

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) informiert über einen grotesken Fall von Online-Betrug, der dazu führen könnte, dass Zehntausende Deutsche ab März keinen Zugang zum Internet mehr haben:

Im November 2011 gelang dem FBI ein großer Schlag gegen das organisierte Online-Verbrechen. Über hundert Server, über die infizierte PCs manipuliert wurden, konnten sichergestellt werden. Da über diese Server jedoch der Online-Verkehr von Millionen von Rechnern in aller Welt lief, konnte das FBI das einstmals kriminelle Netzwerk nicht einfach deaktivieren. Denn die Datendiebe hatten auf den befallenen Rechnern eine Schad-Software namens DNS-Changer installiert:

DNS-Changer sorgt dafür, dass Online-Abfragen gezielt manipuliert werden konnten. Wurde beispielsweise auf einem befallenen Rechner eine Webseite aufgerufen, konnte durch die Manipulation spezielle Werbung eingeblendet werden oder gar eine komplett andere Webseite aufgerufen werden. Auch das Nachladen weiterer Schad-Software war auf diese Weise möglich. Im Internet fungieren DNS-Server als „Übersetzer“ von leicht verständlichen URLs wie beispielsweise computerwissen.de in die entsprechende IP-Adresse.

Wird dieser Vorgang jedoch manipuliert, dann kann auch bei korrekter Eingabe der URL eine andere Webseite ausgeliefert werden.

Der Nutzer bekommt von diesem Vorgang in der Regel nichts mit, sodass Betroffene oft nicht ahnen, dass diese Schad-Software auf ihrem PC vorhanden ist. Das Surfen im Internet ist wie gewohnt möglich mit einem infizierten Rechner. Wenn die DNS-Server aber deaktiviert werden, führen sämtliche Seitenaufrufe ins Leere und der Zugang zum Internet ist nicht mehr möglich.

33.000 PCs in Deutschland davon betroffen

Laut FBI-Informationen werden diese manipulierten DNS-Server von bis zu 33.000 PCs aus Deutschland aufgerufen. Sie sollten deshalb zu Ihrer eigenen Sicherheit einen Selbsttest durchführen, um zu überprüfen, ob Ihr PC infiziert ist oder nicht. Bitte beachten Sie, dass dieser Selbsttest in keiner Weise einen Virenschanner ersetzt: Es wird lediglich überprüft, ob Ihr PC über einen der DNS-Server geleitet wird, die sich bis vor kurzem noch in den Händen der Online-Betrüger befanden. Allzu viel Zeit sollten Sie sich mit dem Selbsttest übrigens nicht lassen: Am 8. März 2012 werden die verbliebenen Server vom FBI abgeschaltet. Dann ist es nicht mehr möglich, mit den infizierten Rechnern auf das Internet zuzugreifen.

So überprüfen Sie, ob Ihr PC infiziert ist oder nicht

Rufen Sie in Ihrem Browser die Webseite www.dns-ok.de auf. Diese Webseite wird vom BSI und der Deutschen Telekom zur Verfügung gestellt. Falls Sie die Meldung „Ihre DNS-Konfiguration ist korrekt“ erhalten, ist Ihr PC nicht mit DNS-Changer infiziert.

Falls Ihnen hingegen „ACHTUNG: Ihre DNS-Konfiguration ist manipuliert“ angezeigt wird, sollten Sie unverzüglich die Anweisungen befolgen, die Ihnen dann angezeigt werden.

Dieser Test wird bereitgestellt durch:



ACHTUNG: Ihre DNS Konfiguration ist manipuliert

QUELLE: Newsletter „Computerwissen Daily“, Tino Hahn, Chefredakteur, 14.01.2012

Informatikbüro Michael Oehler
Diplom-Informatiker (FH)
Stiller Winkel 4
D-76187 Karlsruhe
UST-IdNr. DE209721855

Fon +49 (0)721 53158-79
Fax +49 (0)721 53158-80
E-Mail info@oehler.IT
Internet www.oehler.IT

Bank Volksbank Karlsruhe
BLZ 661 900 00
Konto 57282703
BIC GENODE61KA1
IBAN DE15 6619 0000 0057 2827 03