Augsburger Allgemeine | Wirtschaftsraum Augsburg | NUMMER 156 FREITAG, 10. JULI 2015

Ihre Gegner sind Trojaner im Computer

EDV Wie Augsburger Fachinformatiker gefährliche Erpressersoftware austricksen wollen

VON STEFANIE SCHÖNE

Wer am Computer arbeitet, kennt eine Sorge: Ein Trojaner macht sich breit. Ein Bilddarstellungsprogramm öffnet sich wie von Geisterhand und zeigt einen langen Text mit bunten Buchstaben: „Cryptowall 3.0 hat alle Dateien auf Ihrem Computer verschlüsselt. Gehen Sie zu diesem Server… und bezahlen Sie 1000 Dollar für die Freigabe. Auf dem Server ist ein persönlicher Schlüssel für Sie hinterlegt… Bezahlen Sie mit Bitcoins." Dokumente – ob Textdateien, Bilder, Powerpoint-Präsentationen, Filme – zeigen beim Öffnen nur noch fünf Zeilen kryptischer Zeichen. Nichts geht mehr.

Eine Entschlüsselung, an der derzeit weltweit getüftelt wird, hält auch das Augsburger Systemhaus CT Computer für nahezu unmöglich. Fachinformatiker Manuel Christlieb: „Es handelt sich hier um eine 2048-Bit-Verschlüsselung. Das ist Militärstandard, kaum zu knacken." Er fand jedoch einen anderen

Matthias Pham (links) und Manuel Christlieb vor dem Systemhaus CT Computer in Augsburg. Foto: Stefanie Schöne

Weg, Cryptowall 3.0 auf einem kürzlich befallenen Kundinnen-PC auszutricksen. „Tief im System legen Windows-Betriebssysteme unbemerkt und kontinuierlich sogenannte Schattendateien an, auf die der Verschlüsselungstrojaner offenbar nicht zugreift", erklärt er. Er investierte drei Stunden mit Tests, Recherchen und Nachdenken, bis er die Freeware „Shadow Explorer" auf den gekaperten PC lud. Matthias Pham, Fachinformatiker in Ausbildung bei CT Computer, überwachte den Suchprozess: Die Software entdeckte auf dem Windows-Vista-Rechner von allen Dokumenten Schattendateien und holte sie ans Licht. Christlieb ist selbst etwas überrascht: „Dass eine solche Notoperation nach Cryptowall 3.0 erfolgreich sein könnte, war eigentlich unwahrscheinlich." Er empfiehlt kleinen Unternehmen und Selbstständigen eine professionelle Backup-Software, die gespeicherte Sicherungskopien vor Cyberkriminellen schützt.

Die Dateien werden verschlüsselt

Zum Verständnis: Anders als die meisten sogenannten Ransomware-Schädlinge, die eine vordefinierte Liste von Dateitypen chiffrieren, verschlüsselt die derzeit kursierende Version Cryptowall 3.0 alle Dateien auf dem infizierten Rechner und auch Daten auf angeschlossenen externen Festplatten. Der Trojaner lässt sich zwar mit einem Freewaretool wie „Malwarebytes Anti Malware" rückstandslos entfernen. Doch die Dateien rettet das nicht. Laut jüngstem Bericht des Sicherheits-Spezialisten McAfee ist die Verbreitung von Ransomware (Erpressersoftware) im Vergleich zu den ersten drei Monaten dieses Jahres um 165 Prozent gestiegen. Autoren solcher Software und Plattformbetreiber, die für Provision und Umsatzbeteiligung das automatische Generieren solcher Schadprogramme anbieten, verstecken ihre Server im anonymen Netzwerk Tor. Gefährdet sind Rechner mit einem Windows-Betriebssystem. Antivirenprogramme erkennen den Eindringling nicht. Die Zentrale Ansprechstelle Cybercrime, die 2014 im Bayerischen Landeskriminalamt ihre Arbeit aufnahm, ist für Prävention zuständig. Vorsicht beim Surfen und bei E-Mail-Anhängen wird empfohlen.

Das rät die Polizei

- Öffnen Sie niemals ungeprüft Dateianhänge, ganz gleich, ob es sich um scheinbar ungefährliche Dateien wie Bilder, Dokumente oder sonstige Dateien handelt. Wenn Sie sich unsicher sind, fragen Sie beim Absender nach.
- Klicken Sie niemals auf Links in unaufgefordert zugesandten E-Mails. Diese könnten Sie auf infizierte Webseiten leiten, die zu einem unbemerkten Download des Schadcodes führen.
- Seien Sie in Sozialen Netzwerken kritisch mit dem Klick auf angeblich aufsehenerregende Videos oder Mitteilungen – auch wenn diese von Freunden empfohlen wurden.
- Installieren Sie regelmäßig vom Hersteller bereitgestellte Sicherheitsupdates für Ihr Betriebssystem und die installierten Programme.
- Setzen Sie ein Virenschutzprogramm ein und aktualisieren Sie dieses regelmäßig.