Ransomware

Als Ransomware (engl. ransom = Lösegeld) werden Lösegeld-Trojaner bezeichnet, also Schadprogramme, die einzelne Dateien oder die komplette Festplatte eines Computers sperren. Für die Freigabe wird vom Besitzer Geld gefordert.

Das Vorgehen

Die Erpressung via Internet erfolgt mit Hilfe von sogenannten Lösegeld-Trojanern. Die Ransomware wird unbemerkt über das Anklicken eines Links oder das Öffnen einer Datei auf einen Computer geschleust. Beim nächsten Start des Rechners ist dieser für die weitere Benutzung gesperrt. Auch der Taskmanager wird blockiert. Es erscheint eine Meldung, in der der Nutzer aufgefordert wird, per anonymer Überweisung ins Ausland Geld zu zahlen, damit die Daten wieder freigeschaltet werden. Selbst wenn man dieser Forderung nachkommt, geschieht dies in der Regel allerdings nicht.

Historie und Beispiele

Die Erpressung von Geld durch Verschlüsselung beziehungsweise Sperrung von Computerdaten wurde bereits Ende der 1980er Jahre eingesetzt. Damals wurden die Daten noch mit einer infizierten Diskette verschlüsselt. Heute werden die Trojaner von Computernutzern unbewusst heruntergeladen, indem sie einen E-Mail-Anhang, eine Filesharing-Datei oder einen Link in Sozialen Netzwerken anklicken. Bekannte Beispiele für Ransomware sind:

- BKA- oder Bundespolizei-Trojaner (Dem Nutzer wurde vorgegaukelt, der PC sei von einer Polizeibehörde verschlüsselt worden.)
- Ransom.AN (In einer vermeintlich von Microsoft stammenden Meldung wird unterstellt, man nutze eine illegale Windows-Kopie.)
- Gema-Trojaner (Die Meldung, die aussieht als stamme sie von der deutschen Verwertungsgesellschaft Gema, lastete Nutzern an, gegen das Urheberrecht verstoßen zu haben.)
- GVU-Trojaner und Varianten davon (Der vermeintliche Absender, die Gesellschaft für Verfolgung von Urheberrechtsverletzungen oder andere, wirft dem Nutzer vor, er habe gegen das Urheberrecht verstoßen oder unterstellt ihm schwerste kriminelle Aktivitäten wie den Besitz von Kinderpornographie oder Terrorismus.)

Hilfe für Betroffene

Wer Opfer von Ransomware geworden ist, findet beim Anti-Botnetz-Beratungszentrum sowie beim Bundeskriminalamt und beim Bundesamt für Sicherheit in der Informationstechnik (BSI) Hilfe und nützliche Tipps. Vorbeugend empfehlen BKA und BSI, das Betriebssystem, die Antiviren-Software sowie alle verwendeten Programme stets auf dem neuesten Stand zu halten, also ständig zu aktualisieren.

Siehe auch:
Malware/Spyware
Keylogger

Zurück