Q-107.727 - Erkennung des Virus W32/Mydoom.bb@MM

Q-107.727 - Erkennung des Virus W32/Mydoom.bb@MM

aus Tobit KB importiert - vom 12.10.2005 - Beitrag bei Tobit

Problem

Wird der Virus **W32/Mydoom.bb@MM** von der Virus Protection for DvISE bereits erkannt?

Antwort

Damit der Virus **W32/Mydoom.bb@MM** erkannt wird, sind mindestens die Virensignaturen vom 16.02.2005 erforderlich.

Minimale Version der DAT-Dateien: 4429Release Datum: 16.02.2005

Prüfen Sie im InfoCenter unter »Archive -> System -> David -> Protokoll«, ob am 16.02.2005 oder später ein Eintrag mit dem Betreff "New virus signatures received successful" existiert.

Prüfen Sie auch, ob im »Archive -> System -> David -> Ereignisse« ein Eintrag mit dem Betreff "Virus Engine started" vorhanden ist. Abhängig vom Betriebssystem sollte der Inhalt dieser Nachricht folgendes enthalten:

unter Win32: "Version.....: 4429"

Hinweis:
Die Version 4429 darf durch neuere Virensignaturen selbstverständlich höher liegen.

Beschreibungen des Virus:

Name: W32/Mydoom.bb@MM

Alias: W32.Mydoom.AX@mm, WORM_MYDOOM.BB, Win32.Mydoom.AU

Art: Wurm
Größe des Anhangs: variabel
Betriebssystem: Microsoft Windows
Art der Verbreitung: Massenmailing
Verbreitung: mittel
Risiko: mittel
Schadensfunktion: Massenmailing
Bekannt seit: 16.02.2005

Beschreibung:
W32/Mydoom.bb@MM ist ein Internetwurm, der sich per Massenmailing verbreitet. Er nutzt dabei, wie seine Vorgänger, die eigene SMTP-Maschine. Der Wurm versendet sich selbst als Anhang einer E-Mail.

Generelle Hinweise:
Bei eMail auch von vermeintlich bekannten bzw. vertrauenswürdigen Absendern sollten Sie prüfen, ob der Text der Nachricht auch zum Absender passt (englischer Text von deutschem Partner, zweifelhafter Text

oder fehlender Bezug zu konkreten Vorgängen etc.) und ob die Anlage (Attachment) auch erwartet wurde.