Warnmeldung der Zentralen Ansprechstelle Cybercrime (ZAC) MV:

Nach vorliegenden Information des Bundeskriminalamtes werden aktuell ein oder mehrere Unternehmen angegriffen, indem versucht wird Firewalls vom Typ „Cisco ASA“ zu infiltrieren.

Dabei sind nachfolgende IP-Adressen beim Angriff festgestellt worden:

23.155.24.9

176.111.174.123

194.61.120.214

185.157.162.26

185.81.68.75

Die Scans mit einem Default User Account und Login-Versuche auf die Cisco ASA wurden im Zeitraum vom 17.06. – 22.06.2023 (vormittags) registriert.

Sollten Sie eine solche Firewall im Einsatz haben, prüfen Sie die Logs nach den genannten IOC’s und passen Sie ggf. Ihr Regelwerk dazu an. (Blocken der IP- Adressen usw.)

Ergänzung:

Achten sie darauf, dass Sie die jeweils aktuellste Firmware für ihre Cisco ASA installiert haben. Informieren sie sich über die Sicherheitsinformationen des Herstellers.

(z.B. auch Cisco Security Advisory vom 08.06.2023/09.06.2023)