Info zur Attacke auf Infrastruktur im Rechenzentrum

Sehr geehrte Kundinnen und Kunden

Wie unser Upstream-Provider informiert, konnte die Attacke abgefiltert werden.
Die Attacke kam aus Russland und es wurden ganze IP-Adressblöcke attackiert. Durch die Attacke wurde auch teils das OSFP und BGP Routing in Mitleidenschaft gezogen, resp. die Sessions zwischen den Router wurde heruntergerissen. Die 10G und 100G Interface an den Border-Router (welche im Normalfall ca. 10-20% ausgelastet sind) waren voll am Anschlag, d.h. nahezu 100%ige Auslastung. Dadurch wurde der Traffic massiv eingeschränkt, resp. verunmöglicht.
Leider konnte auch unsere Backup-Anbindung (welche bei einem Ausfall einer Hardwarekomponente oder Unterbruch der Primären Leitung automatisch umschaltet) nichts ausrichten.

Der Upstream-Provider wird nun im Rechenzentrum Anpassungen an der Infrastruktur vornehmen (Anpassung und Verbesserung des Black-Holes Routing, Erweiterung mit Hardware, etc.) damit solche Attacken besser abgewehrt werden können. Leider ist kein Provider von solchen Attacken sicher und es kann jeden treffen (auch die grossen wie Swisscom, Sunrise, UPC, ..).
Auch die Angreifer sind nicht untätig und versuchen immer wieder aufs neue, Schutzmassnahen zu umgehen. Im Jahr 2021 wurden in der Schweiz rund 56800 Attacken auf Netzwerke registriert.

Wir danken für Ihr Verständnis.
GA Ossingen