COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/was-tun-wenn-conficker-heute-doch-zuschlaegt,1891706

Praxistipps von Profis

Was tun, wenn Conficker heute doch zuschlägt

Datum: 01.04.2009
Autor(en): Uli Ries

Ein Team von IT-Sicherheitsexperten hat eine nützliche Liste mit Tipps zusammen getragen, mit deren Hilfe andere Netzwerkverwalter ihre Systeme checken und gegebenenfalls von Conficker befreien können. Für den Fall, dass der Wurm doch kein Aprilscherz ist und heute tatsächlich aktiv wird.

Erste Hilfe: Ein Blog gibt Ratschläge, wie IT-Administratoren eventuellen Infektionen durch den Wurm Conficker Herr werden.
Foto:

In ihrem Blog **IT Risk Space**[1] haben IT-Sicherheitsexperten rund um Andreas Wuchner eine umfassende Liste mit Tipps **Conficker**[2] betreffend zusammen getragen. Wuchner ist Head of IT Risk Management beim Pharmariesen **Novartis**[3], die Tipps stammen laut Wuchner von seinem Team – somit also aus der Praxis.

Laut diverser Analysen von Antiviren-Herstellern soll der weltweit millionenfach installierte Conficker heute nach monatelangem Dämmerschlaf aktiv werden und sich bei von unbekannten Control-Servern mit ersten Instruktionen versorgen lassen. Netzwerkverwalter, die sich unsicher sind, ob es der Wurm auch ins eigene Unternehmensnetzwerk geschafft hat, sollten sich daher die Tipps der Sicherheitsprofis zu Herzen nehmen.

Um sich schnell über eventuell infizierte PCs zu informieren, empfehlen die Experten den Scanner, der von Mitarbeitern der Uni Bonn entwickelt wurde. Der amerikanische IT-Sicherheitsfachmann Dan Kaminsky, weltweit bekannt geworden durch die Entdeckung des DNS-Bugs, **verweist**[4] zudem noch auf eine neue Version des Netzwerkscanners nmap, die nun ebenfalls Conficker-infizierte PCs erkennt.

Für den Fall, dass Maschinen infiziert wurden, diese aber nicht einfach per Neuinstallation vom Wurm befreit werden können, rät das Team des IT Risk Blogs dazu, erst den Arbeitsspeicher zu säubern und Conficker anschließend mit einem ebenfalls genannten Tool zu entfernen.

Einer der wichtigsten Ratschläge überhaupt ist der unter Punkt Fünf genannte: Patchen. Denn bekanntermaßen hätte sich Conficker gar nicht erst über das Internet einschleichen können, wenn alle Windows-Maschinen mit dem seit Oktober 2008 zur Verfügung stehenden Patch **MS08-67**[5] versorgt worden wären.

Die Novartis-Mitarbeiter haben in ihrem Blog außerdem eine **Liste**[6] mit Links zusammen gestellt, die allerlei nützliche Informationen für IT-Sicherheitsprofis in Unternehmen bereithalten – ganz abseits von Conficker, der sich hoffentlich doch als Aprilscherz herausstellt.

Links im Artikel:

[1] **http://itriskspace.com/2009/03/31/1238505660000.html**
[2] **https://www.computerwoche.de/schwerpunkt/c/Conficker.html**
[3] **http://www.novartis.de/**
[4] **http://www.doxpara.com/?p=1294**
[5] **http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx**
[6] **http://itriskspace.com/pages/links.html**
