AV-Test.de

Ein Projekt der Universität Magdeburg und GEGA IT-Solutions GbR

Anti-Viren-Software als integraler Bestandteil einer IT-Security-Strategie

Warum man trotzdem nicht vor Würmern sicher ist

AV-Test.de

Ein Projekt der Universität Magdeburg und GEGA IT-Solutions GbR

Vorstellung

Marc Schneider

Bei AV-Test.de für Server- und Groupware-Tests zuständig

mschneider@gega-it.de

AV-Test.de

Ein Projekt der Universität Magdeburg und GEGA IT-Solutions GbR

Bestandsaufnahme

- Bisher lauerten Gefahren durch Viren, Würmer und Trojaner:
  - auf Wechseldatenträgern,
  - in E-Mails und
  - wo noch?

AV-Test.de
Ein Projekt der Universität Magdeburg und GEGA IT-Solutions GbR

Viren sind nur noch *eine* Gefahr...

- Administratoren kämpfen an neuen Fronten:
  - Dialer
  - Trojaner / Backdoors
  - Würmer
  - Security-Fixes
  - heterogene Netzwerke

AV-Test.de
Ein Projekt der Universität Magdeburg und GEGA IT-Solutions GbR

Dialer – Anschluss unter dieser Nummer

- „Automatische“ Installation während des Surfens
- Veränderung von (Sicherheits-) Einstellungen im Internet Explorer
- Unautorisierte Eingriffe ins Betriebssystem
- Lösungsansatz:
  - Sensibilisierung der Mitarbeiter
  - restriktive Browser-Einstellungen

AV-Test.de

Ein Projekt der Universität Magdeburg und GEGA IT-Solutions GbR

Trojaner und Backdoors – Spionage am Arbeitsplatz

- Industriespionage so einfach wie nie zuvor
- Fertige Programme müssen „nur noch“ konfiguriert werden
- Antiviren-Software versagt hier oft
- Lösungsansatz:
  - Einsatz von (Desktop) Firewalls
  - Sensibilisierung der Mitarbeiter

AV-Test.de
Ein Projekt der Universität Magdeburg und GEGA IT-Solutions GbR

Würmer – High-Speed im Internet

- Ausbreitungsgeschwindigkeit steigt – weshalb?
  - Eigene SMTP-Engine
  - Ausnutzung von Sicherheitslücken in Outlook etc. zur automatischen Aktivierung
  - Kombination mit Merkmalen anderer Malware

AV-Test.de
Ein Projekt der Universität Magdeburg und GEGA IT-Solutions GbR

Würmer – Keine Dateien und trotzdem da!?

- Neue Art des Wirts: Hauptspeicher
- Verbreitung als Wurm über Netzwerke
- Beispiel Code Red:
  - infizierte am 19. Juli 2001 ca. 200.000 Rechner

AV-Test.de
Ein Projekt der Universität Magdeburg und GEGA IT-Solutions GbR

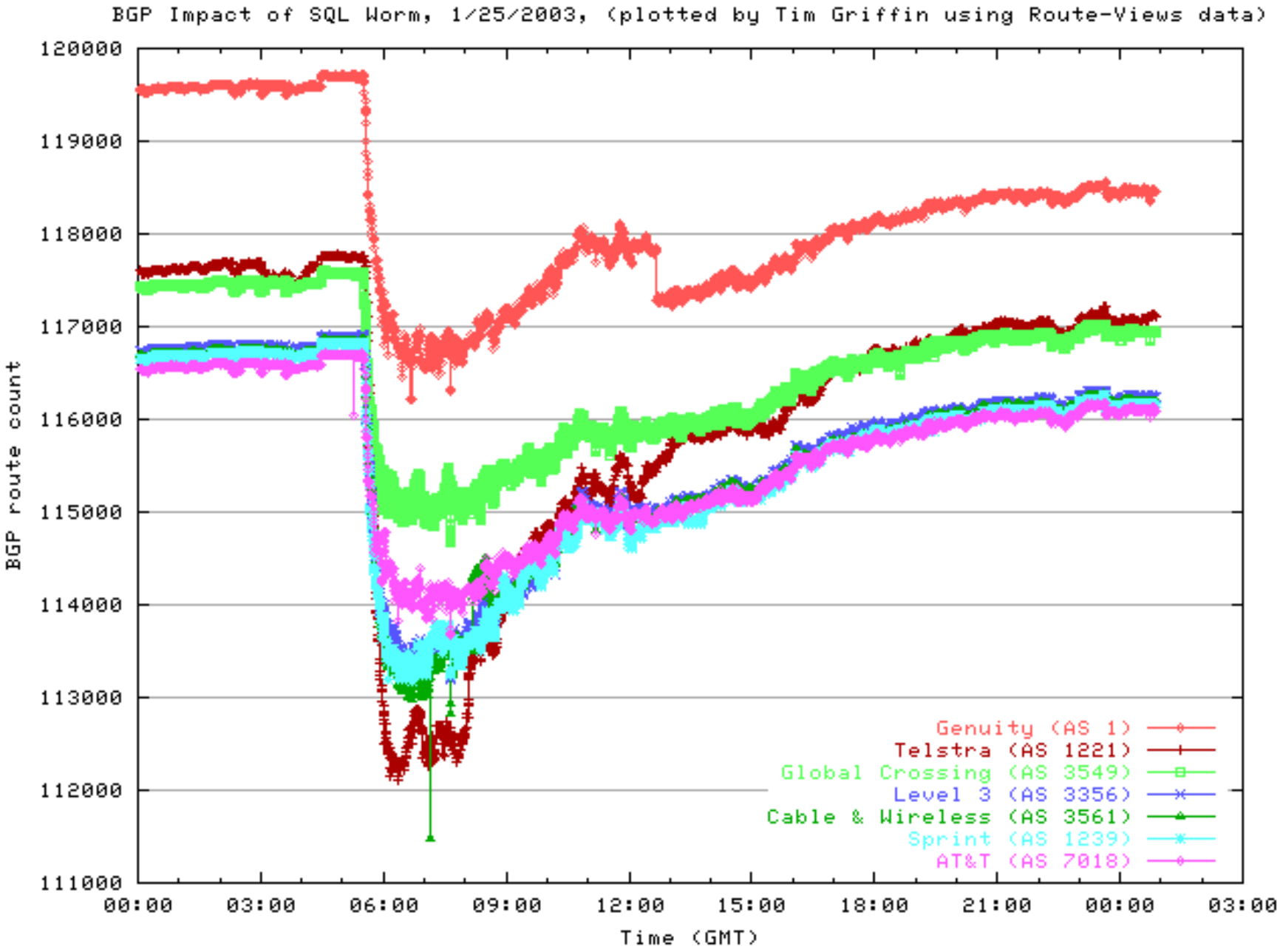
SQL/Slammer – Ein Paket mit großer Wirkung

- Befällt MS SQL-Server 2000, auch MSDE!
- Nutzt Sicherheitslücke, für die bereits seit Juli 2002 ein Patch bereit stand.
- Infektion: UDP-Paket mit 376 Byte Virencode an Port 1434.
- Verbreitet sich von diesem Rechner aus an zufällig gewählte IP-Adressen mit voller Rechnerlast.

AV-Test.de
Ein Projekt der Universität Magdeburg und GEGA IT-Solutions GbR

SQL/Slammer – Zahlen, Fakten

- 30 Minuten um Backbones weltweit zu „überfluten“
- Bsp. Rechenzentrum
  - normal: ca. 50.000 Pakete/Sekunde im Backbone
  - innerhalb von 5 Minuten: 1.000.000 Pakete/Sekunde



Quelle: http://www.research.att.com/~griffin/bgp_monitor/sql_worm.html

AV-Test.de
Ein Projekt der Universität Magdeburg und GEGA IT-Solutions GbR

...und die Antiviren-Software?

- ...konnte nichts finden.
- Grund: Hauptspeichersuche nur unzureichend- wenn überhaupt – implementiert
- Problem: Real-Time Hauptspeicher-Scan würde selbst Power-Rechner in die Knie zwingen

AV-Test.de
Ein Projekt der Universität Magdeburg und GEGA IT-Solutions GbR

Die Lösung solcher Probleme

- Einspielen von Sicherheitspatches.
- Einsatz von restriktiv konfigurierten Firewalls
- Allgemein:
  - Ausarbeitung von Sicherheitsrichtlinien.
  - Durchgehende, lückenlose Sicherheits-strategie

AV-Test.de

Ein Projekt der Universität Magdeburg und GEGA IT-Solutions GbR

Vielen Dank

- Informationen unter

  www.av-test.de