Ransomware per Fernwartung

Cyber-Kriminelle verbreiten Ransomware – Verschlüsselungstrojaner – über Fernwartungstools. Angriffsziele der Täter sind vorwiegend kleine und mittlere Unternehmen.

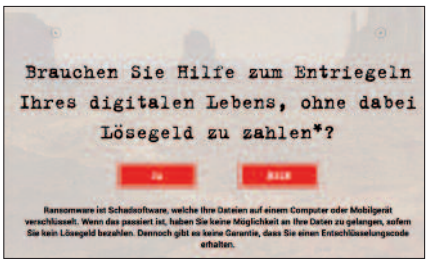
Die Schadsoftware wird laut Experten des *Cybercrime-Competence-Centers (C4)* im Bundeskriminalamt derzeit bevorzugt über Fernwartungstools wie Remote-Desktop-Protokoll-Schnittstellen (RPD) in die Netzwerke eingespielt und verschlüsselt diese. RDP-Schnittstellen werden zum Steuern eines entfernten Computers und Darstellen dessen Bildschirminhaltes benötigt, etwa von einem Außendienstmitarbeiter einer Firma oder einem IT-Techniker.

Cyber-Kriminelle verbreiten über Fernwartungstools Verschlüsselungstrojaner und fordern von Unternehmen Lösegeld.

Die Angriffsziele der Täter sind vorwiegend kleine und mittlere Unternehmen und deren mangelhaft oder mit zu einfachen Passwörtern abgesicherte Schnittstellen. Die Zugangsdaten werden mit spezieller Software geknackt, um in die Systeme der Opfer einzudringen und die Daten zu verschlüsseln. Nach der Infizierung wird auf den betroffenen Computersystemen der Opfer eine Nachricht mit den Instruktionen der Erpresser zur Überweisung des Lösegeldes hinterlegt. Auch die Geldforderungen der Täter haben sich geändert. Früher wurden von den Tätern fixe Geldbeträge für die Entschlüsselung eines Gerätes verlangt. Nun wird nach vorheriger Abschätzung der finanziellen Möglichkeiten der Opfer die Höhe des Lösegeldes individuell abgestimmt. Es sind Forderungen von bis zu 30.000 Euro bekannt.

Ransomware ist ein Sammelbegriff für Schadsoftware, die dafür entwickelt wird, elektronische Daten und Systeme zu verschlüsseln, sodass diese nicht mehr verwendet werden können. Für die Entschlüsselung wird dann Lösegeld (englisch: ransom) erpresst, meistens in Form des virtuellen Zahlungsmittels *Bitcoin* oder durch Prepaid-Karten. Beide Zahlungsformen sind anonym und erschweren die Strafverfolgung. Betroffen sind sowohl Privatpersonen als auch Unternehmen, Behörden und sonstige Organisationen.

Sonderkommission. Aufgrund des Anstieges der Zahl der Erpressungen durch Ransomware wurde Anfang Juni 2016 die Sonderkommission (Soko) Clavis im C4 des BK eingerichtet. Zurzeit besteht das Team aus fünf Mitarbeiterinnen und Mitarbeitern. Diese übernehmen alle bundesweit angezeigten Ransomware-Fälle. Diese Kriminalitätsform erfordert aufgrund der Internationalität und Komplexität eine zentrale Bearbeitung, damit einzelne Straftaten einer Serie oder einer Tätergruppe zugeordnet werden können. Die Ermittler der Soko bearbeiten etwa fünf Anzeigen pro Woche. Im Vorjahr waren es durchschnittlich 20 Anzeigen pro Woche.



Hilfe bei Entschlüsselungsprogrammen gibt es unter *www.nomoreransom.org.*

Hilfe bei Entschlüsselungsprogrammen. Die Internetseite *www.nomoreransom.org* ist von Europol in Kooperation mit dem Bundeskriminalamt sowie privaten und exekutiven Partnern entstanden und unterstützt Opfer von digitaler Erpressung bei der Wiederherstellung ihrer Daten. Die Plattform ist in 14 Sprachen verfügbar und bietet unterschiedliche Entschlüsselungsprogramme gratis an. Auf der Seite können Betroffene Informationen einholen.

Tipps zur Kriminalprävention:

- Zugangsdaten regelmäßig ändern, unterschiedliche und komplexe Passwörter mit Groß-, Kleinbuchstaben und Sonderzeichen für verschiedene Accounts und Anwendungen verwenden.
- Keine Standard-Benutzerkennungen verwenden, wie beispielsweise *user1* oder *Admin001*.
- Firewalls aktivieren.
- Zugangsmöglichkeiten unter Verwendung von IP-Whitelisting einschränken. Die „weiße Liste“ bezeichnet ungefährliche E-Mail-Adressen, Personen oder URLs.
- Prüfen, ob ein Fernzugriff via RDP-Zugang überhaupt benötigt wird. Falls nicht, diese Funktion ausschalten.
- Das Back-up-Medium nach der Sicherung vom System trennen und Share-Links zu Back-up-Servern nach erfolgter Sicherung auflösen.
- Benutzerrechte der jeweiligen User so weit wie möglich beschränken und nur unter dem Administrator-Account arbeiten, wenn dies unbedingt notwendig ist.
- Wer Opfer geworden ist, kann das in jeder Polizeidienststelle anzeigen.

www.bundeskriminalamt.at

FOTO: RAWPIXEL.COM/FOTOLIA