

# Rettingsleck

Liebe Leserinnen, liebe Leser,

vor einigen Jahren nahm ich an einer Wildwasser-Fahrt im Schlauchboot teil.

Bei der Einweisung fiel mein Blick auf die uns zugedachten Boote, und ich staunte nicht schlecht: Im Boden klaffte jeweils ein großes Loch. „Damit das Wasser herauslaufen kann“, erläuterte uns der Bootsführer grinsend – und erntete amüsiert-verwirrte Blicke. Kaum im Wasser klärte sich das vermeintliche Wunder: Der Auftrieb der Luftkammern hielt die Boote so dicht an der Wasseroberfläche, dass das hereinschwappende Wasser tatsächlich durch das Loch abließ. Ohne das Loch hätte es sich im Boot gesammelt, bis jenes tief und schwerfällig im Wasser gelegen hätte.

An dieses Erlebnis musste ich im März des vergangenen Jahres denken, als ein Verschlüsselungstrojaner unter Verwendung des Open-Source-Ransomware-Kits EDA2 sich verbreitete. Dessen Autor, der türkische Sicherheitsforscher Utku Sen, der EDA2 zu Lehrzwecken entwickelt und den Quellcode – vielleicht ein wenig zu gutgläubig – veröffentlicht hatte, hatte eine Entschlüsselungs-Hintertür in EDA2 eingebaut. Sie sollte eine Rekonstruktion der Schlüssel ermöglichen, sollte das Kit von einem Hacker für die Entwicklung einer Ransomware verwendet werden. Tatsächlich kamen dadurch etwa 700 Betroffene ohne Lösegeldzahlung wieder an ihre unerwünscht verschlüsselten Daten.

Die Geschichte klingt nach einem guten Argument für das FBI, das seit einer Weile (nicht nur) von Apple den Einbau von Entschlüsselungs-Hintertüren fordert, um auf die Daten beschlagnahmter iPhones zugreifen zu können.

Aber wie beim Loch im Wildwasser-Schlauchboot gilt auch für die Informationssicherheit: Nicht jede Speziallösung eignet sich als generelles Konzept. Denn nachweislich ist ein Loch im Rumpf normalerweise kein geeigneter Sinkschutz – ganz im Gegenteil. Ebenso gilt uneingeschränkt: Ein Verschlüsselungsverfahren ist nur dann ein sicheres Verfahren, wenn es keine Hintertür besitzt. Denn eine Hintertür ermöglicht nicht nur Sicherheitsbehörden den Zugang zu verschlüsselten Daten.

Sichere Verschlüsselungsverfahren sind zwar bei einem Ransomware-Angriff zweifellos unerfreulich – sie sind jedoch nicht die Ursache des Problems. Der Angreifer könnte, anstatt die Daten zu verschlüsseln, auch mit der Löschung der Daten drohen, Zugangsdaten ausspähen und deren Missbrauch ankündigen oder Dateinamen und Sortierung verändern. Der Schaden wäre vergleichbar, ganz ohne Verschlüsselungsverfahren. Ursächlich ist auch nicht die Unvorsichtigkeit der Benutzer, die die „Klick-nicht-auf-Anhänge“-Empfehlungen ignorieren. Ursache sind allein die zahlreichen von Angreifern ausnutzbaren sicherheitskritischen Fehler in verbreiteter (Standard-) Software. Und, nicht zuletzt: Meist ist der von Ransomware verursachte Schaden deshalb so groß, weil die Betroffenen Schreibrechte für viel zu viele Daten und Verzeichnisse besitzen, obwohl höchstens Leserechte erforderlich wären – und oftmals auch die zugehörigen Backups zu alt sind für eine verlustarme Wiederherstellung.

Da liegen die eigentlichen Hausaufgaben. Verschlüsselungsverfahren hingegen dürfen keine Hintertüren besitzen. Wer das Gegenteil fordert, legt die Säge an den eigenen (Boots-)Rumpf.

Mit herzlichen Grüßen, Ihr



Dirk Fox