Betrüger ergaunern Millionen mit einer Schadsoftware, die als „Polizeivirus“ oder „BKA-Trojaner“ bekannt ist.

Abzocke mit dem „Polizei-Virus“

Immer wieder machen Internetnutzer Erfahrung mit dem „Polizei-Virus“, einer Schadsoftware, die den Bildschirm sperrt. Für dessen Freigabe verlangen Kriminelle Geld.

Plötzlich ist der Bildschirm gesperrt und eine Seite sichtbar, auf der behauptet wird, dass der Computer an einer strafbaren Handlung beteiligt gewesen wäre. Ein Logo mit dem Schriftzug Polizei oder Bundeskriminalamt vermittelt den Eindruck, die Polizei stehe dahinter. Der Computernutzer wird aufgefordert, für die Freischaltung des gesperrten Betriebssystems Geld über Internet-Bezahldienste wie *Paysafe, uKash* oder *MoneyPak* zu überweisen. Die Bildschirme bleiben oft gesperrt, auch wenn Geld überwiesen wird. Die Polizei rät Betroffenen, nicht zu bezahlen. Auf *www.bka-trojaner.de* und *www.botfrei.de* gibt es Hinweise, wie man den Bildschirm entsperren und die Schadsoftware loswerden kann.

Internetnutzer können sich den „Polizei-Virus“ von allen Seiten holen, auf denen sie surfen; hauptsächlich jedoch von Porno-Seiten oder von Plattformen, von denen man illegal Programme, Filme, Musik und dergleichen herunterladen kann. Solche Seiten können mit einem Erpressungsprogramm (Ransomware) infiziert sein, das man unbemerkt auf seinen Rechner lädt, wenn man mit dem Cursor zum Beispiel über ein Werbebanner fährt. Die Schadsoftware wird von herkömmlichen Antiviren-Programmen nicht erkannt, installiert sich selbstständig auf dem *Windows*-Betriebssystem des Rechners und legt Funktionen des PCs lahm. Es gibt verschiedene Versionen davon. Im schlimmsten Fall können neben der Sperre des Betriebssystems Daten verschlüsselt werden. Laut IT-Experten des Bundeskriminalamts ist es derzeit nicht möglich, derart verschlüsselte Dateien wieder herstellen. Deshalb sollte man von allen Dateien Sicherheitskopien herzustellen. Um den „Polizei-Virus“ endgültig loszuwerden, empfehlen Experten, das Betriebssystem neu aufzusetzen. Hilfe dafür gibt es im Forum *www.botfrei.de*.

Operation Ransom. Der Polizei in Spanien gelang es im Februar 2013 mit Unterstützung von Europol und Interpol, eines der größten Netze von Cyberkriminellen in der Welt auszuheben. Bei Razzien in der Provinz Malaga wurden zehn Verdächtige wegen Betrugs und Geldwäsche festgenommen: Sechs Russen, zwei Ukrainer und zwei Georgier. Der Kopf der Bande, ein 27-jähriger Russe, war schon im Dezember 2012 in Dubai verhaftet worden. Die Täter hatten laut Europol bei einer durchschnittlichen Zahlung von 100 Euro für die Aufhebung der Bildschirmsperre mehrere Millionen Euro erbeutet. Ein Großteil des Geldes soll nach Russland transferiert worden sein. Die Verdächtigen nutzten zur Geldwäsche elektronische Bezahldienste, virtuelle Währungen und Online-Gaming-Portale. Die infizierten Rechner wurden auch nach Kreditkartendaten durchstöbert. Der Code für die Schadsoftware soll in einem Franchise-System vertrieben worden sein. Tausende Internet-Nutzer wurden seit dem ersten Auftreten der Schadsoftware im Mai 2011 Opfer dieser „digitalen Erpressung“. In Österreich gab es bei der Staatsanwaltschaft Klagenfurt, die das Verfahren für ganz Österreich führt, bis März 2013 etwa 3.000 Anzeigen. Die Dunkelziffer ist hoch.

Zum Schutz des Computers vor dem „Polizei-Virus“ raten Cybercrime-Experten des Bundeskriminalamts:

- Systemupdates durchführen;
- Firewall und Virenschutz installieren und aktuell halten;
- Programmupdates von einschlägigen Programmen wie *Adobe Flash Player* und *Java* durchführen;
- verdächtige oder unbekannte Mails löschen, ohne zuvor darin enthaltene Links anzuklicken oder Anlagen zu öffnen.

Siegbert Lattacher

Fotos: Archiv