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 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
- 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)
- ftp 1.9.4
- OpenBSD netcat 1.206 Debian Patchlevel 1

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:

Listing 1: 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.

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 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 2: Mittels DirSearch Gefundene Endpoints

```
> 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 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 [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:

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

- `/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.

3.1.4 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.

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.

Nachtrag: Zumindest auf dem Server, der `www.sternwarte.at` ausliefert, ist eine Firewall aktiviert worden, die Anfragen auf diesen Port droppt (keine Antwort zurückschickt). Firewalls sollten solche Anfragen aber sauber abweisen (per Reject).

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 3: Mittels DirSearch Gefundene Endpoints

```
> 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. Bei der ersten Analyse dieses Services war nur eine unverschlüsselte Verbinudung 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 4: 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.
Diese Vermischung unterschliedlicher Services darf in einem Produktivsystem nicht passieren.

Handlungsempfehlung:

- Sofern der Betrieb unterschiedlicher Domains auf einem Host erforderlich ist, sollten zumindest alle Ressourcen auf dem Server (User, Dateien, Berechtigungen) möglichst weitgehend voneinander getrennt werden.

- Stand der Technik ist die Trennung der Webseiten auf Service-Ebene (zB 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.