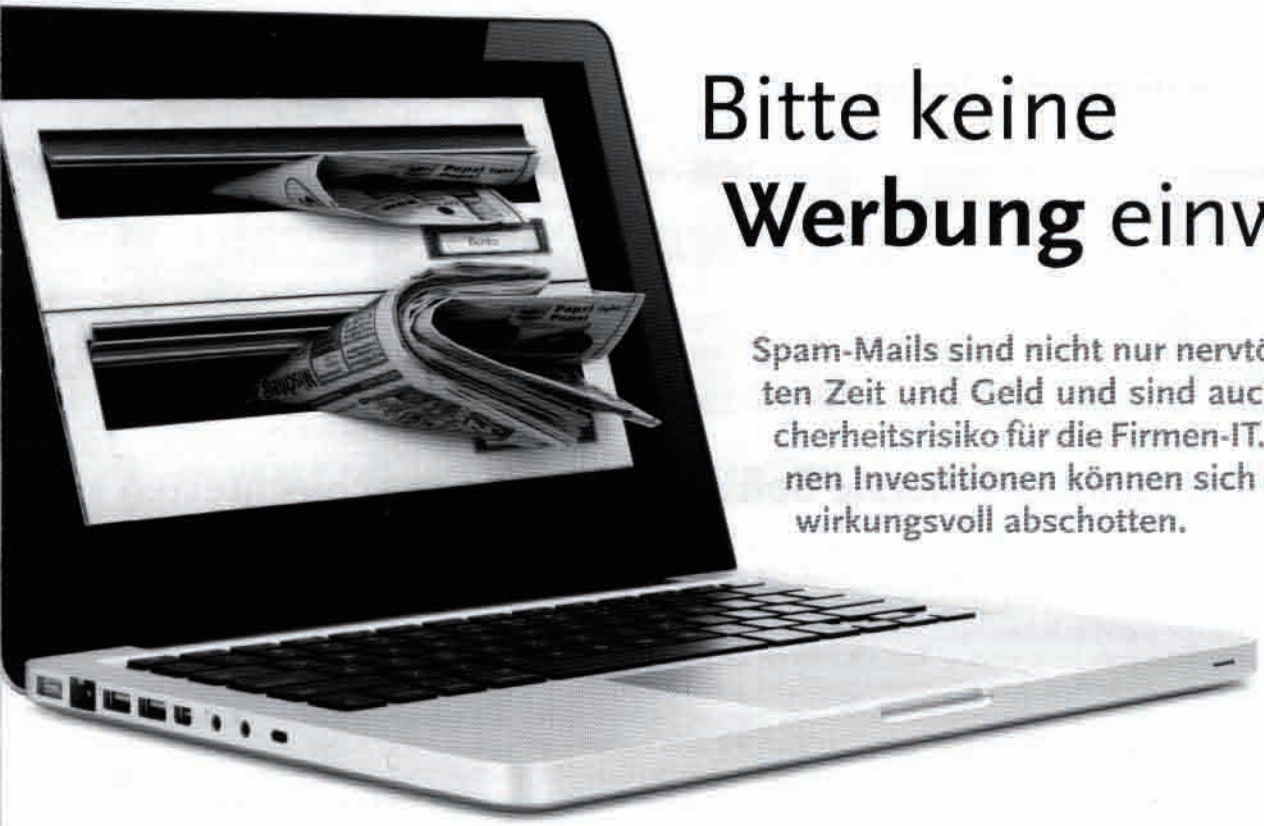

Bitte keine **Werbung** einwerfen!

Spam-Mails sind nicht nur nervtötend. Sie kosten Zeit und Geld und sind auch noch ein Sicherheitsrisiko für die Firmen-IT. Doch mit kleinen Investitionen können sich Unternehmen wirkungsvoll abschotten.

Im unterfränkischen Örtchen Urspringen finden Millionen Spam-Mails täglich ein trauriges Ende – traurig für ihre Absender, nicht für die Empfänger. „Für viele Unternehmen und Behörden sind wir die Türsteher für ihre E-Mail-Postfächer", sagt Andreas Hoffmann, Geschäftsführer der ETHA Elektronik GbR und Erfinder von Spam-Sperre.de. Die Software soll unerwünschte E-Mails bereits im Internet abfangen, damit sie nicht in die IT-Infrastruktur der Kunden eindringen und diese beeinträchtigen können. Und weil das System betroffene Mails direkt zurücksendet, verschwindet auch nichts unbemerkt in den Tiefen von Spam-Ordnern. Zur Einrichtung benötige man laut Anbieter keinen Techniker vor Ort und kein Gerät – alles lasse sich per Internet in etwa 15 Minuten einrichten.

„Wir erkennen Spam an vielen Merkmalen, die wir stündlich aktualisieren", so Geschäftsführer Hoffmann. Wie genau das funktioniert? „Betriebsgeheimnis", sagt er nur und fügt dann hinzu, dass er über einen fast besessenen Programmierer verfüge, der die Spam-Symptome so genau diagnostiziere wie ein Virologe, der ein ständig mutierendes Virus im Zaum halten muss.

Denn die Spammer haben ihren Ehrgeiz. Als im November 2008 der kalifornische Webhosting-Provider McColo vom Netz getrennt wurde, der von

Kriminellen zur Steuerung der Spamflut missbraucht worden war, sank das weltweite Spam-Aufkommen zwar zunächst schlagartig um mehr als 60 Prozent. Doch schon Anfang Februar hatten die Spammer den Schaden wieder wettgemacht. „Die Schnelligkeit, mit der sie ihre Infrastrukturen wieder aufgebaut haben, zeigt, wie flexibel sie auf widrige Umstände reagieren können", sagt Robert Rothe, Geschäftsführer des deutschen E-Mail-Sicherheitsanbieters Eleven, der mehr als 30.000 Unternehmen – unter anderem T-Online – betreut. „Vor allem sind die Spammer lernfähig."

Eleven hat während der CeBIT im März rund 300 IT-Verantwortliche deutscher Firmen zur IT-Sicherheit befragt. Mehr als 40 Prozent nannten die Belastung der IT-Infrastruktur durch Spam als größte Gefahr. Robert Rothe warnt aktuell vor der Nutzung so genannter Botnetze. „Die Spammer bedienen sich legitimer Infrastrukturen." Das heißt: Es werden Programme ohne Wissen des Anwenders auf seinem Rechner installiert und ausgeführt. Die ferngesteuerten Rechner sind untereinander vernetzt und senden heimlich Spam-Mails von legitimen Adressen ab. Damit werde es schwieriger, Spam zu identifizieren.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) spricht in

Link-Service

Weiterführende Informationen erhalten Sie, wenn Sie eine Mail mit „Spam" im Betreff an creditreform-service@vhb.de senden.

seinem Lagebericht 2009 in diesem Zusammenhang von „organisierter Kriminalität". „Im Internet kann man Botnetze mieten und sich zum Spam-Versand mit anderen zusammenschließen." Ein Botnetz aus 1.000 infizierten Rechnern könne die Infrastruktur vieler kleiner Unternehmensnetze lahmlegen.

Neue Viren sofort erkennen

Der Anteil von Spam-Mails am E-Mail-Verkehr hat sich laut BSI weiter erhöht. Von 100 empfangenen Mails seien statistisch gerade einmal 1,5 gewollt. Dabei würden die Inhalte immer individueller: Der Empfänger wird persönlich angesprochen, der Inhalt ist nicht sofort als Spam erkennbar, die Qualität der Texte hat sich verbessert. Ausdrücklich warnt das BSI kleine und mittelständische Unternehmen davor, an der IT-Sicherheit zu sparen. „Angriffe durch neue und komplexe Techniken sind zunehmend schwerer zu bekämpfen", so BSI-Präsident Udo Helmbrecht.
„Die Herausforderung für uns ist auch, neuartige Schädlinge sofort zu erkennen", erläutert Robert Rothe von Eleven. An einigen Tagen gebe es bis zu 25 Ausbrüche neuer Viren. „Die kritische Zeit sind ja die zwölf bis 48 Stunden direkt nach Ausbruch", so Rothe. Wenn Eleven da nicht sofort reagieren würde, könne der Schaden nicht abgewendet werden.
Eine andere Qualität der E-Mail-Sicherheit ist für Rothe die Einhaltung deutscher Datenschutzrichtlinien. „Unternehmen sollten sehr sorgfältig prüfen, wem sie ihre Mailsicherheit anvertrauen." Denn nur ein Unternehmen, das bei einem deutschen Rechenzentrum gehostet sei, müsse auf Grundlage des deutschen Datenschutzes arbeiten.

Rothe beobachtet, dass das Bewusstsein für IT-Sicherheit in allen Unternehmen steige. Vor allem nehme die Nachfrage nach ausgelagerten Diensten zu. So bietet Eleven an, die Schutz- und Prüfmaßnahmen auf seinen Servern durchzuführen. Das sei

vor allem für kleinere Unternehmen interessant, die keine eigene IT-Abteilung haben. Außerdem habe es den Vorteil, dass Spam und Viren den Server des Unternehmens gar nicht erst erreichen.

Risiken in sozialen Netzwerken

Das BSI will auch für persönliche Daten in Mitmach-Anwendungen des Web 2.0 sensibilisieren. Cyberkriminelle könnten potenzielle Opfer dort ausspionieren und gezielt angreifen. Das Fraunhofer Institut für Sicherheit in der Informationstechnologie (SIT) hat dazu bereits eine komplette Studie erstellt, die sich mit privaten Daten in sozialen Netzwerken beschäftigt (siehe Linkservice auf Seite 42). So sollten die Nutzer bei geschäftlichen Plattformen wie Xing und LinkedIn darauf achten, ihre Angaben aufs Berufliche zu beschränken. Wer auch Hobbys dort angibt, kann schnell entsprechende Spam-Mails in seinem dienstlichen Postfach finden. Andererseits warnen die Forscher auch davor, in solchen Plattformen private Mailadressen mit Nicknamen zu benutzen. Es sei beispielsweise denkbar, anhand der Mailadresse schnorcheltaucher78@... den Nicknamen schnorcheltaucher78 in Diskussionsforen aufspüren und ihn damit zu identifizieren – das kann mitunter peinlich sein.
Mit einem Abflachen der Spamflut ist nicht zu rechnen. Denn für Spammer sind Kosten und Aufwand minimal, und ein bisschen Umsatz springt immer heraus. Das Spam-Aufkommen repräsentativer deutscher Unternehmen ist zwischen Juli 2005 und April 2008 um mehr als 10.000 Prozent gewachsen. „Gerade bei Angeboten wie Potenzmitteln, die von der Anonymität im Netz leben, können Spammer Kasse machen", so Andreas Hoffmann von Spam-Sperre.de. Denn die meisten Angebote sind zwar Plagiate, Raubkopien oder Hehlerware – sie würden aber dennoch bei einem Kauf wirklich geliefert.

Christina Kiesewetter

Checkliste I Gute Spamfilter

1. Es sollten nicht mehr als 0,00001 Prozent aller E-Mails fälschlich als Spam erkannt werden. Denn im schlimmsten Fall können Unternehmen damit Aufträge verlorengehen. Liegt die sogenannte False-Positive-Rate zum Beispiel nur bei 0,001 Prozent, können in einem großen Unternehmen mit einer Millionen E-Mails täglich zehn Nachrichten verloren gehen.
2. Ein guter Spam-Filter sollte mindestens 99 Prozent aller Spams erkennen.
3. Nutzer und Administrator sollten keine Wartungsarbeiten durchführen müssen.
4. Die Prüfung der E-Mails sollte nicht dazu führen, dass Mails merklich verzögert beim Empfänger ankommen oder nennenswert Rechenkapazität beansprucht wird.
5. Es sollte sichergestellt sein, dass Spamfilter keinen Zugriff auf die Inhalte der überprüften E-Mails haben.

(Quelle: Eleven-Whitepaper „E-Mail-Sicherheit im Unternehmen")

Hintergrund I Die Rechtslage

Zulässig ist E-Mail-Werbung nur, wenn der Empfänger der Werbung vorher zugestimmt hat oder sein Einverständnis vermutet werden kann, weil zwischen Versender und Empfänger zum Beispiel eine Geschäftsbeziehung besteht. Ist eine Spam-Mail nicht sofort als kommerzielle Werbung zu erkennen, verstößt sie gegen das Gesetz gegen unlauteren Wettbewerb (UWG). Der Empfänger soll allein durch Kopf- und Betreffzeile erkennen können, dass es sich um eine Werbenachricht handelt und wer der Absender ist. Der illegale Versand von Spam-Mails kann mit einem Bußgeld bis zu 50.000 Euro bestraft werden. Auch zivilrechtlich können Schadensersatz und Unterlassung geltend gemacht werden. In der Praxis ist es aber in der Regel zwecklos, rechtlich gegen Spammer vorzugehen, denn sie agieren mit gefälschten E-Mail-Adressen, sitzen im Ausland und sind kaum dingfest zu machen. Realistisch sind die Chancen nur bei einer deutschen Spam-Mail mit klarem Urheber und Absender. Mehr Informationen: www.recht-im-internet.de/themen/spam