
Ihr IT-Dienstleister und Experte in Sicherheitsfragen

## Wichtiger Hinweis: nach Firewall-Update bleiben bestimmte Dateien hängen

Unser Hersteller für IT-Sicherheitsprodukte ist 24 Stunden am Tag für Sie und uns im Einsatz, an verschiedenen Standorten auf der ganzen Welt. Unser Dienstleister wertet Millionen von E-Mails, URLS, Dateien und weiteren Daten aus, um die neuesten IT-Gefahren schnell zu erkennen und entgegenzuwirken. Somit erhalten auch Sie ständig aktuellen und erweiterten Schutz. Notwendig geworden ist jetzt ein Update bei Firewall und Viruswall.

Seit diesem Update werden folgende Dateienanhänge zu Ihrem Schutz ausgefiltert – egal ob diese gezippt oder umbenannt wurden:

.com; .bat; .vbx; .hta; .inf; .js; .jse; .wsh; .vbs; .vbe; .lnk; .chm; .pif; .reg; .scr; .cmd; .htb; .msi; .exe

Ist das ein Problem für Sie? Tauschen Sie die oben aufgeführten Dateiformate häufiger mit Ihren Partnerunternehmen aus? Sprechen Sie mit uns. Wir finden mit Ihnen zusammen die richtige Lösung.

Wir wissen, dass Ihnen diese Maßnahme womöglich Zusatzarbeit macht. Sicher ist dieser Zusatzaufwand geringer, als wenn ein Virus Ihre Arbeit komplett lahmlegt. Womöglich tagelang.

## Eine nicht ganz neue Masche; Lösegeldforderungen für verschlüsselte Daten

Zusätzlich weisen wir Sie auf eine nicht ganz neue Masche hin, die derzeit wieder häufiger angewandt wird:

Anonyme Hacker verschlüsseln unerlaubt die Daten von Unternehmen oder Privatpersonen – jedoch neuerdings durch direkten Zugriff, also ohne sogenannte „Malware“, die man sich unbeabsichtigt auf den Rechner „geladen“ hat. Möchte der Besitzer der Daten auf seine Daten zugreifen, wird er erpresst.

R.B.COM GmbH
Am Brünnele 2a
89291 Holzheim

TELEFON 0 7302 9633 0
FAX 0 7302 9633 55

E-MAIL post@rbcom.de
WEB www.rbcom.de

Das Szenario spielt sich wie folgt ab:

Die Hacker gelangen durch unterschiedliche Sicherheitslücken z. B. in das Netzwerk eines Unternehmens. Dann wird ein Software-Tool installiert, das bestimmte Dateien oder Dokumente verschlüsselt und Unternehmensdaten an einen Hacker-Server liefert. Sind die Hacker der Meinung, sie haben genügend Dateien verschlüsselt, erhält der Anwender die Information, eine bestimmte Summe (Geld oder Bitcoins) zu bezahlen, erst dann werden die Daten (vielleicht) wieder zugänglich gemacht.

Diesem Vorgehen können Sie nur entgegentreten, wenn das unternehmenseigene Netzwerk geschützt wird. Denken Sie daran, auch Ihre Mitarbeiter zu einem verantwortungsvollen Umgang mit der EDV anzuweisen.

Ist Ihnen etwas unklar geblieben? Keine Frage ist zu unwichtig oder zu klein. Wir sind gerne für Sie da.

Mit freundlichen Grüßen

Ihr R.B.COM-Team

R.B.COM GmbH
Am Brünnele 2a
89291 Holzheim

TELEFON 0 7302 9633 0
FAX 0 7302 9633 55

E-MAIL post@rbcom.de
WEB www.rbcom.de