Verschlüsselungs-Trojaner: Schnelle Hilfe durch Emergency-Team

Theoretisch ist wohl jedem klar, dass auf die Forderungen von Erpressern nicht eingegangen werden sollte. Im praktischen Leben ist das nicht ganz so einfach: Mit Verschlüsselungs-Trojanern gelingt es Cyberkriminellen immer wieder, Unternehmen schwer zu schädigen. Dabei sind keineswegs nur große, namhafte Firmen betroffen, wie ein aktuelles Beispiel aus Norddeutschland zeigt. Dank einer IT-Sicherheits-Strategie sowie der Unterstützung durch den IT-Dienstleister mod IT Services gelang es, das befallene System schnell zu isolieren, größeren Schaden zu verhindern und das Problem ganzheitlich zu betrachten.

„Eine gute Vorbereitung, eine ganzheitliche Analyse verbunden mit einer schnellen Reaktion, sind die maßgeblichen Dinge, die bei der Abwehr eines Trojaners helfen", sagt Andreas Scharf, Security-Spezialist bei dem IT-Dienstleister mod IT Services. „Der Schaden, bestehend aus möglicherweise gezahltem Lösegeld, Datenverlust, Systemausfall und nicht zuletzt Image-Verlust kann schnell existenzgefährdend werden."

In den letzten Jahren machten Verschlüsselungs-Trojaner immer wieder Schlagzeilen. Waren bisher vor allem Privatleute betroffen, geraten nun vermehrt Unternehmen ins Visier der Hacker.

Schadensbegrenzung und umfassender Check

„Ein mittelständisches Produktionsunternehmen aus Norddeutschland wurde jüngst Opfer einer Verschlüsselungs-Trojaner-Attacke", erzählt Andreas Scharf. Mit einer Bewerbungs-E-Mail, die der User geöffnet hatte, war die Schadsoftware in die Unternehmens-Infrastruktur gelangt. Das Unternehmen ist dank der proaktiven Beratung durch mod IT Services für derartige Fälle sensibilisiert und arbeitet mit einem umfassenden IT-Security-Konzept.

Schon die Erst-Analyse des Supports ließ einen Trojaner-Befall vermuten. „An dieser Stelle mussten wir sofort und nachhaltig handeln, um den Schaden so gering wie möglich zu halten", erläutert Andreas Scharf. Das Emergency-Team von mod IT Services übernahm alle technischen und organisatorischen Maßnahmen: Es isolierte das befallene System, um Übergriffe auf die Server zu verhindern, sicherte Beweise und startete sofort mit der Fehleranalyse. „Wir mussten zunächst den sogenannten ‚Patient Null' ermitteln – das System, zu dem die nun verschlüsselten Daten gehören. Nach einem umfassenden Check der restlichen Infrastruktur konnten alle anderen User schnell wieder arbeiten." Größerer finanzieller Schaden oder Datenverlust konnte so verhindert werden.

Sich nicht überraschen lassen

„Einen Verschlüsselungs-Trojaner einzuschleusen ist eine Straftat", sagt Andreas Scharf. „Betroffene sollten den Vorfall deshalb dem BSI melden." Im konkreten Fall des norddeutschen Mittelständlers übernahm mod IT Services die Zusammenarbeit mit der Polizei und erntete dafür die Anerkennung der Beamten: „Wir haben der Polizei die notwendigen Informationen zusammengestellt und so aufbereitet, dass die Fahnder schnell die Arbeit aufnehmen konnten." Das befallene System wurde schließlich neu aufgesetzt, das aktuelle Backup eingespielt.

Auf die Frage, was er Unternehmen im Kampf gegen Verschlüsselungs-Trojaner empfehlen würde, antwortet Andreas Scharf: „Man kann solche Angriffe nie hundertprozentig verhindern oder vorhersehen, aber man kann vorbereitet sein. Entsprechend sensibilisierte Mitarbeiter und ein ganzheitliches Security-Konzept sind die Basis und nicht zuletzt die professionelle Unterstützung durch das mod IT Services Emergency-Team, wenn Schadware festgestellt wird."

Andreas Scharf,
Security-Spezialist,
mod IT Services