



Acht Millionen E-Mails durchlaufen täglich das Ikarus-Scancenter in Floridsdorf – „Virenjäger“ und Technikchef Thomas Mandl hat sie alle unter Kontrolle.

Foto: Newald

In Floridsdorf ist Endstation für Riesenmengen Datenmüll

Bei 90 Prozent aller versandten Mails handelt es sich mittlerweile um Spam. Dass diese Flut nicht ungebremst auf Österreichs Computer hereinbricht, dafür sorgen Scancenter, zum Beispiel jenes des Anti-Virus-Pioniers Ikarus im 21. Wiener Gemeindebezirk.

Karin Tzschentke

Wien – Lange, weit verzweigte Gänge, durch die anscheinend ganz selten einmal ein menschliches Wesen huscht, abgesicherte Türen, die in graue Räume mit Gitterabteilen führen, in denen sich hohe Computerschränke aneinanderreihen – für echte Würmer ist hier nicht viel zu holen.

Aber auch jene Würmer, die als harmlos erscheinende E-Mails getarnt versandt werden, um auf Computern Unheil zu stiften, haben hier ebenso wenig Chancen auf eine „erfolgreiche“ Weiterreise wie ihre nächsten Verwandten, die Viren und Trojaner. Und auch für unzähligen Datenmüll, sprich: Spam, ist an diesem unwirtlichen Ort erst einmal Endstation. Denn hier im InterXion Rechenzentrum im 21. Bezirk befindet sich in einer ehemaligen Elin-Fabrik das größte von vier Scancentern des österreichischen Anti-Virus-Unter-

uns auf etwaige Anomalien und ganz konkret nach Spam und Viren gescannt“, berichtet Technikchef Thomas Mandl, „Vier weitere Millionen kommen in den von uns gehosteten Scancentern der Telekom Austria im Wiener Arsenal und in Linz noch dazu.“ An die 3500 österreichische Firmen lassen von dem 1986 gegründeten Anti-Viren-Pionier ihre Mails überprüfen.

Auch wenn mittlerweile neun von zehn E-Mails der Kategorie Spam zuzuordnen sind und 6000 bis 8000 neue Viren pro Monat im Umlauf gesetzt werden, ist Österreich hierbei fast noch so etwas wie eine „Insel der Seligen“: „Die Kleinheit des Landes ist ein Vorteil“, sagt Mandl. „Österreich ist oft eher nur der Nebenschauplatz von Attacken. Wenn neue Angriffswellen losgetreten werden, gleich ob Spam, Viren oder Phishing-Mails, werden wir meist nur von den Ausläufern erfasst – aber das ist immer noch ge-

rack, auf dessen Monitoren der Laie Zahlen- und Buchstabenkolonnen in aberwitziger Geschwindigkeit vorbeiziehen sieht und aufgeregt blinkende Lämpchen hektische Atmosphäre verbreiten. „Die durchschnittliche Verweildauer eines E-Mails im Scancenter beträgt rund 2,6 Sekunden“, erläutert der Techniker. „Ein infiziertes Mail wird binnen 40 Millisekunden entdeckt“, geht er ins Detail. In kürzester Zeit werde anhand eines mehrstufigen Analyseverfahrens jedes Bit und Byte eines Mails geprüft.

Die Guten ins Töpfchen

Wird ein Mail nach mehr als 600 einzelnen Bewertungsschritten als Spam bewertet, wird es den Kundenwünschen gemäß behandelt – gelöscht, markiert oder umgeleitet. Hintergrund dieser Unterscheidung: „Behörden, aber auch manche Unternehmen, sind gezwungen, sämtliche Mails an sie zunächst einmal anzunehmen“, erläutert Ikarus-Chef Joe Pichlmayr.

Ist es noch „relativ“ einfach, Spam zu erkennen und auszufiltern, kann ein völlig neuer Virus schon einmal eine echte Herausforderung für die rund 50 Ikarus-Experten sein. „Je nachdem kann eine Analyse

also ein Gegenmittel, ist auf den Scancentern allerdings schon nach einigen Minuten möglich“, betont Pichlmayr. Viren- und Spamattacken erfolgen meist in mehreren Wellen. Schon nach der Erstinfektion beginnen die Abwehrrountinen zu laufen, innerhalb weniger Stunden steht ein sicheres Anti-Viren-Tool für eine zuverlässige und sichere Früherkennung neuer Attacken zur Verfügung.

Trotz aller Raffinessen eines Profi-Scancenters, auf eigene Viren- und Spamfilter sollte man in Firmen oder im privaten Bereich dennoch nicht verzichten, unterstreicht der Ikarus-Chef: „Eine Infektion kann man sich auch über andere Kanäle einfangen, wie zum Beispiel über USB-Sticks, Tauschbörsen oder „Drive-by-Infektionen“ beim Surfen auf von Viren präparierten Websites.“

Ob man Spam, Viren, Trojanern und Co jemals völlig Herr werden kann, wagt heute niemand zu sagen. „Der Trend geht allerdings dahin, dass wir eines Tages den gesamten virenrelevanten Traffic am Web, also nicht nur E-Mails, über zentrale Scanner routen werden.“ Dann könne man auch den größten Teil an Viren und Trojanern, die andere Wege