Warnung vor Verschlüsselungstrojanern

Sehr geehrte Damen und Herren,
Liebe Kunden,

seit Anfang des Jahres findet eine außergewöhnlich aggressive und gefährliche Angriffswelle von Computerschädlingen statt, wie wir sie in dieser Form noch nicht gesehen haben. Man geht in Deutschland von stündlich 5.000 Neuinfizierungen aus, inzwischen werden auch massenweise Webserver befallen.

Ein infizierter Computer verschlüsselt sämtliche Dokumente auf Ihrem Computer, Ihren externen Festplatten und allen Netzwerklaufwerken, auf die Ihr Rechner Zugriff hat. Danach werden Sie aufgefordert, innerhalb einer kurzen Frist Geld zu bezahlen, damit Ihre Dateien wieder entschlüsselt werden, andernfalls verfällt die Möglichkeit zur Rückholung.

Eine technische Möglichkeit zur Entschlüsselung der Dateien ohne Zahlung des Lösegelds ist bisher nicht bekannt.

Besonders gefährlich: Diese Schädlinge tarnen sich derart raffiniert, **dass selbst aktuelle Virenscanner den Befall meist nicht entdecken**.

Wie verbreiten sich die Schädlinge?

Der häufigste Verbreitungsweg sind Emails mit infizierten Dokumenten, meist getarnt als Rechnungen, Scans oder Faxe. Hier ist große Vorsicht geboten, weil diese Emails in Form und Inhalt inzwischen **kaum noch von echten Mails zu unterscheiden** sind. Oft taucht als (gefälschter) Absender sogar Ihre eigene Firma auf.

Neuerdings **reicht auch der einfache Besuch einer kompromittierten Webseite** zur Infizierung aus, ohne dass Sie irgendetwas herunterladen oder anklicken müssen.

Diese neuartigen Schädlinge wechseln inzwischen derart schnell ihre Verbreitungsmechanismen, dass sie sich wahrscheinlich bald auch von selbst im Netzwerk verbreiten, sobald ein einziges infiziertes Notebook mit dem Netzwerk verbunden wird.

Besonders heimtückisch: Die Schädlinge können sich Tage oder Wochen lang als Schläfer in Ihrer Firma verbreiten, bevor sie plötzlich aktiv werden. Damit ist der Infektionsweg nur noch schwer nachzuvollziehen.

Was können Sie zur Vorbeugung tun?

- Bitte informieren Sie umgehend alle Mitarbeiter über diese **außergewöhnliche Bedrohung** und die Tatsache, dass Virenscanner und andere technische Schutzmechanismen alleine im Moment **keinen ausreichenden Schutz** bieten.
- Öffnen Sie **niemals** unbekannte Dateianhänge, selbst wenn die Emails scheinbar von bekannten Personen oder Firmen stammen
- Klicken Sie **niemals** auf Links in Emails, an denen auch nur der kleinste Verdacht besteht, dass etwas nicht mit Rechten Dingen zugeht. Denken Sie daran, dass ein infizierter

Rechner von Kollegen oder Freunden in deren Namen aber ohne deren Wissen Emails verschicken kann!

- Stellen Sie sicher, dass Microsoft Office so eingestellt ist, dass **nicht automatisch Makros** ausgeführt werden können.
- Verwenden Sie zum Surfen nach Möglichkeit die neueste Version von Firefox, keinesfalls veraltete Versionen vom Microsoft Internet Explorer
- Computer mit **Windows XP** sind ein extremes Sicherheitsrisiko und sollten selbst dann stillgelegt werden, wenn sie keinen Internetzugang und keinen Email-Client haben. Um sie zu infizieren, reicht das Einstecken eines USB-Sticks, das Öffnen eines Dokuments oder – ganz ohne eigenes Zutun – eine Dateifreigabe auf die lokale Festplatte.
- Stellen Sie sicher, dass die Windows-Updates, Virenscanner und insbesondere Hilfsprogramme wie **Adobe Reader**, **Adobe Flash** und Java **auf dem jeweils aktuellen Stand** sind. Verwenden Sie insbesondere keine veralteten Versionen von Microsoft Word oder Excel.
- Legen Sie alle Dokumente auf einem Fileserver ab, von dem ein tägliches Backup gemacht wird. Eine permanent angeschlossene USB-Festplatte ist zur Datensicherung ungeeignet, denn der Schädling kann auch alle darauf befindlichen Dokumente unbrauchbar machen.
- Natürlich müssen auch Ihre Server und Firewalls gepflegt und gesichert sein. Darum kümmern wir uns im Rahmen des Wartungsvertrags, aber das schützt nicht vor dem üblichen Infektionsweg durch einen PC oder ein Notebook.

Wie erkenne ich einen Befall?

Wenn auf Ihrem PC oder Ihrem Dateiserver statt der Ihnen bekannten Dateien plötzlich merkwürdige Dateinamen auftauchen, ist ein Befall wahrscheinlich. Typische Dateiendungen sind **.aaa** oder **,locky**. In den befallenen Verzeichnissen liegen meist zusätzlich Dateien mit Namen wie „Howto_Restore_FILES“ oder „HOW TO DECRYPT FILES.txt“, in der eine Anleitung zur Zahlung des Lösegelds steht.

Was ist nach einem Befall zu tun?

Ist Ihr Rechner betroffen, ziehen Sie sofort das Netzwerkkabel von Ihrem Computer ab und fahren Sie ihn herunter. Ist ein Fileserver betroffen, müssen sofort alle PCs vom Netz getrennt werden, die Zugriff darauf haben. **Rufen Sie uns danach umgehend an, damit wir geeignete Maßnahmen ergreifen können**.

Danach müssen Sie davon ausgehen, dass Sie selbst bei einer vorhandenen Datensicherung bis zur kompletten Diagnose aller PCs und Server für mehrere Tage nicht mehr arbeitsfähig sein werden, denn wenn nur ein einziger befallener Computer vorzeitig wieder ans Netz ginge, würde das zerstörerische Werk dieser Schasoftware von neuem beginnen.

Noch Fragen?

Rufen Sie uns an, wir beraten Sie gerne!

GEOTEK Datentechnik GmbH

Fehrbelliner Str. 50
10119 Berlin
Tel: 030 44 34 23 33
Email: info@geotek.de
Web: www.geotek.de

Berlin, 25.2.2016