

alg.exe

Source:

<http://www.tech-archive.net/Archive/German/Security/microsoft.public.de.security.netzwerk.sicherheit/2005-02/0097>

From: Christian Sattler (*christ.sattler_at_web.de*)

Date: 02/15/05

Date: Tue, 15 Feb 2005 20:59:10 +0100

Hallo,

ich habe ein kleines LAN mit Router, bei dem auch einige Ports geforwardet werden (Voice over IP etc.). Weiterhin starte ich gelegentlich TCPView von Sysinternals, um nachzugucken, ob nicht doch irgendein Hacker was von meiner Kiste saugt. Dabei ist mir jetzt ein paar mal die nette alg.exe aufgefallen (C:\WINDOWS\system32, 44.544 Bytes, Dateiversion 5.1.2600.2180 (xpsp_sp2_rtm.040803-2158)), lokale Ports habe ich mir leider nicht notiert (meine aber, vierstellig, evtl. etwas um 1500), die Gegenstelle war aber stets über den ftp-Port verbunden. Das Ganze ist wie gesagt jetzt schon ein paar mal vorgekommen. Betriebssystem ist ein regelmäßig upgedatetes Windows XP Home SP2 (automatische Updates), Firewall natürlich aktiv, für Virenschutz sorgt ein täglich upgedatetes AntiVir Personal. Die Gegenstelle war natürlich eine (sogar providerfremde) WAN-Adresse (also nichts Lokales), sonst würde ich mir ja keine Sorgen machen. WTF is 'Application Layer Gateway Service' und womit muß ich jetzt rechnen? War das jetzt der securitytechnische SuperGAU? (Mein Rechner hat im LAN auch keine Freigaben...) Die alg.exe war bisher ständig aktiv (z.B. auch nach Rechner-Neustart, meine ich), in letzter Zeit kille ich sie immer sobald wie möglich, bisher noch manuell.. braucht man das Teil eigentlich oder kann ich es ausradieren, und wenn ja, wie und mit welchen Konsequenzen? Eingeschränkte Internetfunktionalität für bestimmte 'Applications' oder was? Konnte bisher keine Nachteile feststellen, wenn ich sie gekillt hatte.. ah ja.. und 'den Fall' hatte ich schon mal pre-SP2, zwischenzeitlich aber wieder verdrängt, weil nicht sein kann, was nicht sein darf.. was kann alles passiert sein? komplettes Directory-Listing ausgelesen? securityrelevante Dateien gesaugt? *zitter*...

TIA und Gruß

--
CS