

«False Positives» in der Spam-Abwehr

Der Anwender muss entscheiden, was Spam ist und was nicht

Anbieter von E-Mail-Diensten gehen in jüngster Zeit immer öfter dazu über, die Leistung ihrer Spam-Filter mithilfe der «False-Positive-Rate» anzupreisen. Ist es aber tatsächlich ein Leistungsmerkmal, wenn nur wenige E-Mails irrtümlich als Spam-Mails erkannt werden? Wenn es nicht brennt – ist das dann ein Zeichen dafür, dass die Feuerwehr gut arbeitet? Betrachtet man die Versprechen einiger Anbieter von Anti-Spam-Lösungen, gewinnt diese Frage erheblich an Bedeutung.

 *inik Obrist*

Die Vielzahl an Produkten und Anbietern von Managed-Mail-Diensten mit sehr unterschiedlichen Tarifstrukturen machen einen Preis- und Angebotsvergleich erforderlich. Dabei ist es nur verständlich, dass sich der Blick auf jene Services lenkt, deren Auswirkungen für den Anwender am leichtesten nachvollziehbar sind: die Abwehr von Viren und sonstigem Schadcode sowie das Herausfiltern unerwünschter Werbe-Mails, also Spam.

Bewertung schwierig

Die Qualität einer Viren-Abwehr lässt sich noch am ehesten bewerten, auch wenn es hier keine hundertprozentige Sicherheit gibt: Erreicht kein Virus die Festplatte des Anwenders, sind alle glücklich. Kommen immer wieder Schaden stiftende E-Mails durch, hat man womöglich den falschen E-Mail-Provider engagiert. Wie aber bewertet man die Qualität von Spam-Filtern? Auch dies klingt auf den ersten Blick einfach: Je

weniger unerwünschte Werbe-Mails im Posteingang landen, umso besser ist der Spam-Filter. Schade nur, dass die Welt nicht



so einfach ist. Verhielte es sich nämlich so, dann könnte man die Leistung der Feuerwehr tatsächlich daran bemessen, ob – oder wie oft – es brennt.

Wo brennts?

Die Welt ist nicht so einfach, denn für einen Spam-Filter reicht es nun mal nicht aus, alles, was auch nur ansatzweise nach Werbe-Müll aussieht, in den Mülleimer zu werfen. Ein Filter darf keine unüberwindliche Barriere sein, sondern muss die Spreu vom Weizen trennen und dabei Ersterer vom Anwender fernhalten, Letzteren hingegen passieren lassen. Dies allerdings ist eine echte Herausforderung: Stellen wir uns nur einen Anwender vor, der tatsächlich per E-Mail und Internet teure Luxus-Uhren oder Potenz-Pillen erwerben will. Das ist schliesslich nicht verboten. Ebenso wenig ist es untersagt, dass auch seriöse Absender ihre Geschäfts-E-Mails so sehr mit Firmenlogos, Bildchen und Internet-Links anreichern, dass sie am Ende aussehen wie Spam. Die letztgültige Entscheidung, ob eine E-Mail

eine sinnvolle Nachricht ist oder eben nur lästiger Werbe-Müll, liegt beim Anwender. Dessen Geduld allerdings mag kein Anbieter überstrapazieren, denn sonst könnte der ja auf die Idee kommen, den falschen Mail-Service-Provider engagiert zu haben. Folglich richtet sich das Bestreben der Provider darauf, die Anzahl der E-Mail-Nachrichten, die fälschlich als Spam eingestuft werden – man spricht hier von den sogenannten «False Positives» – möglichst gering zu halten. So ist es kein Wunder, dass diese False Positives oftmals zu Werbezwecken herangezogen werden.

False-Positive-Rate

Wie beziffert man nun eine False-Positive-Rate? Das hat in erster Linie damit zu tun, wie der jeweilige Provider mit den als Spam eingestuften E-Mails umgeht. Wie erwähnt, ist es ziemlich einfach, alles, was auch nur im Ansatz nach Spam aussieht, in den Müll-eimer zu werfen. Damit wären wir schon mal bei einer False-Positive-Rate von null Prozent. Alle Spam-Mails wurden korrekt identifiziert, alle sinnvollen Nachrichten wurden ordnungsgemäss zugestellt, wir sind Weltmeister und alle sind glücklich. Schade nur, dass das niemand glaubt.

Besser geht es nicht

Um also weder die eigene Glaubwürdigkeit noch den Weltmeister-Titel zu gefährden, wartet man einfach mal ab, ob es nicht doch den einen oder anderen Anwender gibt, der erboht anruft und sich bei der Hotline des Service-Providers darüber beschwert, dass eine lang erwartete und wichtige E-Mail nicht zugestellt wurde. Nachdem es tatsächlich Anbieter von Mail Services gibt, die mit einer «0,00001-Prozent-False-Positive-Rate» und «mehr als 99,99999 Prozent korrekt erkannten Spam-Mails» werben, können wir im Kopf ausrechnen, dass dieser Fall einmal alle zehn Millionen E-Mails vor-

kommt, also nur viermal wahrscheinlicher ist als ein Sechser im Lotto.

Eine andere Möglichkeit bestünde darin, die Wahrscheinlichkeit, dass es sich bei einer E-Mail um Spam handelt, zu beziffern. Dies ist eine Standardfunktion der meisten Spam-Filter und unter anderem der Tatsache geschuldet, dass nicht alle Spam-E-Mails den Erwerb von Rolex-Uhren oder Viagra-Pillen empfehlen. Hier besteht die Option, dem Anwender nicht nur die «sauberen» Nachrichten zu übermitteln, sondern zusätzlich auch die Top Ten jener E-Mails, bei denen es sich möglicherweise doch nicht um Spam handelt. Gehen wir davon aus, dass 95 Prozent aller E-Mail-Nachrichten Spam sind (die tatsächliche Zahl liegt deutlich darüber), dann würde allein das Durchlassen jener zehn Prozent E-Mails, die noch am ehesten sinnvolle Inhalte transportieren könnten, das E-Mail-Aufkommen des Anwenders am Ende der Leitung verdreifachen. Damit entstünde fraglos der Eindruck, dass die Feuerwehr womöglich doch nicht so gut arbeitet – und mit dem Weltmeister-Titel wäre es auch nichts. Damit dürften die einfachen Möglichkeiten, den Anwender vor Spam zu schützen und dennoch alle sinnvollen Nachrichten durchzustellen, ausgeschöpft sein. Um einen – im Sinne des Anwenders – sinnvollen Umgang mit False Positives zu gewährleisten, müssen schwerere Geschütze aufgeföhren werden.

Es geht auch anders

Fakt ist: Einen vergleichbaren, allgemeingültigen und – im Sinne des «schneller, höher, weiter» – messbaren Standard für die Leistungsfähigkeit eines Spam-Filters gibt es nicht und es kann ihn wohl auch nicht geben. Daher wird sich ein seriöser E-Mail-Service-Provider stets darum bemühen, die Entscheidung, was als Spam einzustufen ist und was nicht, da zu belassen, wo sie – nicht zuletzt auch aufgrund des Postgeheimnisses – hingehört: beim Anwender

nämlich. Dazu allerdings muss einiger technischer Aufwand betrieben werden. Der beginnt damit, dass E-Mails, die als Spam erkannt wurden, nicht einfach gelöscht, sondern gespeichert werden. Dies allerdings nicht im Posteingang des Anwenders, sondern auf den Servern des Providers, wo die mutmasslichen Spam-Mails zunächst unter Quarantäne gestellt werden.

Um sich nun selbst davon überzeugen zu können, dass hier keine Nachrichten von Belang sind, erhält der Anwender regelmässig Mitteilung, welche Mails unter Quarantäne gestellt wurden. Um ihn gleichzeitig vor möglichen Schadcodes zu schützen, reicht es aus, lediglich den Absender und den Betreff der mutmasslichen Spam-Mail zu nennen. Entscheidet ein Anwender, dass er eine dieser E-Mails dennoch zur Kenntnis nehmen will, kann er diese innerhalb des definierten Quarantäne-Zeitraums abrufen (ausser virenbehaftete E-Mails versteht sich). Geschieht dies nicht, geht die Spam-Mail am Ende der Quarantäne den Weg allen Irdischen.

Fazit

Ein solches Vorgehen birgt wenig Chancen auf einen Weltmeister-Titel und ist zudem für den Service-Provider mit Kosten verbunden, die keineswegs trivial sind. Gleichzeitig aber belässt es die Entscheidung, was Spam ist und was nicht, beim Anwender und ist zudem deutlich seriöser als die Option, Rekordmarken dadurch zu erreichen, dass man auf Kosten des Anwenders spart. ■

Kontakt



Dominik Obrist

Country Manager Schweiz

Retarus (Schweiz) AG

Badenerstrasse 623, 8048 Zürich

Tel. 043 336 20 10

info@retarus.ch

www.retarus.ch