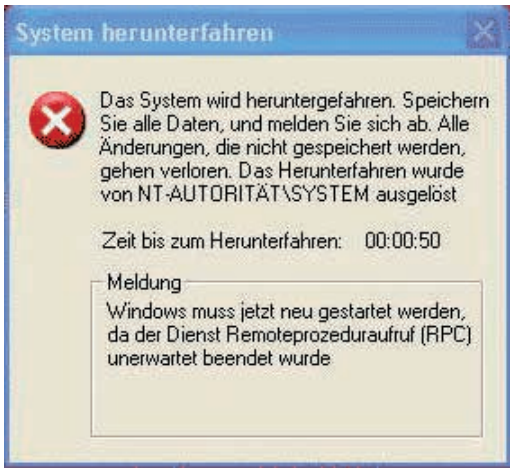
W32.Blaster.Worm und Windows-Update

Marcel Hanselmann

In diesen Tagen wurden vielleicht mehrere Kollegen, die als Betriebssystem Windows XP verwenden, beim Versuch, eine Internetverbindung herzustellen, mit dem folgenden Popup-Fenster überrascht:



Nach Ablauf von 60 Sekunden fährt das ganze System herab, und es muss dann neu gestartet werden. Was geht da vor sich?

In den Nachrichten und in der Presse wurde die Allgemeinheit informiert, dass da weltweit ein Wurm in Umlauf sei, der eine Sicherheitslücke im Windows-Betriebssystem ausnutzt. Er befällt sehr viele Systeme, die ungeschützt am Internet angeschlossen sind, die Ausbreitung geschieht diesmal nicht über E-Mail, und er zeigt exemplarisch die Problematik auf, denen Anwender von Windows ausgesetzt sind: Sie müssen ihr System regelmässig auf den neuesten Stand bringen. Wie sollen sie dies bewerkstelligen?

Liebe Benutzer von Windows 2000, bitte kontrolliert doch mal, welches Service-Pack bei Ihnen installiert ist und welche Internet-Explorer-Version bei Ihnen läuft!

In unserer eigenen Praxis laufen mehrere Computer über ein lokales Netzwerk auf Windows 2000. Die Internet-Verbindung erfolgt wie in guten alten Zeiten über einen kleinen ISDN-Router mit nur kurzzeitigen Verbindungen und dynamischer IP-Adresse, so dass eine gewisse Abschottung nach aussen vorhanden ist. Bei einem Update müssen nun grosse Datenmengen herabgeladen und installiert werden, und zwar für jede Maschine einzeln. Dies hätte eine langdauernde Internetverbindung mit entsprechenden Gefahren und hoher Telefonrechnung zur Folge. Aus diesem Grunde habe ich die Sommerflaute dazu benutzt, die Daten zu Hause über eine schnelle Cable-Verbindung herabzusaugen und auf eine CD zu brennen, um sie dann in aller Ruhe auf den einzelnen Systemen in der Praxis zu installieren. Somit sollten nun alle Systeme auf dem aktuellen Stand laufen, d.h. Service Pack 4, Internet Explorer 6 und einige Patches, und ich könnte eigentlich abends wieder ruhig einschlafen, im Vertrauen auf Bill Gates und seine Mannschaft aus Redmond.

Am 16. Juli 2003 (letzte Aktualisierung am 12. August 2003) hatte Microsoft unter dem Titel «Pufferüberlauf in RPC-Schnittstelle kann Codeausführung ermöglichen (823980)» eine Mitteilung veröffentlicht, die auf eine kritische Sicherheitslücke in ihrem

Dr. med. Marcel Hanselmann
Hauptstrasse 52
CH-4528 Zuchwil
hanselmann.m@datacomm.ch

Betriebssystem hinweist: http://www.microsoft.com/germany/ms/technetservicedesk/bulletin/bulletinms03-026.htm

Genau diese Lücke wird nun von W32.Blaster.Worm ausgenutzt. Dieser Computer-Wurm kann sich über ungeschützte Systeme mit Windows 2000 und Windows XP verbreiten, was er offenbar auch ausgiebig getan hat. Ich wüsste nun allzugerne, wie viele von unseren Kollegen sich diesen Wurm eingefangen haben. Und bei wie vielen davon eine Anti-Viren-Software läuft und alle Updates brav ausgeführt worden sind. Windows 98 und Windows me sind nicht betroffen.

Was bewirkt nun dieses Stück Programm-Code eigentlich? Erstens verbreitet es sich selber auf ausgeklügelte Art und Weise, still und heimlich im Hintergrund. Zweitens wird es den Windows-Update-Server zu bestimmten Zeiten mit unglaublichen Mengen an Anfragen bombardieren und somit im Internet unerreichbar machen (sogenannte «Denial of Service»-Attacke). Alles ist ja nur halb so wild, möchte man meinen, solange die eigenen Daten nicht betroffen sind. Dies trifft tatsächlich zu, wenn man davon absieht, dass der Wurm die Möglichkeit eröffnet, einen direkten Zugriff aus dem Internet auf unseren Computer zu erstellen, indem er eine sogenannte «remote shell» zur Verfügung stellt.

Wir haben also allen Grund, sofort den Patch einzuspielen und uns erst dann des Wurmes zu entledigen. Bei Windows 2000 sollte mindestens Service Pack 2 installiert sein, das automatische Windows-Update ist aber möglicherweise nicht mehr durchführbar.

Unter http://www.microsoft.com/security/incident/blast.asp gibt die Firma aber eine ausführliche Anleitung dazu.

Was ist nun die Schlussfolgerung aus dieser Geschichte? Auch als gewöhnliche Anwender kommen wir nicht darum herum, uns um die Sicherheit unserer Systeme zu kümmern. Dies ist insofern problematisch, wenn wir mehrere Maschinen und eine schmalbrüstige Internetverbindung besitzen. Vielleicht vereinfachen schnelle ADSL- oder Cable-Verbindungen das Problem, schaffen aber durch die permanente Internetverbindung neue Gefahren. Eine Firewall einzurichten, ist ein absolutes Muss. Aber auch diese muss den eigenen Bedürfnissen angepasst und überwacht werden. Eine einfache und sichere Lösung sehe ich vorderhand nicht. Ich ziehe es vor, die Internet-Verbindungen auf unseren eigenen Praxis-Systemen minimal zu halten und die nötigen Updates zu Hause über einen Linux-Computer mit Firewall zu beschaffen und auf CD zu brennen. Aber vielleicht ist dies ja nur der Anfang eines Computer-Paranoia-Syndroms.