Weltweite Raubzüge

Immer öfter werden Daten auf Rechnern von Unternehmen und Heimanwendern mit Schadsoftware verschlüsselt. Die Polizei warnt davor, Lösegeld für die „Entschlüsselung“ zu zahlen.

Unbekannte Angreifer verschlüsselten im Mai 2017 weltweit Daten auf etwa 200.000 Rechnern mit einer Ransomware namens „WannaCry“ und forderten für die Freigabe der Daten 300 Dollar in der Digitalwährung Bitcoin. Bei der Verbreitung der Schadsoftware nutzten die Angreifer eine Sicherheitslücke im Betriebssystem *Windows*. Laut *Microsoft* seien bereits Updates bereitgestellt worden, viele Nutzer hätten sie jedoch nicht installiert. Nach Angaben von Europol waren PCs in mindestens 150 Ländern von den Angriffen betroffen, darunter Österreich.

Ransomware ist eine Schadsoftware, die elektronische Daten und Systeme verschlüsselt, sodass diese nicht mehr verwendet werden können. Für die Entschlüsselung der Daten verlangen die Täter Lösegeld (engl. „Ransom“), meist in Form des virtuellen Zahlungsmittels Bitcoin oder mit Prepaid-Karten. Die Verschlüsselungssoftware wird über präparierte E-Mails, durch Sicherheitslücken in Webbrowsern oder durch unbewusstes Herunterladen aus dem Internet verbreitet. Betroffen sind sowohl Privatpersonen, Unternehmen, Behörden und sonstige Organisationen.

Schutz vor Ransomware: Daten sollten regelmäßig gesichert werden.

Maßnahmen. Sind die Daten auf einem Rechner bereits gesperrt, sollten betroffene Nutzer den Bildschirm mit der Erpressungsnachricht fotografieren und bei der Polizei Anzeige erstatten. Strafverfolgungsbehörden in Österreich und anderen Ländern warnen davor, den unbekannten Erpressern Lösegeld zu zahlen: Es gebe keine Garantie, dass die Daten auf infizierten Computern freigegeben werden. Wer regelmäßig Daten über ein Back-up-System sichert, kann die Daten wieder auf den Rechner spielen, nachdem er neu aufgesetzt worden ist. Für einige Arten von Ransomware gibt es Entschlüsselungswerkzeuge. Die Initiative *No More Ransom* stellt auf ihrer Webseite *www.nomoreransom.org* neben einer Übersicht über diese Werkzeuge die Möglichkeit bereit, anhand der neuen Dateiendung festzustellen, welcher Trojaner für die Verschlüsselung verantwortlich ist.

Soko „Clavis“. Alle österreichischen Ransomware-Fälle werden von einer Sonderkommission im Cybercrime-Competence-Center des Bundeskriminalamts übernommen. Die Ermittler der Soko „Clavis“ bearbeiten etwa 20 neue Fälle pro Woche. Zwischen Juni und Dezember 2016 waren es 446 Fälle, zwischen Jänner und Ende März 2017 259. Immer öfter sind Unternehmen im Visier der Kriminellen. Der Schaden, der Firmen durch einen Ransomware-Angriff entstehen würde, sei der Grund dafür, dass immer mehr Unternehmen Lösegeld zahlen. Zudem seien Angriffe auf Firmen für die Cyber-Kriminellen lukrativer als auf Heimanwender.

Darknet. Die Soko Clavis ermittelte 2016 in Österreich gegen einen Tatverdächtigen, der mit Hilfe von im Darknet gekaufter Schadsoftware Daten von Unternehmen verschlüsselte und für die Entschlüsselung Geld forderte.

Auf die Spur des Verdächtigen kamen die Ermittler durch eine Anzeige eines oberösterreichischen Unternehmers, dessen Firmendaten durch die Verschlüsselungssoftware unbrauchbar gemacht worden waren. Dem oberösterreichischen Unternehmen entstand durch den Angriff ein Schaden von 3.000 Euro. Das Lösegeld wurde nicht gezahlt, da die Firma die nötigen Sicherungskopien der Firmendaten durchgeführt hatte.

Bei Hausdurchsuchungen in Linz und im Nahbereich von Wien stellten die Ermittler zahlreiche Computer und Datenträger sicher. Der mutmaßliche Täter wurde angezeigt und bestritt die Taten. *S. L.*

RANSOMWARE

Präventionstipps

- Regelmäßig Sicherheits-Updates bzw. Patches für Betriebssystem und Software installieren.
- Vorsicht beim Erhalt von E-Mails, deren Absender man nicht kennt oder von dem man keine Nachrichten erwartet.
- Absenderadresse kontrollieren, auf Ungereimtheiten achten. Bei Weblinks den Mauszeiger über den entsprechenden Link legen, ohne diesen zu aktivieren. Sollte die Weblink-Adresse aufscheinen, kontrollieren, ob sie zu einem vertrauenswürdigen Absender gehört.
- Auf die Schreibweise und Rechtschreibung von E-Mail-Nachrichten achten. Kriminelle verwenden Übersetzungsprogramme, was die Bedrohung leichter erkennbar macht.
- Keine unbekannten Dateianhänge öffnen, ohne sich vorher von deren Unbedenklichkeit zu überzeugen. Bei übermittelten Rechnungen besonders vorsichtig sein.
- Zugangsdaten regelmäßig ändern, unterschiedliche und komplexe Passwörter für verschiedene Accounts und Anwendungen verwenden.
- Das Back-up-Medium nach der Sicherung vom System trennen und Share-Links zu Back-up-Servern nach der Sicherung wieder auflösen, um ein Übergreifen durch Schadsoftware zu verhindern.
- Benutzerrechte der jeweiligen User so weit wie möglich beschränken und nur unter dem Administrator-Account arbeiten, wenn dies unbedingt notwendig ist.

FOTO: SURADECH_K/FOTOLIA