# Bericht für *www.sternwarte.at*

10. Februar 2020

## Disclaimer

Es wurden für diesen Bericht nur öffentlich einsehbare Daten verwendet. Es wurden keine verschlüsselten oder durch Passwort geschützten Daten kopiert oder verwendet.

## 1 Zusammenfassung

Tests wurden im Zeitraum von 15. Jänner 2020 bis 3. 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. Dies ist meiner Ansicht nach mit der aktuellen Version der DSGVO nicht vereinbar. Auch der Admin-login ist unverschlüsselt und kann daher sehr einfach in einem überwachten Netzwerk abgefangen werden. Eine Verschlüsselung mit TLS1.2 oder höher in Kombination mit einem Zertifikat von Let's Encrypt löst dieses Problem effektiv.

2. Unauthentifiziert einsehbare Log-Datei, die Server-Fehler ausgibt:

   - Nicht gefundene Dateien,
   - Fehlercodes der CGI-Skripte
   - Fehler von anderen Webseiten, die auf diesem Host betrieben werden
   - Fehler des SMTP-Servers auf diesem Host

   Der unauthentifizierte Zugriff auf diese und weitere Dateien MUSS verhindert werden.

3. CGI Skripts können direkt ausgeführt werden und über die log-Datei können auch weitere Skripte gefunden werden. Auch hier sollten Maßnahmen getroffen werden, die den Zugriff nur über ausgefüllte Formulare zulassen.

4. Der FTP-Server ist auf dem Standardport verfügbar und es ist mutmaßlich verwundbar auf Bruteforce-Attacken. Einerseits sollte auch hier der Zugang verschlüsselt werden, etwa mit FTP over SSH. Gegen Bruteforce-Attacken helfen zusätzlich Fail2ban und Public Keys statt Passwörtern. Dies müssen die verwendeten Anwendungen aber unterstützen.

5. Die Webseite kann durch modifizierte URLs in der Darstellung verändert werden. Die Daten auf dem Server müssen dafür nicht verändert werden. Dazu muss die Webseite selbst angepasst werden, um nicht versehentlich aus dem vorgesehenen Arbeitsverzeichnis rauszufallen bzw. das Laden externer Frames zu verhindern.

6. Die verwendete Software (4D Webstar 2004) ist mittlerweile über 15 Jahre alt. Es gibt zwar keine bekannten Bugs, jedoch sollte es nicht schwierig sein, mit heutigen Mitteln welche zu finden. Deshalb wird dringend empfohlen, den verwendeten Software-Stack auf eine gut gewartete, aktuelle Basis zu stellen. Populäre Lösungen sind dafür ein aktuelles Linux mit Apache oder Nginx und den gewünschten Erweiterungen für Datenbanken und Skripting.

# 2 Methodik

In die Untersuchungen waren folgende Personen involviert:

- Robert Führicht
- Tobias Höller
- Michael Preisach

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

## 2.1 Informationsgewinnung

Ziel dieser Analyse ist 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)

# 3 Erkenntnisse

Die Analyse wird hier in die Services unterteilt, die auf dem Server zu finden sind.

## 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:

```
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. Mit diesem Argument kommen wir zu der Einschätzung, dass dringend eine Verschlüsselung der Kommunikation eingeführt werden muss, 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 `www.sternwarte.at/default.html?<url>` mit einer beliebigen URL aufzurufen. `http://www.sternwarte.at/default.html?https://jku.at` ruft dann die Startseite der JKU als Frame in der Vereinsseite auf. Des Weiteren 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.

**Handlungsempfehlung:**

- Variante 1: `default.html` darf nur eine definierte Liste an Links entgegennehmen - die der vorhandenen Subseiten (Whitelisting).
- Variante 2: Umbau von `default.html` in eine Seite mit nur einem Frame und das Laden von weiteren Frames per URL ganz abschalten.

### 3.1.3 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:

```
dirsearch -u www.sternwarte.at -E

|. _ _  _  _  _ _|    v0.3.9
(||| _) (/(|| (| )

Extensions: php, asp, aspx, jsp, js, html, do, action | HTTP method: get | \
  Threads: 10 | Wordlist size: 8673

Error Log: /home/fuero/.dirsearch/logs/errors-20-01-19_19-32-00.log

Target: www.sternwarte.at

[19:32:00] Starting:
[19:32:01] 200 -    2KB - /%3f/
[19:32:03] 200 -   21KB - /.DS_Store
[19:32:13] 200 -   46KB - /log/error.log
[19:32:30] 500 -  294B  - /ActiveDirectoryRemoteAdminScripts/
[19:34:27] 200 -   64KB - /favicon.ico
[19:35:02] 200 -  408KB - /log/error.log
[19:35:35] 500 -  294B  - /phpMyAdmin-2.11.5.1-all-languages/
[19:35:35] 500 -  294B  - /phpMyAdmin-2.11.7.1-all-languages-utf-8-only/
[19:35:35] 500 -  294B  - /phpMyAdmin-2.11.7.1-all-languages/
[19:35:35] 500 -  294B  - /phpMyAdmin-2.11.8.1-all-languages-utf-8-only/
[19:35:35] 500 -  294B  - /phpMyAdmin-2.11.8.1-all-languages/
[19:35:53] 200 -  118B  - /robots.txt
[19:36:14] 200 -   15KB - /start.html
[19:36:40] 500 -  294B  - /WebSphereSamples.Configuration.config

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 2 `.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. Im Anhang befindet sich eine Version von Anfang Februar. Es werden alle Dateiaufrufe am Server geloggt, die einen Rückgabewert ungleich 0 haben. Dieses Log bietet eine Vielzahl an Meta-Informationen, die ich hier nur beispielhaft aufzählen möchte:

- 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 (`www.kalendermanufaktur.at`, `www.baer.co.at`)

- 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 (`http://www.island-data.com/downloads/books/4D_Web_Companion.pdf`), weitere gültige Pfade gefunden:

- `/4dstats` - Abrufstatistiken
- `/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.
**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.
- Skripte dürfen nicht direkt per URL ohne Parameter aufgerufen werden können, es sie denn dieses Skript übernimmt auch die Darstellung des Formulars selbst.

### 3.1.4 Sehr alte Version des Servers

Laut unseren Recherchen ist der Webserver gepatcht, die letzten bekannten Bugs CVE 2004-0696 und CVE 2006-6131 scheinen hier gefixt zu sein. 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)