Alte Verschlüsselungsverfahren über Plesk für nginx deaktivieren

https://nissel.it/index.php/2020/07/23/alte-verschluesselungsverfahren-ueber-plesk-fuer-nginx-deaktivieren/

Im default von plesk wird auch noch das veraltete TLSv1.1 zugelassen. Dies sollte längst nicht mehr genutzt werden. Eine immer noch sehr konservative Einstellung um z.B: auch noch den Internet Explorer 11 zu unterstützen ist die folgende:

```
plesk bin server_pref --update -ssl-protocols 'TLSv1.2 TLSv1.3'
```

Zusammen mit den ssl-ciphers ist dies die von Mozilla empfohlene Einstellung für einen öffentlichen Server:

```
plesk bin server_pref --update -ssl-ciphers 'ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384'
```

Die aktuelle Konfiguration kann über folgenden Befehl angezeigt werden:

```
plesk bin server_pref --show
```

Linux: Ubuntu 18.04.4
Plesk: Obsidian 18.0.28

Links

https://order.weblink.ch/knowledgebase/11/So-aktivieren-or-deaktivieren-Sie-eine-bestimmte-TLS-Version-in-Plesk-12.5-oder-hoher.html?language=english

https://wiki.mozilla.org/Security/Server_Side_TLS#Intermediate_compatibility_.28recommended.29

https://raymii.org/s/tutorials/Strong_SSL_Security_On_nginx.html