

REAKTIONSZEIT BEI VIRENALARME

Alle an F-Secure gesendeten Virenproben werden vom Anti-Virus Research Team bearbeitet. Dieses Expertenteam erhält jede Woche Hunderte solcher Proben, von denen jede einzelne analysiert wird, um mögliche neue und unbekannte Viren aufzudecken. An einem ganz normalen Tag finden wir in den Dateien, die unsere Kunden aus der ganzen Welt an uns senden, etliche neue Viren oder Würmer.

Das Virus Lab von F-Secure versendet überdies die Updates, mit denen diese neuen Viren erkannt, aufgehalten und entfernt werden. Im Durchschnitt werden wöchentlich etwa 11 Updates versendet – normalerweise zwei Updates pro Arbeitstag. Damit ein neuer Virenausbruch unterbunden werden kann, bevor er außer Kontrolle gerät, muss innerhalb weniger Stunden nach dem Erkennen des Virus ein Update versendet werden. Das Virus Lab hat sich sehr darum bemüht sicherzustellen, dass unsere Reaktionszeiten so kurz wie möglich sind.

Damit solche kurzen Reaktionszeiten eingehalten werden können, wurde ein Großteil des Vorgangs automatisiert und der Mechanismus für die Bereitstellung der Updates im Hinblick auf die Leistung optimiert. Die meisten unserer Kunden erhalten ein neues Update, sobald wir es über unseren Versandmechanismus veröffentlichen. So können sie die neuen aktualisierten Definitionsdateien sofort nutzen. Bei größeren Virenausbrüchen beträgt unsere Reaktionszeit im Durchschnitt ca. 2,5 Stunden – eine der schnellsten Reaktionszeiten weltweit, auf die wir sehr stolz sind. Dieser Zeitraum beginnt ab dem Moment, an dem die erste Virenprobe von unserem Labor empfangen wird, und endet zu dem Zeitpunkt, an dem wir das Update weltweit veröffentlichen.

Dank solcher Reaktionszeiten kann F-Secure den größeren Mitbewerbern in Übersee stets eine Nasenlänge voraus sein. Bei größeren Unternehmen ist der bürokratische Aufwand häufig viel höher, was zu langsameren Reaktionszeiten führt. Unabhängige Berichte zeigen, dass wir hier immer wieder unschlagbar sind.

Lassen Sie uns das anhand von Sobig.F veranschaulichen, einem der größten Virenausbrüche, der dieses Jahr am 18. August begann.

Zeitlicher Ablauf des Ausbruchs:

Dienstag, 19. August 2003

06.10 Uhr F-Secure erhält das erste Beispiel von Sobig.F
08.43 Uhr F-Secure versendet ein Update
09.45 Uhr Die Sobig.F-Epidemie gerät außer Kontrolle
10.37 Uhr Sophos versendet ein Update
12.53 Uhr Symantec versendet ein Update
13.39 Uhr Trend versendet ein Update
14.21 Uhr McAfee versendet ein Update

Nachfolgend finden Sie einige Beispiele für unsere Reaktionszeit bei den bisher größten Virenausbrüchen:

Melissa 1999:	3 h 15 min
Loveletter 2000:	1 h 40 min
Anna Kournikova 2001:	2 h 5 min
Sircam 2001:	1 h 50 min
Nimda 2001:	1 h 57 min
Slapper 2002:	4 h 10 min
Bugbear 2002:	2 h 47 min
Blaster 2003:	2 h 3 min
Sobig.F 2003:	2 h 33 min

Diese Reaktionszeiten wurden von Messagelabs UK bestätigt. Messagelabs bietet Unternehmen verwaltete Sicherheitsdienste über E-Mail. Die Unterschiede in der Versandzeit der Updates scheinen auf den ersten Blick nicht sehr groß zu sein. Sie hatten jedoch immense Auswirkungen auf das Endergebnis. Grundsätzlich wäre Ihr Unternehmen nicht von dem Wurm betroffen gewesen, wenn Ihre E-Mail-Gateways vor zehn Uhr morgens damit begonnen hätten, Sobig.F abzuwehren. Wenn Sie das Update jedoch erst nach 10.00 Uhr erhalten haben, war der Virus höchstwahrscheinlich bereits in Ihr internes Netzwerk eingedrungen, hat sich innerhalb Ihres lokalen Netzwerks repliziert und von Ihren Systemen aus an ihre Kunden und Partner verbreitet. F-Secure Corporation wird sich nach besten Kräften bemühen, den guten Ruf im Hinblick auf die schnellen Reaktionszeiten aufrecht zu erhalten, und wird in dieser Hinsicht auch weiterhin eine führende Stellung einnehmen.