

Spam: Der Kampf geht weiter





Auch wer ein gut funktionierendes Anti-Spam-System einsetzt, kann immer noch sein blaues Wunder erleben. Christian Ebert, Leiter Security Services beim Kölner Telekommunikationsanbieter QSC, schildert die häufigsten Anwenderfehler sowie die wichtigsten Schutzmaßnahmen und Vorteile einer netzbasierten Filterung von Spam und Viren.

Im Kampf gegen die Flut unerwünschter E-Mails stehen Verursacher auf der einen und Entwickler von Anti-Schadsoftware auf der anderen Seite in einem ständigen Wettstreit. Schon vor gut 30 Jahren, noch lange vor der Zeit des World Wide Webs, als die ersten Rechner an das Internet-Urgestein „Arpanet“ angeschlossen waren, fanden sich die ersten Werbemails in den Postfächern ihrer Nutzer. Damals waren es nur eine Handvoll, heute sind es Millionen. Spam und Viren überfluten das Internet täglich mit neuem Datenmüll und sorgen nicht selten für immensen Schaden.

FACTS: *Herr Ebert, wie steht es um das Thema IT-Sicherheit in deutschen Unternehmen?*

Christian Ebert: Häufig werden die Gefahren aus dem Netz komplett unterschätzt. Dem normalen Menschen ist es meistens nicht klar, mit welcher ausgefeilten technischen Mitteln die Angreifer heute hantieren. Viele denken, sie wären für einen solchen Angriff kein attraktives Angriffsziel. Das ist aber ein Irrglaube! Jeder Rechner, der am Internet angeschlossen ist, stellt eine mögliche Zielscheibe dar.

FACTS: *Das müssen sie uns erklären.*

Ebert: Interessant sind nicht nur die Daten, die auf einem einzelnen Rechner gespeichert sind, sondern interessant ist auch das Gerät an sich. Die Bandbreite des Rechners ist das eigentlich Wertvolle. Solche mit eingeschleuster Schadsoftware gekaperten Rechner bilden mit ▶



CHRISTIAN EBERT: Leiter Security Services beim Kölner Telekommunikationsanbieter QSC.

› vielen anderen gekaperten Rechnern ein sogenanntes Bot-Netz, über das es möglich wird, Spam und Viren zu verschicken, die sich für weitere Angriffe nutzen lassen, um beispielsweise Webserver in die Knie zu zwingen.

FACTS: *Wie kann ich als Nutzer verhindern, dass mein Rechner von Unbekannten „gekapert“ wird?*

Ebert: Wichtig ist es vor allem, das Betriebssystem und die Applikationen stets auf dem aktuellen Stand zu halten. Am besten automatisiert. Wer keine automatische Einrichtung vornimmt, vergisst es leicht. Ein aktueller Virens Scanner und eine Firewall sind ebenfalls ein Muss. Das kann zum einen eine softwarebasierte Firewall, also eine so genannte „Personal-Firewall“ sein, oder auch eine Hardware-Lösung, die zwischen Rechner und Internet geschaltet wird. Bei einem Webserver ist die Hardware-Firewall unerlässlich.

FACTS: *Und dann bin ich vollkommen sicher?*

Ebert: Immer noch nicht. Die beste Firewall sitzt immer noch zwischen den Ohren. Das heißt, die Mitarbeiter müssen die Grundregeln des sicheren Umgangs mit dem Internet kennen. Die erste Grundregel lautet: Wenn der PC anfängt, sich unnormal zu verhalten, nicht einfach weitermachen, als wäre nichts gewesen,

sondern Hilfe hinzuziehen. Für E-Mails gilt: Auf Spam niemals antworten. Niemals reagieren. Auch nicht, wenn man sich angeblich von einem Verteiler entfernen lassen kann. Wer reagiert, bestätigt dem Versender nur die Echtheit der Mail und wird künftig mit noch mehr Werbung überflutet. Beim Schutz vor Viren sollte man vor allem auch darauf achten, niemals Dateianhänge von unbekanntem Absendern zu öffnen. Auch nicht, wenn so angeblich wichtige Dinge wie „Mahnung“ oder „Anzeige vom Bundeskriminalamt“ drinstehen. Das ist alles gelogen, die Dateianhänge enthalten Viren oder Trojaner, die das System kapern, Daten ausspähen oder zerstören.

FACTS: *Und bei E-Mails von Bekannten?*

Ebert: Auch bei E-Mails von vertrauten Absendern, die einem aber aufgrund untypischer Schreibweisen verdächtig vorkommen, sollte man nicht unbekümmert sein. Im Zweifelsfall Rücksprache halten, ob die E-Mail wirklich bewusst geschickt wurde.

FACTS: *Wie können denn die Zugangsanbieter für mehr Sicherheit sorgen?*

Ebert: Wichtig ist hier ein gutes Missbrauchsmanagement. Das heißt, die Anbieter müssen bei Beschwerden auf möglichen Missbrauch reagieren und prüfen. Bei uns ist das über die

E-Mail-Adresse abuse@qsc.de möglich. Hier überprüfen wir eingehende Beschwerden und ob von bestimmten Absendern Gefahren in Form von Spam oder Viren ausgehen. Identifizieren wir einen Rechner eines unserer Kunden als Versender schädlicher Inhalte, nehmen wir Kontakt mit dem Kunden auf und helfen, die Schadsoftware zu entfernen. Darüber hinaus bieten wir für unsere Kunden eine netzbasierte Firewall und einen ausgefeilten Spam- und Virenschutz. Hier werden die meisten Schadmails bereits aussortiert, noch bevor sie durch die Leitung zum Endkunden vordringen können.

FACTS: *Welche Vorteile bringt die netzbasierte Filterung dem Kunden?*

Ebert: Zum einen den entscheidenden Vorteil, dass die Flut an unerwünschten Daten bereits aussortiert wird, bevor sie überhaupt in Richtung Kundenleitung geht. So werden die Systeme beim Kunden nicht belastet. Zum anderen werden unsere Filter permanent aktualisiert. Beim Virenfilter raten wir dennoch zu einer Doppelstrategie: Netzbasiert filtern und zusätzlich einen Virenfilter lokal auf jedem Rechner installieren. Der Einsatz von unterschiedlichen Scannern erhöht die Trefferquote.

FACTS: *Gilt das auch für Spamfilter?*

Ebert: Nein, bei Spamfiltern reicht die netzbasierte Lösung. Zwei unterschiedliche Filter könnten sich hier in die Quere kommen und dann am Ende doch eine wichtige Mail in den Papierkorb befördern.

FACTS: *Wie effektiv kann netzbasierter Schutz vor Spam denn sein?*

Ebert: Die automatisierte Beurteilung von Spam ist nicht unkompliziert. Während sich beim Virenschutz die Schadprogramme relativ schnell anhand bekannter Strukturen erkennen und entfernen lassen, ist die Erkennung einer Werbemail subjektiv. Für den einen ist bereits ein Newsletter Spam, für den anderen eine nicht gewünschte Information. Wir ermitteln nach dem Prinzip der Wahrscheinlichkeit. So vergibt unser System Punkte für häufige Spam-Merkmale in einer E-Mail, beispielsweise welche Wörter in welchem Zusammenhang verwendet werden. Diese Kriterien werden ständig aktualisiert. Der Kunde kann individuell einstellen, ab wie vielen Punkten er möchte, ›



DATENMÜLL:
Spam und Viren überfluten das Internet täglich und sorgen nicht selten für immensen Schaden.

› dass unsere Systeme eine E-Mail als Spam einstufen und aussortieren. So lässt sich Spam auf ein erträgliches Maß reduzieren.

FACTS: *Gibt es denn keinen hundertprozentigen Schutz vor Spam?*

Ebert: Die Aufgabe eines Spamfilters ist anders als die Aufgabe eines Virenfilters. Ein Virenfilter muss unter allen Umständen verhindern, dass ein Virus hindurchkommt. Ein Spamfilter hat nur die Aufgabe, unerwünschte Mails zu reduzieren. Er darf keine E-Mail fälschlicherweise blockieren. Ein Virus, der durchkommt, kann hohen Schaden verursachen. Eine Spam, die durchkommt, kann man löschen. Aber eine wichtige E-Mail, die fälschlicherweise entfernt wird, kann ebenfalls einen hohen Schaden be-

deuten. Deswegen wird es immer sinnvoll sein, einen Spamfilter so einzustellen, dass ein kleiner Teil Spam durchkommt, aber ganz sicher alle legitimen E-Mails ihren Empfänger erreichen.

FACTS: *Steigt denn die Anzahl der Spam-Mails weiter an?*

Ebert: Die steigt immer noch exponentiell. Spam kommt immer in Wellen. Und jede Welle ist höher als die vorangegangene. Es ist ein Wettrüsten. Dadurch, dass die Abwehrmaßnahmen immer ausgefeilter werden, werden die Spammer in ihren Konzepten immer aggressiver, um überhaupt noch Werbebotschaften versenden zu können. Das Problem dabei: Diejenigen, die keine Abwehrmaßnahmen treffen, oder nur unzureichende, werden immer

härter getroffen. Wer professionell geschützt ist, hat kaum noch Probleme mit Spam.

FACTS: *Wenn wir doch alle so von Spam genervt sind, warum gibt es dann noch so viel davon? Was haben die Versender für einen Nutzen?*

Ebert: Solange jede zehntausendste oder gar hunderttausendste E-Mail zum Erfolg führt, lohnt es sich für die Spammer, ihre Mails millionenfach zu verschicken.

FACTS: *Wir könnten Spam also nur dann aus der Welt schaffen, wenn wir alle nicht mehr darauf reagieren würden.*

Ebert: Richtig. Aber das ist wohl ein sehr frommer Wunsch.

Graziella Mimic ■