BSI und Polizei weisen auf besonders aggressive Schadsoftware hin

Erpresser missbrauchen offizielle Logos und erpressen Geldbeträge durch Verschlüsselung von PCs – Vollständige Wiederherstellung von betroffenen Rechnern selten möglich.

Bonn / Stuttgart, 31.07.2012.
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Polizeiliche Kriminalprävention der Länder und des Bundes weisen auf eine neue und besonders dreiste Variante von Schadsoftware hin. Kriminelle versuchen damit, Geld von PC-Besitzern zu erpressen. Bei den Attacken werden die PCs von Betroffenen so verschlüsselt, dass eine vollständige Wiederherstellung aller Daten oft nicht möglich ist. Die Polizei und das BSI zeigen Schutzempfehlungen auf und geben konkrete Handlungshilfen für den Ernstfall.

Die neueste Variante der Schadsoftware, der so genannte Windows-Verschlüsselungs-Trojaner, wird bundesweit über Spam-Mails verbreitet. Die angeschriebenen Personen werden beispielsweise im Namen einer Staatsanwaltschaft im Bundesgebiet dazu verleitet, die beigefügten Anhänge zu öffnen. Doch schon beim Öffnen des Anhangs wird der PC verschlüsselt und Geld gefordert. Auch nach Bezahlen der Forderung, in der Regel 100 Euro per Paysefecard oder 50 Euro per Ukash, wird die Sperrung nicht aufgehoben. Vielmehr sind sämtliche Dateien auf dem PC so verschlüsselt, dass auch die Wiederherstellung mit einer Rettungs-CD ("Rescue Disk") nur teilweise erfolgreich ist.

Immer wieder tauchen neue Varianten dieser bereits seit 2011 bekannten Schadsoftware auf. Um Glaubwürdigkeit vorzutäuschen, missbrauchen die Erpresser offizielle Logos von bekannten Unternehmen und Behörden. So wurden bereits Logos des Bundeskriminalamts, der Bundespolizei oder verschiedener Softwareunternehmen zu betrügerischen Zwecken verwendet. Eine andere Variante der Schadsoftware täuscht die Nutzer mit den Logos des BSI und der Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e.V. (GVU).

Kritisch sein und Anzeige erstatten

"Das BSI sowie die anderen Behörden und Unternehmen sind nicht Absender dieser Meldungen", betont BSI-Präsident Michael Hange. *"Wir rechnen mit einer weiteren Zunahme relevanter Schwachstellen und neuer Schadprogramme beziehungsweise deren Varianten"*, führt Hange weiter aus. *"Insofern wird die Gefährdungslage tendenziell eher noch zunehmen. Mit Standard-Schutzmaßnahmen lassen sich aber auch im privaten Umfeld bereits 80 Prozent aller Cyber-Angriffe abwehren."* Anwender sollten daher stets auf aktuelle Virenschutzprogramme achten, sowie Sicherheitsupdates für die von ihnen genutzte Software einspielen, sobald diese von den Herstellern bereitgestellt werden. Die Programme der im Markt bekannten Antivirensoftware-Hersteller erkennen in der Regel die bekannten Varianten der Erpressungsschadsoftware und hindern sie daran, den Rechner zu infizieren.

Das BSI und die Polizeiliche Kriminalprävention der Länder und des Bundes raten allen Betroffenen, die geforderte Gebühr unter keinen Umständen zu bezahlen. *"Sollten Internet-Nutzer von einer der Erpressungsvarianten betroffen sein, sollten sie umgehend Anzeige bei der nächstgelegenen Polizeidienststelle erstatten"*, empfiehlt Professor Dr. Wolf Hammann, Vorsitzender der Polizeilichen Kriminalprävention der Länder und des Bundes. *"Eine Zahlung des geforderten Betrags führt nicht zu einer Entschlüsselung des Rechners. Jeder sollte sich bewusst machen, dass offizielle Stellen in dieser Form niemanden ansprechen und in dieser Form kein Geld fordern würden"*, betont Hammann.

Eine Möglichkeit, einen durch Trojanerbefall gesperrten Rechner von der Schadsoftware zu befreien, können Rettungs-CDs sein, die beispielsweise die Anbieter von Antivirensoftware auf ihren Webseiten zum Teil kostenfrei bereitstellen. Diese Rettungs-CDs müssen über einen nicht infizierten Rechner heruntergeladen und auf den betroffenen Rechner aufgespielt werden. Im Falle der neuesten Schadsoftware-Variante empfehlen Polizei und BSI jedoch, sich an IT-Experten zu wenden, die bei der Entschlüsselung des Rechners behilflich sein können. Darüber hinaus bietet das Anti-Botnetz-Beratungszentrum auf seinem Internet-Angebot unter https://www.botfrei.de/ [https://www.botfrei.de] eine Schritt-für-Schritt-Anleitung, mit der Betroffene ihren Rechner reinigen können.

Schutzempfehlungen vor Schadsoftware

- Öffnen Sie niemals ungeprüft Dateianhänge. Ganz gleich, ob es sich um scheinbar ungefährliche Dateien wie Bilder, Dokumente oder sonstige Dateien handelt: Wenn Sie unsicher sind, fragen Sie sicherheitshalber beim Absender nach.
- Oft verraten sich virenbehaftete E-Mails durch eine entweder leere oder neugierig machende Betreffzeile.
- Seien Sie misstrauisch, wenn Sie E-Mails mit fremdsprachigem Betreff erhalten. Wenn Sie solche E-Mails unaufgefordert erhalten, sollten Sie diese sofort löschen.
- Vermeiden Sie es, auf Links in unaufgefordert zugesandten E-Mails zu klicken. Immer häufiger leiten diese auf infizierte Webseiten; rufen Sie diese auf, können Sie Ihren Rechner bereits mit Schadsoftware infizieren. Geben Sie die gewünschte Internetadresse per Hand in die Adresszeile Ihres Browsers ein.
- Nehmen Sie regelmäßige Sicherheitsupdates (Backups) des Systems und des Datenbestands vor, um im Fall einer Infektion mit Schadsoftware keine Daten zu verlieren.
- Auch Anwendungsprogramme (z.B. Webbrowser, Office-Programme, Adobe Reader, Java, Flash Player, Media Player u.a.) sollten regelmäßig aktualisiert werden.

Weitere generelle Informationen und Hinweise zum Schutz vor Schadsoftware können auf der Webseite des BSI unter www.bsi-fuer-buerger.de/Schadprogramme [https://www.bsi-fuer-buerger.de/Schadprogramme] abgerufen werden. Auf den Seiten der Polizei-Beratung unter http://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet.html [http://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet.html] finden sich zusätzliche Hinweise rund um das Thema "Gefahren im Internet".

Pressekontakte:

Bundesamt für Sicherheit in der Informationstechnik
Postfach 200363
53133 Bonn
Telefon: 0228 99 9582-5777
+49 228 99 9582-5777
Telefax: 0228 99 9582-5455
+49 228 99 9582-5455
E-Mail: presse@bsi.bund.de

POLIZEILICHE KRIMINALPRÄVENTION
der Länder und des Bundes (ProPK)
ZENTRALE GESCHÄFTSSTELLE
c/o Landeskriminalamt Baden-Württemberg
Taubenheimstraße 85
70372 Stuttgart
Telefon (0711) 54 01-20 62 - Fax (0711) 2 26 80 00
E-Mail: presse@polizei-beratung.de
Internet: www.polizei-beratung.de [http://www.polizei-beratung.de]