Bericht für *www.sternwarte.at*

2. 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

Die Tests wurden im Zeitraum von 15. Jänner 2020 bis 31. Jänner 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. 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 Passwörtrn. 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.