger Kryptogrfie sichergestellt werden.
- Availability: Die Veränderung der Daten kann auch die Verfügbarkeit des Services beeinträchtigen.

Handlungsempfehlung:
Wie beim Webserver sollte auch für den SMTP-Service die Verschlüsselung auf den Stand der Technik gebracht werden.

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`

```
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

Liebe(r) Bürger(in)!

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:


1. Klicken Sie auf folgenden Link: http://sms.zivilschutz-ooe.at/ex4D/valid/free/key=646976/
    sec=91B7C3185E86CFA3E315F82F0142028F/id=4861077/

2. Daraufhin erhalten Sie eine SMS mit dem Aktivierungslink auf Ihr Handy.

3. Nach dem Anklicken des Aktivierungslinks ist Ihre Mobiltelefon-Nummer für das Zivilschutz-
    SMS aktiviert.

4. Ab sofort erhalten Sie das Zivilschutz-SMS Ihrer Gemeinde und somit Informationen in
    Katastrophenfällen, Notfällen oder bei besonderen Ereignissen!


Bei Fragen wenden Sie sich bitte an das Zivilschutz-Team unter office@zivilschutz-ooe.at
    oder unter der Telefonnummer 0732 65 24 36!

Mit freundlichen Grüßen

Josef Lindner
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.

Informationssicherheit:

- Confidentiality: Die Anzeige von Fehlern eines komplett unabhängigen Services darf nicht passieren.
- Integrity: Schwachstellen fremder Services wirken sich auf die Integrität des Webauftritts der Sternwarte Linz aus.
- Availability: Die gleichen Schwachstellen können auch die Verfügbarkeit des Webauftritts beeinträchtigen.

Handlungsempfehlung:
Trennung des Services für die Sternwarte von den anderen, die auf diesem Server zurzeit laufen.

4. Zusammenassung

Im Folgenden sind die wichtigsten Handlungspunkte zusammengefasst:

- Software aktualisieren
- Webauftritt nur über TLS anbieten und die TLS-Konfiguration auf Stand der Technik bringen
- FTP-Server durch SFTP ersetzen
- TLS-Konfiguration am Mailserver auf den Stand der Technik anpassen
- Trennen der Inhalte der unterschiedlichen Webauftritte. Alle Inhalte von `sternwarte.at` sollten auf einem eigenen System gehostet werden und sich mit anderen Inhalten nicht überschneiden.

A. TestSSL Ergebnisse der Mailserver

Listing 9: TestSSL Ergebnis für `nihal.mag.eu`

```
> testssl.sh -t smtp nihal.mag.eu:25

###########################################################
   testssl.sh   3.0 from https://testssl.sh/

     This program is free software. Distribution and
            modification under GPLv2 permitted.
     USAGE w/o ANY WARRANTY. USE IT AT YOUR OWN RISK!

      Please file bugs @ https://testssl.sh/bugs/

###########################################################

 Using "OpenSSL 1.0.2-chacha (1.0.2k-dev)" [~183 ciphers]
 on gandalf:/home/fuero/Appz/testssl.sh/bin/openssl.Linux.x86_64
 (built: "Jan 18 17:12:17 2019", platform: "linux-x86_64")


 Start 2020-02-19 18:01:26 -->> 85.126.106.144:25 (nihal.mag.eu) <<--

 rDNS (85.126.106.144): nihal.mag.eu.
```

```
Service set:      STARTTLS via SMTP

Testing protocols via sockets

SSLv2   not offered (OK)
SSLv3   offered (NOT ok)
TLS 1   offered (deprecated)
TLS 1.1 offered (deprecated)
TLS 1.2 offered (OK)
TLS 1.3 not offered and downgraded to a weaker protocol

Testing cipher categories

NULL ciphers (no encryption)      not offered (OK)
Anonymous NULL Ciphers (no authentication) not offered (OK)
Export ciphers (w/o ADH+NULL)     not offered (OK)
LOW: 64 Bit + DES, RC[2,4] (w/o export) offered (NOT ok)
Triple DES Ciphers / IDEA         offered
Obsolete: SEED + 128+256 Bit CBC cipher offered
Strong encryption (AEAD ciphers)  offered (OK)


Testing robust (perfect) forward secrecy, (P)FS -- omitting Null Authentication/Encryption,
    3DES, RC4

PFS is offered (OK)   ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-
    SHA ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA
Elliptic curves offered: prime256v1


Testing server preferences

Has server cipher order? no (NOT ok)
Negotiated protocol   TLSv1.2
Negotiated cipher     AES128-GCM-SHA256 -- inconclusive test, matching cipher in list
    missing, better see below
Negotiated cipher per proto (matching cipher in list missing)
   ECDHE-RSA-AES256-SHA:  SSLv3, TLSv1, TLSv1.1
   ECDHE-RSA-AES256-GCM-SHA384: TLSv1.2
No further cipher order check has been done as order is determined by the client


Testing server defaults (Server Hello)

TLS extensions (standard) "renegotiation info/#65281" "EC point formats/#11" "session ticket
    /#35" "heartbeat/#15"
Session Ticket RFC 5077 hint 300 seconds, session tickets keys seems to be rotated < daily
SSL Session ID support yes
Session Resumption    Tickets: yes, ID: yes
TLS clock skew        Random values, no fingerprinting possible
Signature Algorithm   SHA256 with RSA
Server key size       RSA 2048 bits
Server key usage      Digital Signature, Key Encipherment
Server extended key usage TLS Web Server Authentication, TLS Web Client Authentication
Serial / Fingerprints 94B98C3B5E188707B87E3226540AB8A8 / SHA1 971883
    B598B6A6D94BDC1965C728D406EE9F9DFF
                      SHA256 3
                          F8F389AA515D67A96BE0CF2B1E4B796B6855C49F5AA22AEE7C97DDD1BFFF400
Common Name (CN)      nihal.mag.eu
subjectAltName (SAN)  nihal.mag.eu www.nihal.mag.eu
Issuer                Don Dominio / MrDomain RSA DV CA (Soluciones Corporativas IP, SL from
    ES)
Trust (hostname)      Ok via SAN (same w/o SNI)
Chain of trust        Ok
EV cert (experimental) no
ETS/"eTLS", visibility info not present
Certificate Validity (UTC) 114 >= 60 days (2018-06-13 02:00 --> 2020-06-13 01:59)
# of certificates provided 4
Certificate Revocation List http://crl.usertrust.com/DonDominioMrDomainRSADVCA.crl
OCSP URI              http://ocsp.usertrust.com
OCSP stapling         not offered
OCSP must staple extension --
```

```
DNS CAA RR (experimental) not offered
Certificate Transparency yes (certificate extension)


Testing vulnerabilities

Heartbleed (CVE-2014-0160)      not vulnerable (OK), timed out
CCS (CVE-2014-0224)             not vulnerable (OK)
ROBOT                           not vulnerable (OK)
Secure Renegotiation (RFC 5746) supported (OK)
Secure Client-Initiated Renegotiation VULNERABLE (NOT ok), potential DoS threat
CRIME, TLS (CVE-2012-4929)      not vulnerable (OK) (not using HTTP anyway)
POODLE, SSL (CVE-2014-3566)     VULNERABLE (NOT ok), uses SSLv3+CBC (check TLS_FALLBACK_SCSV
     mitigation below)
TLS_FALLBACK_SCSV (RFC 7507)    Downgrade attack prevention supported (OK)
SWEET32 (CVE-2016-2183, CVE-2016-6329) VULNERABLE, uses 64 bit block ciphers
FREAK (CVE-2015-0204)           not vulnerable (OK)
DROWN (CVE-2016-0800, CVE-2016-0703) not vulnerable on this host and port (OK)
                                make sure you don't use this certificate elsewhere with
                                    SSLv2 enabled services
                                https://censys.io/ipv4?q=3
                                    F8F389AA515D67A96BE0CF2B1E4B796B6855C49F5AA22AEE7C97DDD1BFFF400
                                     could help you to find out
LOGJAM (CVE-2015-4000), experimental not vulnerable (OK): no DH EXPORT ciphers, no DH key
    detected with <= TLS 1.2
BEAST (CVE-2011-3389)           SSL3: ECDHE-RSA-AES256-SHA AES256-SHA ECDHE-RSA-AES128-SHA
    AES128-SHA DES-CBC3-SHA
                                TLS1: ECDHE-RSA-AES256-SHA AES256-SHA ECDHE-RSA-AES128-SHA
                                    AES128-SHA DES-CBC3-SHA
                                VULNERABLE -- but also supports higher protocols TLSv1.1
                                    TLSv1.2 (likely mitigated)
LUCKY13 (CVE-2013-0169), experimental potentially VULNERABLE, uses cipher block chaining (
    CBC) ciphers with TLS. Check patches
RC4 (CVE-2013-2566, CVE-2015-2808) VULNERABLE (NOT ok): RC4-SHA


Testing 370 ciphers via OpenSSL plus sockets against the server, ordered by encryption
    strength

Hexcode Cipher Suite Name (OpenSSL) KeyExch. Encryption Bits Cipher Suite Name (IANA/RFC)
-----------------------------------------------------------------------------------------------------------------

xc030 ECDHE-RSA-AES256-GCM-SHA384 ECDH 256 AESGCM 256
    TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
xc028 ECDHE-RSA-AES256-SHA384   ECDH 256 AES     256
    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
xc014 ECDHE-RSA-AES256-SHA      ECDH 256 AES     256    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
x9d   AES256-GCM-SHA384         RSA      AESGCM  256    TLS_RSA_WITH_AES_256_GCM_SHA384
x3d   AES256-SHA256             RSA      AES     256    TLS_RSA_WITH_AES_256_CBC_SHA256
x35   AES256-SHA                RSA      AES     256    TLS_RSA_WITH_AES_256_CBC_SHA
xc02f ECDHE-RSA-AES128-GCM-SHA256 ECDH 256 AESGCM 128
    TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
xc027 ECDHE-RSA-AES128-SHA256   ECDH 256 AES     128
    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
xc013 ECDHE-RSA-AES128-SHA      ECDH 256 AES     128    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
x9c   AES128-GCM-SHA256         RSA      AESGCM  128    TLS_RSA_WITH_AES_128_GCM_SHA256
x3c   AES128-SHA256             RSA      AES     128    TLS_RSA_WITH_AES_128_CBC_SHA256
x2f   AES128-SHA                RSA      AES     128    TLS_RSA_WITH_AES_128_CBC_SHA
x05   RC4-SHA                   RSA      RC4     128    TLS_RSA_WITH_RC4_128_SHA
x0a   DES-CBC3-SHA              RSA      3DES    168    TLS_RSA_WITH_3DES_EDE_CBC_SHA


Running client simulations via sockets

Android 8.1 (native)  TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256, 256 bit ECDH (P-256)
Android 9.0 (native)  TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256, 256 bit ECDH (P-256)
Android 10.0 (native) TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256, 256 bit ECDH (P-256)
Java 6u45             TLSv1.0 RC4-SHA, No FS
Java 7u25             TLSv1.0 ECDHE-RSA-AES128-SHA, 256 bit ECDH (P-256)
Java 8u161            TLSv1.2 ECDHE-RSA-AES256-SHA384, 256 bit ECDH (P-256)
Java 11.0.2 (OpenJDK) TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256 bit ECDH (P-256)
Java 12.0.1 (OpenJDK) TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256 bit ECDH (P-256)
```

```
OpenSSL 1.0.2e        TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256 bit ECDH (P-256)
OpenSSL 1.1.0l (Debian) TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256 bit ECDH (P-256)
OpenSSL 1.1.1d (Debian) TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256 bit ECDH (P-256)
Thunderbird (68.3)    TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256, 256 bit ECDH (P-256)

Done 2020-02-19 18:03:25 [ 124s] -->> 85.126.106.144:25 (nihal.mag.eu) <<--
```

Listing 10: TestSSL Ergebnis für `mizar.mag.eu`

```
> testssl.sh -t smtp nihal.mag.eu:25

###########################################################
   testssl.sh   3.0 from https://testssl.sh/

     This program is free software. Distribution and
          modification under GPLv2 permitted.
     USAGE w/o ANY WARRANTY. USE IT AT YOUR OWN RISK!

      Please file bugs @ https://testssl.sh/bugs/

###########################################################

 Using "OpenSSL 1.0.2-chacha (1.0.2k-dev)" [~183 ciphers]
 on gandalf:/home/fuero/Appz/testssl.sh/bin/openssl.Linux.x86_64
 (built: "Jan 18 17:12:17 2019", platform: "linux-x86_64")


 Start 2020-02-19 17:59:15 -->> 85.126.106.142:25 (mizar.mag.eu) <<--

 rDNS (85.126.106.142): mizar.mag.eu.
 Service set:      STARTTLS via SMTP

 Testing protocols via sockets

 SSLv2   not offered (OK)
 SSLv3   offered (NOT ok)
 TLS 1   offered (deprecated)
 TLS 1.1 offered (deprecated)
 TLS 1.2 offered (OK)
 TLS 1.3 not offered and downgraded to a weaker protocol

 Testing cipher categories

 NULL ciphers (no encryption)      not offered (OK)
 Anonymous NULL Ciphers (no authentication) not offered (OK)
 Export ciphers (w/o ADH+NULL)     not offered (OK)
 LOW: 64 Bit + DES, RC[2,4] (w/o export) offered (NOT ok)
 Triple DES Ciphers / IDEA         offered
 Obsolete: SEED + 128+256 Bit CBC cipher offered
 Strong encryption (AEAD ciphers)  offered (OK)


 Testing robust (perfect) forward secrecy, (P)FS -- omitting Null Authentication/Encryption,
     3DES, RC4

 PFS is offered (OK)   ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-
     SHA ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA
 Elliptic curves offered: prime256v1


 Testing server preferences

 Has server cipher order? no (NOT ok)
 Negotiated protocol   TLSv1.2
 Negotiated cipher     AES128-GCM-SHA256 -- inconclusive test, matching cipher in list
     missing, better see below
 Negotiated cipher per proto (matching cipher in list missing)
    ECDHE-RSA-AES256-SHA:  SSLv3, TLSv1, TLSv1.1
    ECDHE-RSA-AES256-GCM-SHA384: TLSv1.2
 No further cipher order check has been done as order is determined by the client


```

```
Testing server defaults (Server Hello)

TLS extensions (standard) "renegotiation info/#65281" "EC point formats/#11" "session ticket /#35" "heartbeat/#15"
Session Ticket RFC 5077 hint 300 seconds, session tickets keys seems to be rotated < daily
SSL Session ID support yes
Session Resumption    Tickets: yes, ID: yes
TLS clock skew        Random values, no fingerprinting possible
Signature Algorithm   SHA256 with RSA
Server key size       RSA 2048 bits
Server key usage      Digital Signature, Key Encipherment
Server extended key usage TLS Web Server Authentication, TLS Web Client Authentication
Serial / Fingerprints C1EF1BDD3E650999BE7A8114A4E7FC02 / SHA1 4418 A20B57042BE0FD24CBF81A5677FE63AFF784
                      SHA256 A2A65517606658C876BB107A89C102E8A6CDA718B6D78082B6B497E1457F7581
Common Name (CN)      mizar.mag.eu
subjectAltName (SAN)  mizar.mag.eu www.mizar.mag.eu
Issuer                Don Dominio / MrDomain RSA DV CA (Soluciones Corporativas IP, SL from ES)
Trust (hostname)      Ok via SAN (same w/o SNI)
Chain of trust        Ok
EV cert (experimental) no
ETS/"eTLS", visibility info not present
Certificate Validity (UTC) 114 >= 60 days (2018-06-13 02:00 --> 2020-06-13 01:59)
# of certificates provided 4
Certificate Revocation List http://crl.usertrust.com/DonDominioMrDomainRSADVCA.crl
OCSP URI              http://ocsp.usertrust.com
OCSP stapling         not offered
OCSP must staple extension --
DNS CAA RR (experimental) not offered
Certificate Transparency yes (certificate extension)


Testing vulnerabilities

Heartbleed (CVE-2014-0160)      not vulnerable (OK), timed out
CCS (CVE-2014-0224)             not vulnerable (OK)
ROBOT                           not vulnerable (OK)
Secure Renegotiation (RFC 5746) supported (OK)
Secure Client-Initiated Renegotiation VULNERABLE (NOT ok), potential DoS threat
CRIME, TLS (CVE-2012-4929)      not vulnerable (OK) (not using HTTP anyway)
POODLE, SSL (CVE-2014-3566)     VULNERABLE (NOT ok), uses SSLv3+CBC (check TLS_FALLBACK_SCSV mitigation below)
TLS_FALLBACK_SCSV (RFC 7507)    Downgrade attack prevention supported (OK)
SWEET32 (CVE-2016-2183, CVE-2016-6329) VULNERABLE, uses 64 bit block ciphers
FREAK (CVE-2015-0204)           not vulnerable (OK)
DROWN (CVE-2016-0800, CVE-2016-0703) not vulnerable on this host and port (OK)
                                make sure you don't use this certificate elsewhere with SSLv2 enabled services
                                https://censys.io/ipv4?q=A2A65517606658C876BB107A89C102E8A6CDA718B6D78082B6B497E1457F7581 could help you to find out
LOGJAM (CVE-2015-4000), experimental not vulnerable (OK): no DH EXPORT ciphers, no DH key detected with <= TLS 1.2
BEAST (CVE-2011-3389)           SSL3: ECDHE-RSA-AES256-SHA AES256-SHA ECDHE-RSA-AES128-SHA AES128-SHA DES-CBC3-SHA
                                TLS1: ECDHE-RSA-AES256-SHA AES256-SHA ECDHE-RSA-AES128-SHA AES128-SHA DES-CBC3-SHA
                                VULNERABLE -- but also supports higher protocols TLSv1.1 TLSv1.2 (likely mitigated)
LUCKY13 (CVE-2013-0169), experimental potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches
RC4 (CVE-2013-2566, CVE-2015-2808) VULNERABLE (NOT ok): RC4-SHA


Testing 370 ciphers via OpenSSL plus sockets against the server, ordered by encryption strength

Hexcode Cipher Suite Name (OpenSSL) KeyExch. Encryption Bits Cipher Suite Name (IANA/RFC)
-----------------------------------------------------------------------------------------------------------------
```

```
xc030 ECDHE-RSA-AES256-GCM-SHA384 ECDH 256 AESGCM 256
    TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
xc028 ECDHE-RSA-AES256-SHA384   ECDH 256 AES     256
    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
xc014 ECDHE-RSA-AES256-SHA      ECDH 256 AES     256    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
x9d   AES256-GCM-SHA384         RSA      AESGCM  256    TLS_RSA_WITH_AES_256_GCM_SHA384
x3d   AES256-SHA256             RSA      AES     256    TLS_RSA_WITH_AES_256_CBC_SHA256
x35   AES256-SHA                RSA      AES     256    TLS_RSA_WITH_AES_256_CBC_SHA
xc02f ECDHE-RSA-AES128-GCM-SHA256 ECDH 256 AESGCM 128
    TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
xc027 ECDHE-RSA-AES128-SHA256   ECDH 256 AES     128
    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
xc013 ECDHE-RSA-AES128-SHA      ECDH 256 AES     128    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
x9c   AES128-GCM-SHA256         RSA      AESGCM  128    TLS_RSA_WITH_AES_128_GCM_SHA256
x3c   AES128-SHA256             RSA      AES     128    TLS_RSA_WITH_AES_128_CBC_SHA256
x2f   AES128-SHA                RSA      AES     128    TLS_RSA_WITH_AES_128_CBC_SHA
x05   RC4-SHA                   RSA      RC4     128    TLS_RSA_WITH_RC4_128_SHA
x0a   DES-CBC3-SHA              RSA      3DES    168    TLS_RSA_WITH_3DES_EDE_CBC_SHA


Running client simulations via sockets

Android 8.1 (native)  TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256, 256 bit ECDH (P-256)
Android 9.0 (native)  TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256, 256 bit ECDH (P-256)
Android 10.0 (native) TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256, 256 bit ECDH (P-256)
Java 6u45             TLSv1.0 RC4-SHA, No FS
Java 7u25             TLSv1.0 ECDHE-RSA-AES128-SHA, 256 bit ECDH (P-256)
Java 8u161            TLSv1.2 ECDHE-RSA-AES256-SHA384, 256 bit ECDH (P-256)
Java 11.0.2 (OpenJDK) TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256 bit ECDH (P-256)
Java 12.0.1 (OpenJDK) TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256 bit ECDH (P-256)
OpenSSL 1.0.2e        TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256 bit ECDH (P-256)
OpenSSL 1.1.0l (Debian) TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256 bit ECDH (P-256)
OpenSSL 1.1.1d (Debian) TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256 bit ECDH (P-256)
Thunderbird (68.3)    TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256, 256 bit ECDH (P-256)

Done 2020-02-19 18:01:03 [ 114s] -->> 85.126.106.142:25 (mizar.mag.eu) <<--
```