SynoLocker: Virus verschlüsselt Netzwerkfestplatten und erpresst Lösegeld

Die Welle der Lösegeld-Trojaner hat Besitzer von Netzwerkfestplatten (*network attached storage*, kurz: NAS) erreicht. Mehrere Nutzer einer Diskstation vom NAS-Hersteller Synology berichten davon, dass der Lösegeld-Trojaner SynoLocker ihnen den Zugang zu ihren Daten versperrt. Nur gegen eine Zahlung von 0,6 Bitcoin, derzeit rund 260 Euro, würden sie wieder Zugriff auf ihre Daten bekommen. Ein Countdown warnt: Nach Ablauf dieser Zeit verdoppelt sich das Lösegeld. Betroffen sind Modelle, die Synology selbst unter der Bezeichnung Diskstation führt. Woher genau der Schädling stammt und wie er sich Zugang verschafft, ist bislang unklar.

"Alle wichtigen Dateien auf diesem NAS wurden mit starker Kryptografie verschlüsselt", lesen die betroffenen Nutzer, wenn sie über das Browser-Interface auf ihre Festplatte zugreifen wollen. Die auf der NAS gespeicherten Daten erscheinen zwar noch im Explorer, aber sie lassen sich nicht mehr öffnen - sie werden als korrupt oder beschädigt angezeigt.

Was also tun? Betroffene sollten auf keinen Fall auf die Lösegeldforderung eingehen, eine Zahlung garantiert keine Lösung, sondern nur weitere Nachforderungen.

Schlechte Nachricht auch für Kunden anderer Anbieter

Wer betroffen ist, heißt es von Synology, soll sofort seine Diskstation ausschalten und mit dem Support Kontakt aufnehmen, um eine weitere Verschlüsselung der Daten zu verhindern. Einzelne Nutzer berichten allerdings, dass ihnen eine etwas riskantere Wiederherstellung geholfen habe.

Leider gibt es derzeit keinen befriedigenden Schutz vor SynoLocker - und nur Netzwerk-Experten dürften die Notfall-Prozedur verstehen: Im Router sollte man erst mal jede Portweiterleitung an die Diskstation unterbinden, den Default-Port von der Standardeinstellung 5000 oder 5001 extern auf einen Zufallsport ändern und intern auf 5000 oder 5001 umleiten. Wer dringend externen Zugriff auf seine NAS braucht, sollte einen VPN-Zugang einrichten.

Wer die Laien-freundliche "EZ Internet"-Funktion von Synology zur Einrichtung der Kommunikation zwischen Diskstation und Router benutzte, hat seine NAS für SynoLocker empfänglich gemacht und sollte sie sofort vom Netz trennen, bis eine Lösung da ist.

Das könnte dauern. Derzeit ist nicht einmal klar, welche Versionen der Diskstation-Software DSM überhaupt betroffen sind: Auch wenn es derzeit so aussieht, dass nur ältere Versionen bis 4.3 die entsprechende Sicherheitslücke aufweisen (SynoLocker könnte ein Abkömmling einer anderen Diskstation-Malware sein), sollte man darauf derzeit nicht vertrauen, mit einer neuen DSM-Version geschützt zu sein.

Aber SynoLocker ist auch eine schlechte Nachricht für alle Kunden anderer Netzwerkspeicher. Denn dieser Lösegeld-Schädling zeigt das zunehmende Interesse von Internet-Kriminellen an den Netz-Festplatten. Sie sind oft allzu leichte Beute. Viele aktuelle

NAS-Systeme richten sich an Laien, ihre sichere Konfiguration ist aber selbst für Experten eine Herausforderung. Im schlimmsten Fall stehen diese Festplatten voller privater Daten, Videos und Bilder dem Internet offen. Gleichzeitig ist es nur extrem schwer herauszufinden, ob und wie man gefährdet ist.

Wer eine NAS verwendet und auf sie auch aus dem Internet zugreifen will, sollte sich also immer bewusst sein, dass das möglicherweise auch andere können.