Hinweise und Informationen
zu den aktuellen Gefahren durch Crypto-Trojaner oder Ransomware

Aus aktuellem Anlass möchten wir Ihnen einige Hinweise und Informationen geben, die Ihnen helfen sollen, sich vor den Gefahren durch sogenannte Crypto-Trojaner zu schützen.

Crypto-Trojaner oder auch Ransomware stellen eine Gruppe von „PC-Schädlingen" dar, die in erpresserischer Absicht Dateien und Dokumente verschlüsseln, sobald sie aktiv geworden sind. Damit sind diese Dateien für Sie nicht mehr nutzbar. Davon betroffen sind vor allem Bilder und Office-Dokumente. Die Schadsoftware suggeriert dann über entsprechende Hinweisdateien .html oder .txt, dass Sie nach der Zahlung einer bestimmten Summe, Ihre Dateien wieder entschlüsselt bekommen. Da es sich hier aber um kriminelle Aktivitäten handelt, gibt es keine Sicherheit dafür, dass Sie nach der Bezahlung Ihre Daten wieder freikaufen können.

Unabhängig von den weiteren Information in diesem Dokument: Sichern Sie Ihre Daten auf externe Datenträger, die nicht ständig an Ihrem PC angeschlossen sind! Wir beraten Sie gerne!

Die Schadsoftware versucht Ihren Weg aktuell vor allem über Email zu Ihrem Rechner zu finden. In einer immer besseren Art und Weise wird versucht, Sie zum Öffnen der Mail und der angehängten Schadsoftware zu motivieren.

Deshalb ist es wichtig, sich Emails genau anzuschauen und auf Plausibilität zu prüfen, besonders wenn Anhänge hinterlegt sind. Achten Sie besonders auf ZIP-Dateien oder Office-Dokumente, die Sie unaufgefordert bekommen! Hier sollte die Mail auf Unstimmigkeiten geprüft werden. Angefangen bei der Absenderbeschreibung und der Absenderadresse der Mail. Klingt dieser plausibel oder verbirgt sich hier schon ein generierter Name ähnlich gfqwrstz@yahoo.com? Passt der Anzeigename und die Email-Adresse zusammen? Überprüfen Sie, ob die Voransicht der Anhänge genau so wie artgleiche Dokumente auf Ihrem PC dargestellt werden! Beispielsweise werden die Datei-Endungen standardmäßig ausgeblendet, so dass eine Word-Datei auf Ihrem PC als „Das ist mein Text" und dem Word-Symbol angezeigt wird. Wenn nun in der Email plötzlich „Das ist Schadsoftware**.doc**" steht, versucht Ihnen jemand ein falsches Dokument mit einer anderen Dateiendung unterzuschieben.

Fragen Sie sich vor allem, ob Sie die Mail überhaupt erwarten konnten. Würden Sie eine Rechnung, eine Bestellbestätigung oder eine Mahnung erhalten, wenn Sie dort weder vertraglich gebunden sind oder etwas bestellt haben? Aktuell sind es beispielsweise Bewerbungen, die angeblich aufgrund bestehender Stellenangebote im Internet, versandt wurden.

Weitere Unstimmigkeiten, die für Spam/Malware sprechen:

- eine Anrede, die verallgemeinert ist, obwohl in der Email versucht wird, ein persönliche Beziehung zu Ihnen darzustellen
- eine Anrede, die Sie zwar persönlich anspricht, aber Rechtschreibfehler enthält
- ein Text indem sich vermehrt grammatikalische oder orthografische Fehler befinden, die bei einer gewissen Häufigkeit ein Indiz sein könnten

i.based: Systemhaus GmbH & Co. KG
18439 Stralsund • Langenstraße 38
http://www.ibased.de

- Links innerhalb der Mail können auf Internetseiten mit Schadsoftware leiten, hier ist es sinnvoll, den Mauszeiger über den Link zu halten und sich in der Statusleiste am unteren Bildschirmrand das Ziel anzusehen. Die Zieladresse sollte einerseits plausibel sein und andererseits genau zu den Daten des Linktextes passen. Achten Sie dabei auch auf Details, wie Buchstabendreher oder weitere Domainendungen!
- wenn Anhänge beim Öffnen unerwartet nach einem Passwort fragen oder nicht das Programm startet, welches Sie erwartet haben
- wenn der PC nach dem Öffnen eines Anhangs sehr langsam und träge wird, kann dies auch für bereits im Hintergrund laufende Prozesse sprechen

Leiten Sie derartige Emails bitte nicht an andere Benutzer weiter, die Sie bitten, das Dokument ebenfalls einmal zu testen! (Nach dem Motto, ich krieg' das nicht auf, kannst Du das mal öffnen?) Informieren Sie uns bitte bereits beim Verdacht, dass etwas faul sein könnte, wir schauen dann gemeinsam.

Meist sind es kleine Details, die erkennen lassen, dass es sich um eine unerwünschte Mail, im schlimmsten Fall mit Schadsoftware, handelt. Wenn Sie sich nicht sicher sind, ob es sich um eine solche handelt, ist auch das schon ein Warnsignal. In diesem Fall scannen Sie die Email mit einem Anti-Virenprogramm und scheuen Sie sich nicht davor, notfalls einen kurzen Anruf zu tätigen und sich abzusichern. Wir sind Ihnen dabei gerne behilflich.

Falls es zu einer Infektion kommt - dafür genügt schon ein Klick auf einen Link oder angehängtes Dokument, verrichtet die Schadsoftware, im Zweifelsfall sofort, ihre Arbeit und verschlüsselt alle erreichbaren Dokumente/Daten auf dem lokalen System - aber auch Freigaben, welche durch die Server bereitgestellt werden. Wenn die Daten einmal verschlüsselt sind, gibt es keine Möglichkeit mehr, diese wiederherzustellen!

Der Aufforderung solcher Programme, durch Zahlung eines gewissen Betrages an die Hintermänner die Daten wieder zu entschlüsseln, sollte man nicht nachkommen. Es gibt genug Berichte von Fällen in denen, auch nach besagter Zahlung, keine Wiederherstellung der Daten erfolgte.

Sorgen Sie in jedem Fall vor! Legen Sie regelmäßig eine Sicherung Ihrer Daten an, deren Datenträger nicht ständig an Ihrem PC angeschlossen ist! Sichern Sie Ihren Rechner zusätzlich mit einem Antivirenprogramm ab!

Öffnen Sie nur Anhänge von Emails, die Sie als sicher einschätzen und fragen Sie lieber nach einer zweiten Meinung! Denn trotz sorgfältiger Prüfung und Vorsicht ist ein Restrisiko nicht auszuschließen.

Sie haben Fragen zu diesen Informationen?

Rufen Sie uns an! Telefon: **03831 28944-0**
oder besuchen Sie unsere Website: **www.ibased.de**

i.based: Systemhaus GmbH & Co. KG
18439 Stralsund • Langenstraße 38
http://www.ibased.de

11 gute Gründe dafür, dass wir der richtige IT-Dienstleister für Ihr Unternehmen sind

1 **Wir** sind ein inhabergeführtes Unternehmen - als Inhaber kümmern wir uns auch persönlich um Sie. Die Nähe zu unseren Kunden ist uns wichtig, um ihre Belange und Anliegen zuverstehen und umzusetzen.

2 **Wir** sind ein freundliches, motiviertes und kompetentes Team mit Ansprechpartnern, die sie persönlich kennen und die Sie persönlich kennen.

3 **Wir** haben kurze Entscheidungswege und Begeisterung für alle Belange der Informationstechnologie im kompletten Team.

4 **Wir** garantieren Kompetenz und Know-How im Aufbau und dem Betrieb von IT- und Telekommunikationsstrukturen und sind als ein Ansprechpartner für beide Welten und Sie da.

5 **Wir** sind flexibel, aktiv und engagiert bei der Betreuung Ihrer Mitarbeiter und Ihrer Infrastruktur.

6 **Wir** nutzen zur Wartung der IT/TK-Systeme leistungsfähige Kontrollverfahren und ermöglichen Kostentransparenz durch Dokumentation der ausgeführten Arbeiten.

7 **Wir** denken und handeln strikt kundenorientiert und bieten Ihnen individuelle, auf Ihr Unternehmen abgestimmte Lösungen.

8 **Wir** gestalten individuelle und flexibele Serviceverträge - genau auf Ihre Bedürfnisse abgestimmt.

9 **Wir** betreuen kleine und große Unternehmen mit mehr als 150 Mitarbeitern und mehr als 120 EDV-Plätzen und sind stolz darauf.

10 **Wir** agieren als regionales Unternehmen mit Sitz in Stralsund, mittlerweile seit 11 Jahren erfolgreich auf dem Markt.

11 **Wir** arbeiten mit namhaften Partnern zusammen, damit wir Ihnen eine erfolgreiche und langfristige Zusammenarbeit garantieren können.

i.based
NETWORK APPLICATIONS

gutegruende@ibased.de
Telefon: 03831 **28944-0**
www.ibased.de

Elf gute Gründe.
Starten Sie eine vielversprechende Zusammenarbeit mit uns!

Sie suchen noch mehr Gründe?

Rufen Sie uns an! Telefon: **03831 28944-0**
oder besuchen Sie unsere Website: **www.ibased.de**

i.based: Systemhaus GmbH & Co. KG
18439 Stralsund • Langenstraße 38
http://www.ibased.de

KOMPETENZ IN IT