Conficker: Protokoll einer Entwurmungsaktion

Die Statistiken der professionellen Anti-Viren-Spezialisten suggerierten lange Zeit, dass die Schweiz nicht von der Conficker-Epidemie betroffen sei. Dieser Tatsachenbericht aus einem Schweizer Unternehmen belegt das Gegenteil.

BILD: FOTOLIA

→ **VON CHRISTOPH BAUMGARTNER**

Der Notfall tritt gewöhnlich immer dann ein, wenn man ihn gar nicht brauchen kann: Freitagnachmittag, kurz vor dem Wochenende oder wenn der Spezialist in den Ferien ist. So auch in diesem Fall.

FREITAG, 2. 1. 09, 12:45 UHR

Im Neu-Ulmer Büro von OneConsult klingelt das Telefon. Weil die Schweizer Mitarbeiter des Sicherheitsexperten an diesem zweiten Neujahrstag in den Betriebsferien sind, hat die Telefonanlage das Gespräch vom Thalwiler Hauptsitz an die deutsche Niederlassung weitergeleitet. Am anderen Ende der Leitung ist der IT-Leiter eines grossen Schweizer Versicherungskonzerns: Es werde schnellstmöglich Unterstützung vor Ort benötigt, vermutlich Virenbefall – ein Notfall.

Die deutsche Kollegin informiert sofort die Assistentin am Hauptsitz, diese wiederum kontaktiert umgehend Oliver Gruskovnjak, Security Consultant bei OneConsult. Der geniesst zwar gerade seine Ferien in Frankreich, bricht den Urlaub aber sofort ab und telefoniert noch auf der Rückreise mit dem Kunden, um keine wertvolle Zeit zu verlieren. Dem Security-Spezialisten wird klar, dass es sich beim Übeltäter um den Wurm Conficker/Downadup handeln könnte. Parallel dazu wird ein Angebot für den Notfalleinsatz erstellt und umgehend vom Kunden akzeptiert.

SAMSTAG, 3. 1. 09, 08:00 UHR

Oliver Gruskovnjak trifft beim Kunden ein. Die mittlerweile vom Dauereinsatz gezeichneten IT-Spezialisten vor Ort informieren ihn, dass sie bereits seit zwei Tagen erfolglos versucht haben, die infizierten Computer zu desinfizieren. Der Wurm wurde bereits zur Analyse an den Anti-

MEHR ZUM THEMA

OneConsult GmbH → **www.oneconsult.com**
MS-Sicherheits-Newsletter → **www.microsoft.com/germany/technet/sicherheit/newsletter**
Hintergrundinformationen zu Conficker → **http://blogs.zdnet.com/security/?p=2228**

virenhersteller gesendet – bisher noch ohne Ergebnis. Gruskovnjak macht sich umgehend an die Analyse. Dabei fallen ihm folgende Punkte auf: Die stark ansteigende Anzahl von Verbindungen auf den Port 445 und die geloggten Accounts auf den Systemen. Das Ausmass der Infektion lässt sich mittlerweile abschätzen: Es sind zirka 3000 Nodes betroffen.

Da zu der Zeit weder vom Antivirenhersteller noch vom Software-Anbieter («Sie hätten die Patches einspielen sollen») verlässliche Informationen über Conficker zu bekommen sind, untersucht Oliver Gruskovnjak das Binary des Wurms mittels Reverse Engineering und rekonstruiert den Tathergang:

❶ Nachdem Conficker den Server Service infiziert hat, kopiert er sich unter einem zufällig generierten Namen in das System32-Verzeichnis von Windows. Sofort fällt auf, dass der Zeitstempel der DLL der gleiche ist wie der des Kernel32.dll. So versucht der Wurm, sich zu verstecken.

«Selbst das beste Antivirensystem ist kein Ersatz für zeitnahes Patchen»

Christoph Baumgartner, CEO OneConsult

❷ Der Wurm blockt systematisch den Zugriff auf Webseiten mit vordefinierten Wörtern (z. B. Antiviren-Software, Microsoft etc.).

❸ Conficker verändert Registry, File System sowie Dienste und nutzt geschickt den flüchtigen Speicher. Deshalb nützt es auch nichts, nur die zugrunde liegende DLL zu löschen.

❹ Ist der Wurm gestartet, sucht er nach neuen Opfern, um diese mittels der Server-Service-Sicherheitslücke zu kompromittieren. Gelingt dies nicht, versucht er, Zugriff auf das ADMIN$ Share zu bekommen, kopiert sich auf das System und legt dort einen Scheduled Task an, damit er auf dem System gestartet wird.

SAMSTAG, 3. 1. 09, 15:45 UHR

Inzwischen ist das weitere Vorgehen klar: Erstens: Einspielen der nötigen Patches, um eine Neuinfektion zu verhindern. Zweitens: Säubern. Drittens: letzte Anpassungen vornehmen. Die Arbeiten sind aufgeteilt: Das Team des Kunden patcht systematisch alle Systeme. Gruskovnjak selbst macht sich anhand der Ergebnisse des Reverse Engineerings an die Programmierung eines Desinfektions-Tools.

SONNTAG, 4. 1. 09, 07:30 UHR

Nach einer kurzen Nacht ist Oliver Gruskovnjak wieder vor Ort beim Kunden. Während er weiter Reverse Engineering betreibt, fliessen seine Erkenntnisse in die von seinem Teamkollegen Matthieu Bonetti, ebenfalls Security Consultant bei OneConsult, übernommene Tool-Weiterentwicklung ein. Inzwischen führen die Analyse-Aktivitäten des Antivirenherstellers dazu, dass die Wurm-DLL mittels des Antivirenprogramms entfernt werden kann. Dies gilt aber nicht für die durch den Wurm ausgeführten Systemveränderungen. Montagmorgen muss alles wieder laufen. Mittlerweile rapportiert der IT-Leiter der Geschäftsleitung stündlich über den Verlauf. Jetzt kommt das selbstentwickelte Desinfektions-Tool zum Einsatz: Alle Nodes lassen sich erfolgreich in den Ursprungszustand zurückversetzen. 60 Stunden nach dem ersten Anruf ist die Gefahr gebannt, der Rest ist Fleissarbeit.

MONTAG, 5. 1. 09, 07:00 UHR

Die ersten Versicherungsangestellten beginnen ihre Arbeitswoche. Für viele ist es der erste Arbeitstag im neuen Jahr – und kaum einer hat realisiert, dass noch Stunden vorher ein grosser Teil der IT-Infrastruktur lahmgelegt war. Die letzten infizierten Systeme werden im Laufe des Vormittags gesäubert. Ziel erreicht, Auftrag erfolgreich gemeistert.

URSACHENANALYSE & FAZIT

Im Schlussbericht für die Geschäftsleitung analysieren Oliver Gruskovnjak und OneConsult-CEO Christoph Baumgartner die Ursachen der Beinahekatastrophe: Die Wurm-Epidemie entstand durch eine Verkettung unglücklicher Umstände. Zwar hätte sich Conficker im Netzwerk nicht ausbreiten können, wenn die Patches kurz nach Bereitstellung im Oktober 2008 eingespielt worden wären. Andererseits birgt das unbesehene Einspielen von Patches nachgewiesenermassen gewisse Inkompatibilitätsrisiken für Nicht-Microsoft-Software. Doch warum hat die Antiviren-Software die Infrastruktur nicht geschützt? Aufgrund der grossen Anzahl an Wurmvarianten war es keinem der Antivirenhersteller zu diesem Zeitpunkt möglich, alle Varianten zuverlässig zu erkennen bzw. zu eliminieren – deshalb blieb der Wurm unerkannt. Der Kunde ging übrigens davon aus, dass die Infektion mittels eines Memorysticks erfolgte.

Obwohl der Notfall auf den ersten Blick zum ungünstigsten Zeitpunkt kam, hatte der Kunde damit Glück im Unglück: Die Webseiten, von denen der Wurm weitere Software herunterladen wollte, standen nicht zur Verfügung. Dank der engen Zusammenarbeit und des Dauereinsatzes von internen Mitarbeitern und OneConsult-Beratern kam der Versicherer mit einem blauen Auge davon: Die Geschäftsprozesse während der Bürozeiten wurden nicht tangiert. Der Wurmbefall zeigt dennoch auf, dass ein zeitnahes Patch-Management mehr als ratsam ist. ←

Christoph Baumgartner ist CEO der auf technische Security Audits spezialisierten OneConsult GmbH

Conficker → Angriffsziel und Verbreitung

Die von Conficker ausgenutzte Sicherheitslücke ist in der Security Notification CVE 2008 4250 (Buffer Overflow im RPC Interface des Windows Server Service) beschrieben: Der Windows Server Service ist für die Freigabe von Shares, Druckern und Named Pipes im Netz zuständig. Im RPC Interface des Dienstes lässt sich ein Buffer Overflow auslösen. Ein Angreifer kann diese Schwachstelle über das Netz ausnutzen, um beliebigen Code mit Systemrechten auszuführen.

Die ersten Ausbreitungen wurden im November 2008 registriert. Zu dieser Zeit war in Hackerkreisen ein Konstruktions-Tool erhältlich, mit dem sich der Wurm automatisch generieren liess. Tage später wurde das Tool frei zum Download zur Verfügung gestellt – die Infektionsrate stieg rasant an. Am 2. Dezember 2008 betrug die geschätzte Anzahl weltweit infizierter Maschinen ca. 500 000 – mittlerweile sind es zig Millionen. Ist ein PC erst einmal mit Conficker infiziert, kann er beliebigen Code von einer Website nachladen bzw. installieren. So können die Computer von Kriminellen für beliebige Delikte missbraucht werden.

Firmenprofil

OneConsult GmbH → Die international tätige IT-Security-Consulting-Firma unterhält Büros in der Schweiz sowie in Deutschland, Frankreich und Österreich. Angeboten werden Hersteller-unabhängige Beratung, Schulung und Coaching durch ausgewiesene Spezialisten. Der Fokus liegt auf technischen Security Audits (Penetration Test, Application Security Audit & Ethical Hacking) plus zugehöriger Schulung. OneConsult ist Isecom Licensed Auditor (ILA), Platinum Level und Isecom-Schulungspartner. Das OneConsult-Team hat seit 2002 über 180 OSSTMM-konforme technische Security Audits durchgeführt.