COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/essentielle-tipps-fuer-netzwerk-verwalter,1888051

Kampf dem Conficker-Wurm

Essentielle Tipps für Netzwerk-Verwalter

Datum: 24.02.2009
Autor(en): Uli Ries

Nachdem sich der Wurm Conficker nach wie vor verbreitet, sind offenbar noch zu wenige Unternehmensnetze geschützt. Dabei lassen sich Unternehmens-PCs und -Server in nur fünf Schritten vor dem grassierenden Conficker-Wurm absichern. Auch die Desinfektion infizierter Rechner ist vergleichsweise simpel.

Obwohl der Wurm **Conficker**[1] nun schon seit Monaten Gegenstand ausführlicher Berichterstattung diverser, auch fachfremder Medien ist, grassiert die **Malware**[2] nach wie vor. Inzwischen treibt sogar eine nochmals **verfeinerte Variante**[3] des Wurms ihr Unwesen. Dabei ist es auch für Verwalter größerer Unternehmensnetzwerke vergleichsweise leicht, alle Clients und **Server**[4] vor Conficker zu schützen. So hat unter anderem **Microsoft**[5] inzwischen eine **übersichtliche Anleitung**[6] veröffentlicht, welche Schutzmaßnahmen Conficker wirksam abhalten.

Um Infektionen von Clients und Servern aus dem Internet zu verhindern, muss zwingend das seit Oktober verfügbare **Windows-Update MS08-67**[7] installiert werden. Der Patch wurde seinerzeit außerplanmäßig veröffentlicht, also zwischen zwei Patch-Dienstagen. Entsprechend dringlich sollte der Softwareflicken auch installiert werden. Darüberhinaus rät das Microsoft-Dokument natürlich eine stets aktualisierte Antiviren-Software zu verwenden.

Unternehmen, die noch Legacy-Systeme auf Basis von Windows NT 4.0 oder Windows 98 betreiben, sollten zur Absicherung dieser Uralt-Betriebssysteme laut Microsoft unbedingt die Ratschläge eines **TechNet-Artikels**[8]. Weiterhin empfehlen die Redmonder, unabhängig von den im **Netzwerk**[9] vorhandenen Betriebssystemen per Gruppenrichtlinie für komplexe und schwer zu knackende Passworte zu sorgen. Denn zur Verbreitung im Intranet nutzt Conficker nicht die durch den außerplanmäßigen Patch geschlossene Lücke aus, sondern versucht durch Wörterbuch-Attacken die lokalen Administratorpasswörte zu knacken, um sich dann über die ADMIN$-Freigaben auf andere Rechner zu kopieren.

Microsoft empfiehlt zudem, die Autorun-Funktion der Windows-Clients **abzuschalten**[10]. Das lässt sich per Registry-Eintrag, oder durch eine Gruppenrichtlinie erzielen. Wichtig ist auch zu wissen, Administratoren von Systemen mit Windows 2000, **Windows XP**[11] und Windows Server 2003 zuvor das jeweils passende, **hier**[12] genannte Update installieren müssen. **Windows Vista**[13] und **Windows Server 2008**[14] müssen mit einem anderen **Sicherheitsupdate**[15] versehen werden, damit sich die Autorun-Funktion zuverlässig abschalten lässt.

Sind die Clients bereits von Conficker befallen, helfen verschiedene Removal-Tools wie beispielsweise das Microsoft **Malicious Software Removal Tool**[16] oder F-Secures **Gratis-Programm**[17]. Da Conficker auf infizierten PCs den Zugriff auf diverse Download- und Hilfsseiten der Antiviren-Hersteller blockiert, müssen die Anwendungen auf einen sauberen Rechner heruntergeladen und dann entsprechend verteilt werden. Alternativ bleibt auch immer noch der Weg der **manuellen Entfernung**[18] des Wurms.

Links im Artikel:

[1] **https://www.computerwoche.de/schwerpunkt/c/Conficker.html**
[2] **https://www.computerwoche.de/schwerpunkt/m/Malware.html**
[3] **https://www.computerwoche.de/knowledge_center/security/1887888/**
[4] **https://www.computerwoche.de/schwerpunkt/s/Server.html**
[5] **https://www.computerwoche.de/schwerpunkt/m/Microsoft.html**
[6] **http://technet.microsoft.com/de-de/security/dd452420(en-us).aspx**
[7] **http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx**
[8] **http://technet.microsoft.com/de-de/library/cc751251(en-us).aspx**
[9] **https://www.computerwoche.de/schwerpunkt/n/Netzwerk.html**
[10] **http://support.microsoft.com/kb/953252**
[11] **https://www.computerwoche.de/knowledge_center/security/1884066/**
[12] **http://support.microsoft.com/kb/953252**
[13] **https://www.computerwoche.de/knowledge_center/software_infrastruktur/1865775/**
[14] **https://www.computerwoche.de/knowledge_center/virtualisierung/1878122/**
[15] **http://www.microsoft.com/germany/technet/sicherheit/bulletins/ms08-038.mspx**
[16] **http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=ad724ae0-e72d-4f54-9ab3-75b8eb148356**
[17] **ftp://ftp.f-secure.com/anti-virus/tools/beta/f-downadup.zip**
[18] **http://support.microsoft.com/kb/962007**
