MessageLabs®

Be certain

MessageLabs Intelligence: August 2006

Einleitung
Herzlich willkommen zur neuesten Ausgabe des monatlichen Intelligence Reports von MessageLabs. In diesem Bericht informieren wir Sie über die aktuellen Gefahrentrends im August 2006, um Sie über die Entwicklung von Bedrohungen durch Viren, Spam und andere unwillkommene Online-Inhalte auf dem Laufenden zu halten.

Die wichtigsten Ergebnisse dieses Berichts in Kürze:

Spam-Quote – Die Spam-Quote betrug im August 64,5 Prozent (ein Anstieg um 1,8 Prozentpunkte gegenüber dem Vormonat)
Viren-Quote – Im August war eine von 98,4 E-Mails verseucht (ein Rückgang um 0,02 Prozentpunkte gegenüber dem Vormonat)
Phishing-Quote – Hinter einer von 321 E-Mails verbarg sich der Versuch, persönliche Daten auszuspionieren (ein Anstieg um 0,1 Prozentpunkte gegenüber dem Vormonat)

Die relativ konstante Viren-Quote, die sich im August bei ca. 1 Prozent einpendelte, weist darauf hin, dass die Cyber-Kriminellen ihre Aktivitäten zunehmend auf andere Bereiche verlagern. Der Versand virenverseuchter E-Mails nimmt ab, während ein Anstieg der zielgerichteten Phishing-Angriffe zu beobachten ist. Im Verhältnis zu den Viren- und Trojaner-Aktivitäten haben die Phishing-Angriffe erheblich zugenommen und machen nun fast ein Drittel aller Bedrohungen aus – im Juli war es noch ein Fünftel. Auch dies ist ein deutliches Zeichen dafür, dass die Cyber-Kriminellen ihre Aktivitäten zunehmend auf diesen Bereich konzentrieren, vielleicht um ihre derzeit noch guten Erfolgschancen zu nutzen, bevor die zweistufige Authentisierung von den Banken rigoroser durchgesetzt wird. Darüber hinaus wird erwartet, dass die lang ersehnte Veröffentlichung von Microsoft Windows Vista im kommenden Jahr die Sicherheit von Desktop-Computern generell verbessern wird. Zuvor wird außerdem mit der Veröffentlichung von Version 7.0 des Internet Explorers gerechnet, die über eine integrierte Anti-Phishing-Technologie verfügen soll. Diese Neuerung soll das Erkennen neuer Phishing-Websites erleichtern und es Kriminellen dadurch erheblich erschweren, mit ihren betrügerischen E-Mails erfolgreich zu sein.

Die Gefahren breiten sich auf immer mehr Bereiche des Web aus, auf die Cyber-Kriminelle mit ihren Angriffen abzielen. Schon länger sind nicht mehr nur Bankkunden die Opfer hochentwickelter Phishing-Angriffe, sondern auch Kunden anderer bekannter Plattformen oder Dienste wie eBay und PayPal wurden bereits mit Phishing-Mails zur Herausgabe persönlicher Daten aufgefordert. In jüngster Zeit wurden auch beliebte Social-Networking-Sites wie MySpace von Betrügern unter Druck gesetzt. Um sich dieser Probleme anzunehmen, gab MySpace vor kurzem sogar bekannt, einen Chief Security Officer eingestellt zu haben.

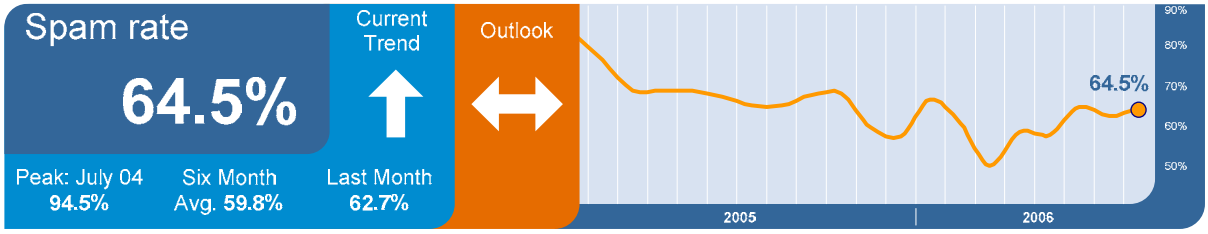
Anfang August veröffentlichte Microsoft ein weiteres kritisches Sicherheitsupdate zur Schließung von 9 „kritischen“ und 3 „wichtigen“ Sicherheitslücken seiner Windows-, Browser- und Office-Anwendungen, die dazu führen konnten, dass die betroffenen Computer von Online-Kriminellen für ihre Zwecke missbraucht wurden. Eine Schwachstelle, die in dem Microsoft Security Bulletin MS06-040 beschrieben wurde, war bereits von zwei Viren ausgenutzt worden. Diese Viren waren Varianten von W32/IRCBot und beide in der Lage, sich sowohl über den AOL Instant Messenger als auch über die MS06-040-Schwachstelle auszubreiten. Nutzer des Instant-Messaging-Dienstes konnten von anderen Nutzern dazu verleitet werden, den Bot-Code über eine externe Website herunterzuladen und auszuführen. Diese Vorgehensweise ermöglicht jenem bösartigem Code, die Firewalls von Unternehmen zu umgehen, deren Instant-Messaging-Kommunikation nicht geschützt ist, und sich

ungehindert innerhalb des internen Netzwerks auszubreiten, sobald ein Rechner erfolgreich kompromittiert worden ist.

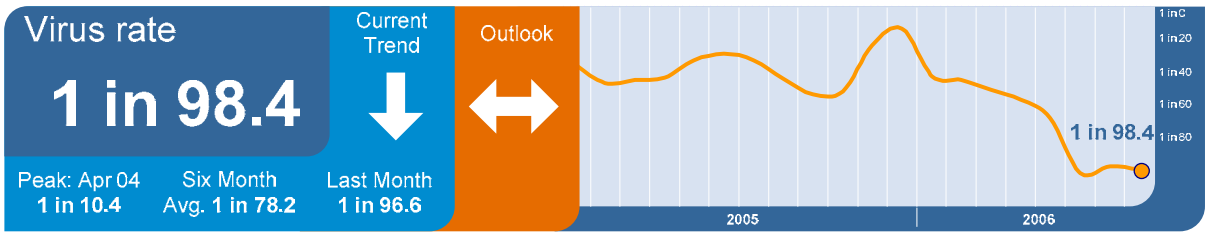
Darüber hinaus wird seit dem 16. August ein bekannter russischer Spammer verdächtigt, die MS06-040-Schwachstelle auszunutzen, um E-Mail-Server von Unternehmen, die noch ohne Sicherheitsupdate laufen, unter seine Kontrolle zu bringen und mit der berüchtigten Spam-Software Pro Mailer DMS die massenhafte Aussendung von Spam-Mails zu veranlassen. DMS hat verheerendere Auswirkungen als die meisten anderen Arten von Spam-Software, da diese Anwendung eine innovative „Spamkanonen"-Technik nutzt, die eine leistungsfähige „Serienbrieffunktion" mit fertigen Spam-Vorlagen verwendet. Dieser Ansatz ermöglicht dem Spammer, seinen Durchsatz zu maximieren und innerhalb von einer Stunde mehrere Millionen Spam-Mails über einen einzigen kompromittierten Computer zu versenden, wie bereits im MessageLabs Intelligence Report vom Mai 2006 berichtet wurde.

Weltweite Trends & Content-Analyse
Die Anti-Spam- und Anti-Viren-Dienste von MessageLabs konzentrieren sich auf die Erkennung und Abwehr unerwünschter E-Mails, die aus unbekannten, zweifelhaften Quellen stammen und an gültige E-Mail-Adressen gerichtet sind.

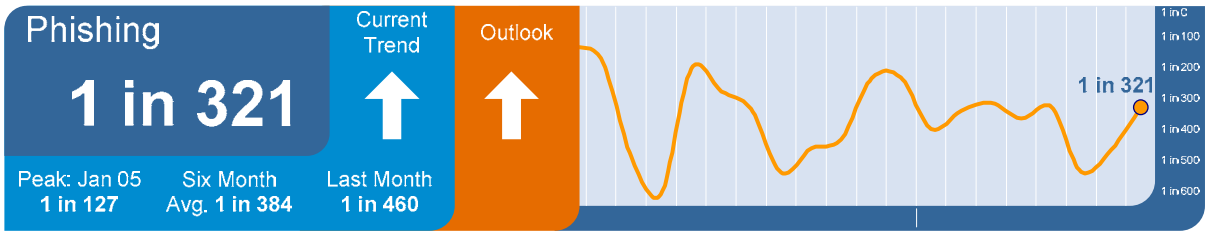
Spam-Schutz mit Skeptic™: Der Anteil von Spam am weltweiten, an gültige Empfänger adressierten E-Mail-Verkehr aus neuen oder bislang unbekannten zweifelhaften Quellen belief sich im August auf 64,5 Prozent (1 von 1,55 E-Mails). Das entspricht einem Anstieg um 1,8 Prozentpunkte gegenüber dem Vormonat.



Viren- und Trojaner-Abwehr mit Skeptic™: Der Anteil der virenverseuchten E-Mails am weltweiten, an gültige Empfänger adressierten E-Mail-Verkehr sank im August gegenüber dem Vormonat um 0,02 Prozentpunkte auf 1,02 Prozent. Eine von 98,4 an gültige Empfängeradressen gerichteten E-Mails aus neuen oder bislang unbekannten zweifelhaften Quellen war verseucht.



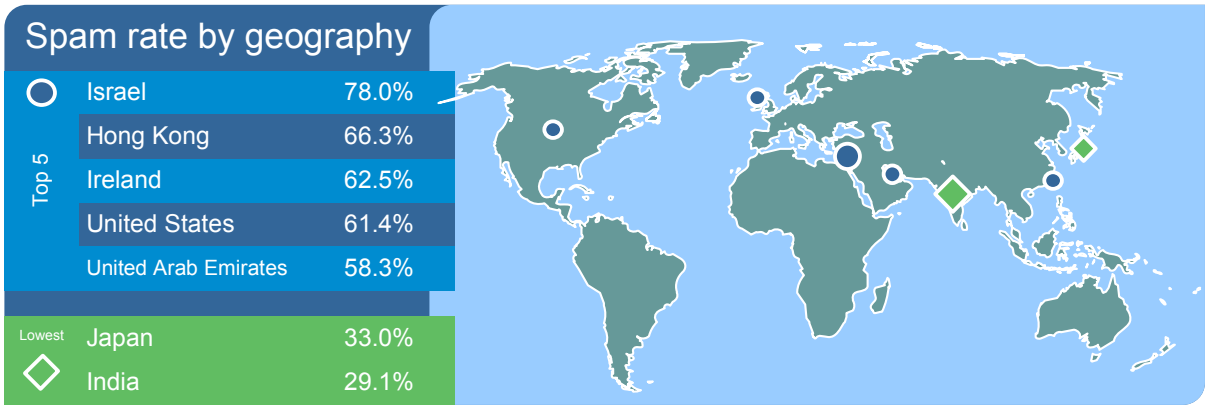
Phishing: Im August stieg die Phishing-Quote gegenüber dem Vormonat um 0,1 Prozentpunkte auf 0,31 Prozent. Hinter einer von 321 E-Mails verbarg sich der Versuch, persönliche Authentisierungsdaten auszuspionieren.



Der Anteil von Phishing-Mails an allen per E-Mail verbreiteten Gefahren einschließlich Viren und Trojanern stieg seit Juli um 9,7 Prozentpunkte an. 30,7 Prozent aller bösartigen E-Mails, die MessageLabs im August abgefangen hat, waren Phishing-Versuche.

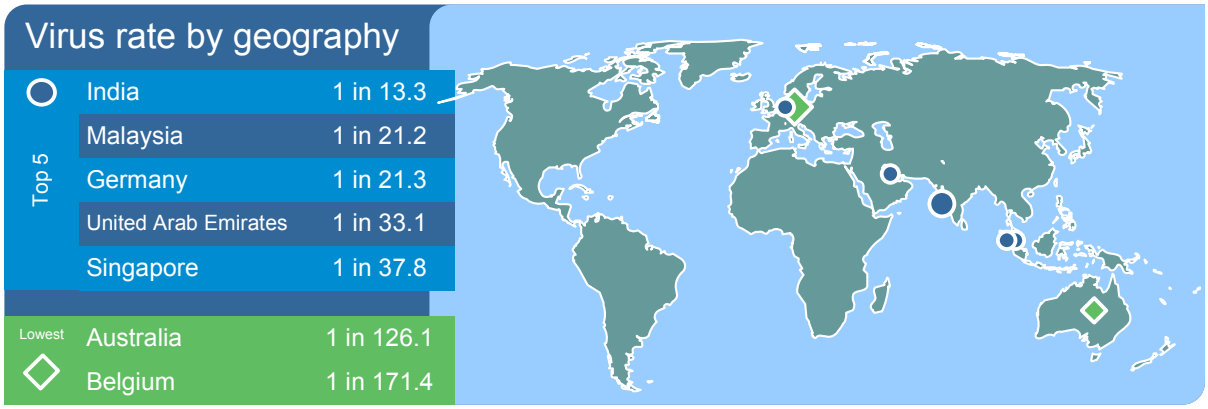
Online-Gefahren nach Zielländern

Monatsanalyse: Soweit dies möglich ist, analysiert MessageLabs die geografische Verteilung des E-Mail-Verkehrs und gewinnt auf diese Weise Daten zu den regionalen Auswirkungen von Spam und Viren sowie zu der Anfälligkeit der verschiedenen Länder für diese Gefahren. Die folgenden Grafiken zeigen die Auswirkungen und Quoten für die einzelnen Länder im August 2006.



Unter den „Top 5"-Ländern war der größte Anstieg der Spam-Aktivitäten in Israel zu beobachten. Das Land verzeichnete im August eine Spam-Quote von 78 Prozent, was einem Anstieg um 0,7 Prozentpunkte gegenüber Juli entspricht. Den größten Rückgang gab es in Irland – dort sank die Spam-Quote um 8 Prozentpunkte auf 62,5 Prozent.

Beim Vergleich aller Regionen verzeichnete Belgien im August den größten Anstieg der Spam-Quote, und zwar um 9,5 Prozentpunkte auf 53,6 Prozent. Am meisten zurück ging die Spam-Belastung in Schweden – dort sank die Spam-Quote um 8,5 Prozentpunkte auf 42,5 Prozent. In Großbritannien und Australien war ebenfalls ein deutlicher Rückgang der Spam-Quoten zu beobachten, und zwar um 7 bzw. 6,9 Prozentpunkte.

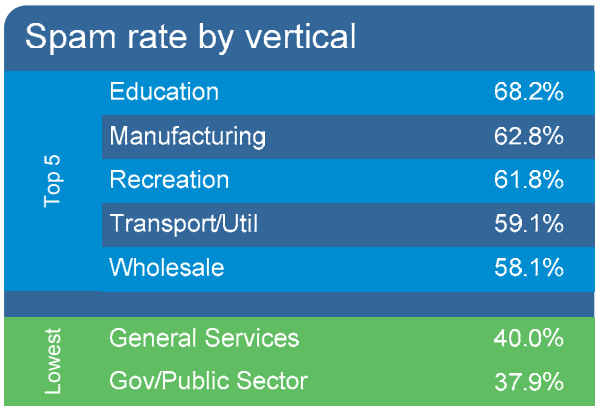


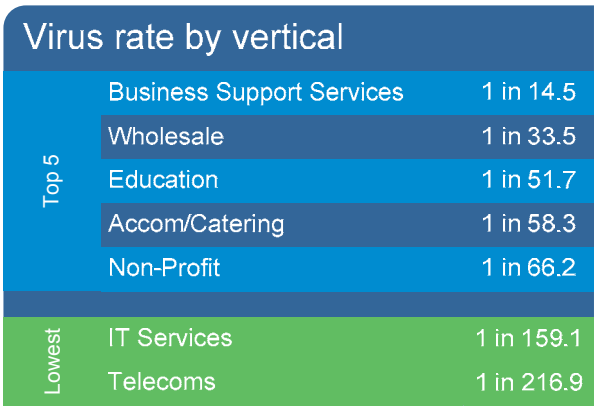
Beim Vergleich aller Regionen waren sowohl der höchste Anstieg als auch der größte Rückgang der Viren-Aktivitäten in der Liste der „Top 5"-Länder zu finden: Die stärkste Zunahme gab es in Deutschland, wo die Quote der mit Viren verseuchten E-Mails um 2 Prozentpunkte von 2,7 Prozent im Juli auf 4,7 Prozent im August anstieg und sich damit im Laufe eines Monats beinahe verdoppelte. Statt einer von 36,5 E-Mails wie im Juli war in Deutschland im August eine von 21,3 E-Mails verseucht.

Indien bleibt weiterhin das Land, das weltweit am meisten unter Viren-Angriffen zu leiden hat. Obwohl die Viren-Quote dort im August um 1,5 Prozentpunkte von 9,0 Prozent (bzw. 1 zu 11,1) auf 7,5 Prozent (bzw. 1 zu 13,3) fiel und das Land damit einen stärkeren Rückgang als alle anderen untersuchten Länder verzeichnen konnte, belegt Indien nach wie vor die Spitzenposition in diesem Vergleich.

Sicherheitsgefahren nach Branchen

Monatsanalyse: Sofern möglich, analysiert MessageLabs den E-Mail-Verkehr verschiedener Branchen und ermittelt, wie stark die größten Wirtschaftssektoren von Spam und Viren betroffen und für diese unerwünschten E-Mails anfällig sind. Die folgenden Grafiken zeigen die entsprechenden branchenspezifischen Auswirkungen und Quoten im August 2006.





Innerhalb der „Top 5"-Branchen verzeichnete der Großhandel im August den größten Anstieg der Spam-Quote, und zwar um 3,6 Prozentpunkte auf 58,1 Prozent. Den größten Rückgang innerhalb der „Top 5" gab es in der Freizeit-Industrie – dort sank dies Spam-Quote um 5,2 Prozentpunkte auf 61,8 Prozent. Von allen Wirtschaftszweigen verzeichnete der Immobiliensektor im August den größten Rückgang der Spam-Quote, und zwar um 15,1 Prozentpunkte. Mit einer Spam-Quote von nun 51,9 Prozent verließ diese Branche im August die Spitzenposition der Tabelle, die sie im Juli mit 67 Prozent noch innehatte.

Innerhalb der „Top 5“ stieg die Viren-Quote im August im Bildungssektor am stärksten, von 1,4 Prozent im Juli auf 1,9 Prozent im August. Demnach war gegenüber einer von 71,1 E-Mails im Juli im August eine von 51,7 E-Mails, die diese Branche erreichten, mit einem Virus verseucht. Dies ist auch der größte Anstieg im gesamten Branchenvergleich.

Die Anbieter unternehmensbezogener Dienstleistungen hatten auch im August weiterhin am meisten unter unerwünschten E-Mails zu leiden, obwohl sie innerhalb der „Top 5“ den größten Rückgang der Viren-Quote verzeichnen konnten, und zwar um 1,4 Prozent (von 8,3 Prozent im Juli auf 6,9 Prozent in diesem Monat). Gegenüber einer von 12,0 E-Mails im Juli war demnach im August nur noch eine von 14,5 an diese Unternehmen gerichteten E-Mails mit einem Virus verseucht. Im gesamten Branchenvergleich verzeichnete die Baubranche den stärksten Rückgang, und zwar um 7,4 Prozent, d.h. von 8,3 Prozent im Juli auf 0,9 Prozent im August. Gegenüber einer von 12,0 E-Mails im Juli war demnach im August nur noch eine von 113,3 E-Mails verseucht, die an Unternehmen dieser Branche gerichtet waren.

Traffic-Management (auf Protokoll-Ebene)
Traffic Management reduziert das Gesamtaufkommen an unerwünschten Nachrichten durch Verwaltungstechniken auf Protokollebene. Mithilfe von im TCP-Protokoll eingebetteten Funktionen werden nicht erwünschte Absender identifiziert und die Verbindungen zum Mailserver verlangsamt. Dadurch erreichen deutlich weniger E-Mail-Nachrichten von bekannten Spam-Quellen ihre Adressaten, während gleichzeitig die Übertragung legitimer E-Mails beschleunigt wird.

Verbindungsmanagement
Das Verbindungsmanagement erweist sich als ein besonders effektives Instrument, um insbesondere Directory-Harvest-Attacken, Brute-Force-Attacken und E-Mail-basierte Denial-of-Service-Angriffe zu verhindern – also Angriffe, bei denen unerwünschte Massenmails die Postfächer eines Unternehmens überfluten und auf diese Weise dessen Kommunikationssystem zum Erliegen bringen sollen.

Anwendungen für das Verbindungsmanagement arbeiten auf SMTP-Ebene und nutzen folgende Methoden, um die Legitimität von Verbindungen zum Mail-Server zu überprüfen:

SMTP-Validierung: Die SMTP-Validierung dient der Erkennung unerwünschter E-Mails von Quellen, die für den Versand von Spam und Viren bekannt sind. Das Verfahren ermöglicht die eindeutige Identifizierung unerwünschter Quellen in Gestalt offener Proxyserver oder Botnets und weist Verbindungsanfragen von solchen Quellen zurück. Im August konnte MessageLabs auf diese Weise im Schnitt 4,8 Prozent aller eingehenden Mails identifizieren und abfangen, die von Botnets oder anderen bekannten bösartigen Quellen stammten.

Prüfung der Empfängeradressen: Dieses Verfahren reduziert das Gesamtvolumen der E-Mails, die von registrierten Domains empfangen werden, indem E-Mails an Empfängeradressen abgelehnt werden, die als ungültig oder nicht existent identifiziert werden. Im August hat MessageLabs durchschnittlich 11,9 Prozent der Empfängeradressen als ungültig identifiziert und konnte dadurch Directory Harvest-Attacken auf Domains abwehren.

Die folgende Tabelle zeigt im Detail, welchen Einfluss die Verbindungsmanagement-Methoden auf das Aufkommen an unerwünschten E-Mails haben (lt. Messungen von MessageLabs). Ohne diese zusätzlichen Abwehrebenen hätte der im August an MessageLabs-Kunden gerichtete Spamverkehr etwa 84,9 Prozent des weltweiten E-Mail-Verkehrs betragen − ein Rückgang um 1,9 Prozentpunkte gegenüber dem Vormonat.

Region	SMTP Validation *(botnet sources)*	User Validation *(directory attacks)*
USA	5.0%	12.3%
UK	4.5%	11.9%
Europe	4.7%	10.9%
Asia Pacific	4.3%	10.7%
Worldwide	**4.8%**	**11.9%**

Effects of Connection Management Techniques

MessageLabs ist ein führender Anbieter von integrierten Managed Services für die Messaging- und Web-Sicherheit. Bereits mehr als 14.000 Kunden aus 80 Ländern greifen auf die Dienste des Security-Spezialisten zurück – angefangen von Kleinunternehmen bis hin zu Konzernen aus dem Kreis der Fortune 500. Das Portfolio von MessageLabs umfasst eine Vielzahl von verwalteten IT-Sicherheits-Services, um die Kommunikation via E-Mail, Web und Instant Messaging zu schützen, zu kontrollieren, zu verschlüsseln und zu archivieren.

Alle Dienste werden über eine weltweit verteilte Infrastruktur bereitgestellt. Darüber hinaus kommen Kunden in den Genuss eines rund um die Uhr verfügbaren Supports durch ausgewiesene Sicherheitsexperten. Dies gewährleistet einen komfortablen und kosteneffizienten Ansatz, um Risiken durch Online-Gefahren systematisch zu minimieren und beim Austausch von Geschäftsinformationen vor unliebsamen Überraschungen gefeit zu sein. Weitere Informationen finden Sie unter www.messagelabs.com.

Unter der Internetadresse www.messagelabs.com/intelligence haben Sie die Möglichkeit, sich detailliert über die Leistungen des Geschäftsbereichs MessageLabs Intelligence zu informieren und einen News-Dienst zu abonnieren, der sie mit aktuellen Alarmmeldungen und Studien versorgt.

Hinweis: Alle in diesem Bericht genannten Zahlen waren zum Zeitpunkt der Drucklegung korrekt.

Anhang

Anhang I: Spam-Quote nach Ländern (August 2006)

Spam Rate by Geography	August 06	July 06	Change
Israel	78.0%	77.3%	0.7%
Hong Kong	66.3%	68.5%	-2.2%
Ireland	62.5%	70.5%	-8.0%
United States	61.4%	61.1%	0.3%
United Arab Emirates	58.3%	60.1%	-1.8%
Austria	58.0%	56.2%	1.8%
Germany	57.4%	60.6%	-3.2%
France	54.9%	52.0%	2.9%
Belgium	53.6%	44.1%	9.5%
Canada	51.7%	49.9%	1.8%
Netherlands	50.5%	49.7%	0.8%
United Kingdom	49.3%	56.3%	-7.0%
Singapore	46.2%	45.4%	0.8%
Spain	43.1%	45.9%	-2.8%
Sweden	42.5%	51.0%	-8.5%
Australia	41.9%	48.8%	-6.9%
Switzerland	41.3%	37.4%	3.9%
Malaysia	36.5%	36.3%	0.2%
Japan	33.0%	28.4%	4.6%
India	29.1%	23.1%	6.0%

Anhang II: Viren-Quote nach Ländern (August 2006)

Virus Rate by Geography	August 06	July 06	Change
India	1 in 13.3 (7.5%)	1 in 11.1 (9.0%)	-1.5%
Malaysia	1 in 21.2 (4.7%)	1 in 19.2 (5.2%)	-0.5%
Germany	1 in 21.3 (4.7%)	1 in 36.5 (2.7%)	2.0%
United Arab Emirates	1 in 33.1 (3.0%)	1 in 28.7 (3.5%)	-0.5%
Singapore	1 in 37.8 (2.6%)	1 in 29.9 (3.3%)	-0.7%
Ireland	1 in 38.7 (2.6%)	1 in 67.0 (1.5%)	1.1%
Spain	1 in 39.4 (2.5%)	1 in 32.3 (3.1%)	-0.6%
France	1 in 39.6 (2.5%)	1 in 43.9 (2.3%)	0.2%
Hong Kong	1 in 55.2 (1.8%)	1 in 48.9 (2.0%)	-0.2%
Switzerland	1 in 69.5 (1.4%)	1 in 73.1 (1.4%)	0.0%
Japan	1 in 85.8 (1.2%)	1 in 56.4 (1.8%)	-0.6%
Austria	1 in 88.0 (1.1%)	1 in 95.6 (1.0%)	0.1%
Sweden	1 in 91.4 (1.1%)	1 in 140.5 (0.7%)	0.4%
United States	1 in 94.8 (1.1%)	1 in 75.3 (1.3%)	-0.2%
Netherlands	1 in 95.4 (1.0%)	1 in 100.3 (1.0%)	0.0%
United Kingdom	1 in 105.9 (0.9%)	1 in 135.1 (0.7%)	0.2%
Israel	1 in 107.6 (0.9%)	1 in 108.1 (0.9%)	0.0%
Canada	1 in 116.2 (0.9%)	1 in 108.8 (0.9%)	0.0%
Australia	1 in 126.1 (0.8%)	1 in 127.6 (0.8%)	0.0%
Belgium	1 in 171.4 (0.6%)	1 in 149.2 (0.7%)	-0.1%

Anhang III: Spam-Quote nach Branchen (August 2006)

Spam Rate by Vertical	August 06	July 06	Change
Education	68.2%	67.0%	1.2%
Manufacturing	62.8%	63.9%	-1.1%
Recreation	61.8%	67.0%	-5.2%
Transport/Util	59.1%	60.7%	-1.6%
Wholesale	58.1%	54.5%	3.6%
Telecoms	57.9%	63.8%	-5.9%
Chem/Pharm	57.8%	62.7%	-4.9%
Marketing/Media	56.2%	61.1%	-4.9%
Health Care	56.1%	54.3%	1.8%
Retail	56.0%	54.4%	1.6%
Prof Services	54.3%	59.1%	-4.8%
IT Services	53.3%	55.6%	-2.3%
Mineral/Fuel	52.9%	54.5%	-1.6%
Estate Agents	51.9%	67.0%	-15.1%
Non-Profit	51.1%	55.0%	-3.9%
Accom/Catering	50.6%	51.3%	-0.7%
Building/Cons	49.0%	49.5%	-0.5%
Finance	45.0%	48.9%	-3.9%
General Services	40.0%	43.0%	-3.0%
Gov/Public Sector	37.9%	36.3%	1.6%

Anhang IV: Viren-Quote nach Branchen (August 2006)

Virus Rate by Vertical	August 06	July 06	Change
Business Support Svcs	1 in 14.5 (6.9%)	1 in 12.0 (8.3%)	-1.4%
Wholesale	1 in 33.5 (3.0%)	1 in 27.2 (3.7%)	-0.7%
Education	1 in 51.7 (1.9%)	1 in 71.1 (1.4%)	0.5%
Accom/Catering	1 in 58.3 (1.7%)	1 in 56.5 (1.8%)	-0.1%
Non-Profit	1 in 66.2 (1.5%)	1 in 64.6 (1.5%)	0.0%
Manufacturing	1 in 70.5 (1.4%)	1 in 60.8 (1.6%)	-0.2%
Mineral/Fuel	1 in 76.0 (1.3%)	1 in 72.6 (1.4%)	-0.1%
Gov/Public Sector	1 in 84.8 (1.2%)	1 in 104.2 (1.0%)	0.2%
Marketing/Media	1 in 87.4 (1.1%)	1 in 106.2 (0.9%)	0.2%
Transport/Util	1 in 95.6 (1.0%)	1 in 97.0 (1.0%)	0.0%
Retail	1 in 104.9 (1.0%)	1 in 96.7 (1.0%)	0.0%
Chem/Pharm	1 in 107.8 (0.9%)	1 in 118.4 (0.8%)	0.1%
Recreation	1 in 109.4 (0.9%)	1 in 104.1 (1.0%)	-0.1%
Prof Services	1 in 112.1 (0.9%)	1 in 114.7 (0.9%)	0.0%
Building/Cons	1 in 113.3 (0.9%)	1 in 12.0 (8.3%)	-7.4%
General Services	1 in 122.1 (0.8%)	1 in 142.1 (0.7%)	0.1%
Finance	1 in 128.0 (0.8%)	1 in 120.4 (0.8%)	0.0%
Health Care	1 in 148.1 (0.7%)	1 in 117.6 (0.9%)	-0.2%
IT Services	1 in 159.1 (0.6%)	1 in 163.1 (0.6%)	0.0%
Telecoms	1 in 216.9 (0.5%)	1 in 238.9 (0.4%)	0.1%