

.04 Security

Sicherheit im Unternehmen



.04 Malware-Spammer spielen Internet-Polizei

.....Frank Ziemann * 18|9|2008



Angst ist ein schlechter Ratgeber und deshalb ein gut geeignetes Mittel, um jemanden zu unbedachtem Handeln zu verleiten. Das haben sich offenbar auch Online-Kriminelle gedacht und verschicken seit ein paar Tagen Mails, in denen sie den Empfängern mit der Sperrung ihres Internet-Zugangs drohen. Sie geben sie als "Internet Service Provider Consortium" aus und behaupten die Rechte von Autoren und Künstlern zu schützen. Sie werfen den Empfängern angebliche "illegale Aktivitäten" vor.

Die Mails kommen mit dem Betreff "Your internet access is going to get suspended" und der Absenderangabe "ICS Monitoring Team". Sie fordern die Empfänger auf ihre Downloads von urheberrechtlich geschütztem Material zu stoppen, sonst werde der Internet-Zugang gesperrt. Da viele der Empfänger schon einmal etwas aus dem Internet herunter geladen haben dürften, das eventuell in diese Kategorie fällt, könnte sie ein solcher Schreck in der Morgenstunde zum Öffnen des Mail-Anhangs verleiten.

Laut Mail-Text soll der Anhang einen Bericht über die Aktivitäten des Empfängers in den letzten sechs Monaten enthalten. Der Anhang besteht aus einem 33 KB großen ZIP-Archiv mit dem Dateinamen "user-EA49943X-activities.zip". Darin steckt eine gleichnamige EXE-Datei. Es handelt sich dabei um ein Trojanisches Pferd. Es legt im Verzeichnis Windows\System32 die Dateien "cabpck.dll" und "knlcab.sys" an und löscht sich dann selbst.

Die beiden Dateien sind Schädlinge aus der Goldun-Familie. Die Datei knlcab.sys ist ein so genanntes Rootkit, also eine Tarnkappe für andere Malware. Die andere Datei ist ein Key-Logger. Der Schädling soll die Zugangsdaten zum Online-Bezahlungssystem "E-Gold" ausspionieren.