Die Rückkehr zum Fax

Spam zerstört Email als Kommunikationsmittel

Jan Manuel Tosses

12. November 2004

Zusammenfassung

Was ist Spam, woher kommt er und welchen Schaden richtet er an? Wie gibt sich Spam zu erkennen, mit welchen Mitteln wird er bekämpft und was kann man selbst dagegen tun? Worin unterscheiden sich Spam, Scam und Phishing? Der nachfolgende Artikel beschäftigt sich mit Antworten zu diesen Fragen und liefert wichtige Tipps und Tricks im Kampf gegen unerwünschte Emails.

1 Was ist Spam und wo kommt er her?

Spam ist ganz allgemein Email, die der Empfänger nicht bestellt hat und auch nicht haben will. Spam kommt ebenso von Kleinunternehmern, Kriminellen und Geschäftemachern - aber auch von Geschäftsleuten, die sich mit den scheinbaren Vorzügen des offensichtlich schnellen Kommunikationsmittels Email befassen. Spam ist so nahliegend wie Postwurfsendungen und Mailing Aktionen. Jedem, der Email einmal benutzt hat, drängt sich Spam als perfekte und beinahe kostenfreie Werbemöglichkeit regelrecht auf. Mit nur einem Klick erreicht der Versender tausende, meistens sogar Millionen Empfänger. Dabei nimmt er billigend in Kauf, dass auch andere diese plausible Werbeform für sich nutzen. Auch Verbrecher haben diese einfache Form, Kontakt zu ihren Opfern aufzunehmen, für sich entdeckt. Mit Scam und Phishing Attacken starten sie immer häufiger ihre Raubzüge im Internet.

2 Woran erkennt man Spam, woran Scam, was ist ein Hoax und was Phishing?

Man unterscheidet heute zwischen Spam, Scam und Phishing. Dabei ist Spam fast ein Oberbegriff für unerwünschte Email, genauer aber meint man damit unerwünschte Werbenachrichten. Mailing Aktionen und Newsletter mögen nach einer Weile zwar wie Spam wirken, fallen aber dank vorheriger Opt-In Registrierung genau genommen nicht in diese Kategorie. Opt-In bedeutet im Gegensatz zu Opt-Out, dass man sich explizit für einen optionalen (Opt-) Empfang entschieden (In) hat. Zu den Details des Opt-Out kommen wir später noch. Als Scam bezeichnet man generell Email, die in betrügerischer Absicht formuliert und versendet wurde. Zum verbreitetsten Vertreter der Scam Email gehören vor allem die scheinbaren Angebote der so genannten Nigeria Connection, die dem

Opfer auf unterschiedlichste Arten eine lukrative Teilnahme an Geldverschiebungen in Aussicht stellen, für die die Opfer nur ihre Kontendaten zu übermitteln haben. Da die Nachrichten zum Teil sehr subtil aufgebaut sind und die Verbrecher äußerst geschickt vorgehen, führen diese Delikte weiterhin zum Erfolg. Das Phishing (von fishing mit PH geschrieben) ist nun eine sehr moderne Spielart der Scam Emails. Hier wird dem Opfer eine offiziell anmutende Email einer Bank, eines Kreditkartenunternehmens, oder einer Versicherung geschickt. Nach einer kleinen Geschichte wird dem Opfer der Besuch der Unternehmensseite nahegelegt und gleich ein passender Link mitgeliefert. Diese Links verbergen die tatsächliche Adresse, zu der das Opfer geleitet werden soll. Hinter ihr verbirgt sich natürlich nicht der Server des Unternehmens, von dem die Email scheinbar stammt, sondern ein Server des Betrügers. befindet man sich nun auf der Seite, wird einem nahegelegt, Anmeldedaten einzugeben, um auf das System zuzugreifen. Ist man "angemeldet", wird man zur Eingabe nahezu aller persönlichen Daten aufgefordert, was mit verschieden plausiblen Begründungen einhergeht. Die gewonnenen Daten werden vom Betrüger dann dazu verwendet, um nach Belieben Konten zu plündern, oder die Identität des Betroffenen für seine Aktivitäten zu verwenden. Die Zeche zahlt dann das Opfer.
Unter einem Hoax versteht man im Internet ein Gerücht, das zumeist per Kettenmail verbreitet wird. Der Autor erzählt dabei meistens eine plausible Geschichte mit der Bitte um vielfache Weiterleitung an Freunde und Bekannte. Hoaxe haben schon ganze Rechnernetze dadurch lahm gelegt, dass sie nicht nur "an alle" versendet wurden, sondern danach auch noch von nahezu jedem Rezipienten beantwortet wurden.

3 Woher nehmen die Versender ihre Adressaten?

Die Adressen der Spam Empfänger werden zum einen generiert, indem gängige Vor- und Nachnamen Paare vor bekannte Internet Domänen gehängt werden. Zum Beispiel ist ein Benutzer "Hans Schmidt" beim, in Deutschland weit verbreiteten, Dienstleister Web.DE sehr wahrscheinlich. Daher werden verschiedene Schreibweisen des Namens einfach ausprobiert:
"h.schmidt@web.de", "hans.schmidt@web.de", "schmidt.h@web.de"
Andererseits werden Adressen auch gekauft und "geerntet". So lassen sich Email Adressen zum Beispiel sehr einfach aus Webseiten oder aus den Antworten auf Hoax Emails und Phishing Attacken gewinnen. Gilt eine Adresse als bestätigt, das heisst, befindet sich hinter der Adresse ein Mensch, so steigt ihr Wert und sie wird gewinnbringend verkauft. Gerne hängen Spam Verfasser so genannte "Opt-Out" Links an die Spam Email. Scheinbar kann man sich über diese aus dem vermeintlichen Verteiler austragen lassen. Tatsächlich steigert man aber nur den Verkaufswert seiner Email Adresse. Links in Spam Emails sind für Gewöhnlich fest mit der Email Adresse des Empfängers verdrahtet, ebenso, wie die Bilder. Zeigt das Email Programm also Bilder an, oder klickt der Leser auf einen Link in der Spam Email, sendet er dem Autor ein Lebenszeichen und hat künftig mehr Spam im Posteingang.

4 Wo liegen die Gefahren des Spam? Wozu führt Spam?

Gefährlich wird eigentlicher Spam erst, wo er ablaufkritische Kommunikation verhindert. Solche Verhinderung kann auftreten, wo wichtige Email in Massen von Spam untergeht, aber auch da, wo Filtermechanismen wichtige Email als Spam zu erkennen glauben und vor dem wartenden Empfänger verbergen. Die Gefahren in betrügerischer Absicht verfasster Email, liegen auf der Hand, hier wird direkt in den Geldbeutel des Betroffenen gegriffen. Durch die Unsicherheiten, die Spam mit sich bringt, werden in der Unternehmenskommunikation viele praktische und kostensparende Schritte teils mehrfach vollzogen, teils durch weitere, im eigentlichen Ablauf nicht vorgesehene Schritte, ad Absurdum geführt. So ist es heute vorherrschende Praxis, einer Email, einen Anruf oder ein Fax folgen zu lassen. Auch wird gerne vor versenden einer Nachricht angerufen und beharrlich darauf gewartet, dass der Kommunikationspartner den Empfang der Sendung bestätigt. Dies führt natürlich dazu, dass Email all ihre Vorteile verliert und nur noch ihre Nachteile zum tragen kommen. Email kostet Zeit, anstatt sie zu sparen, ist kompliziert, anstatt Prozesse einfacher und transparenter zu gestalten, belastet, anstatt zu helfen.

5 Wie wird Spam bekämpft und was kann man selbst gegen Spam tun?

Es gibt unterschiedlich wirksame Mittel, Spam zu bekämpfen. Auf drei einfache Punkte reduziert ergibt das: erkennen, filtern, ignorieren. Spam zu erkennen ist nicht immer einfach, jedoch entwickelt man mit der Zeit ein geübtes Auge dafür. Ebenso, wie Menschen lernt hier auch die Filtersoftware, wie neuer Spam aufgebaut ist und nach welchen Kriterien die eingehende Post zu filtern ist. Ist mal eine Spam Email durchgerutscht und doch im Posteingang gelandet, "füttert" man jene an den Spam Filter und die nächste Spam Email derselben Sorte kommt voraussichtlich nicht mehr durch. Es gibt viele Produkte, die mit unterschiedlichen Methoden gegen Spam eingesetzt werden. Manche laufen schon auf dem Email Server, manche erst im Email Programm. Die server basierten prüfen die Netzwerkadresse des Versenders gegen Listen mit spam auffälligen Versendern ab und verweigern bei Übereinstimmung die Annahme. Auf Servern und in Email Programmen laufen gleichermaßen Filter, die bestimmte Merkmale in eingehenden Emails bewerten. Für jeden Verdachtsmoment erhält die Nachricht Punkte, je mehr Punkte die Nachricht sammelt, desto wahrscheinlicher ist sie Spam. Je niedriger die Punkte Akzeptanz des Filters eingestellt ist, desto mehr Spam wird erkannt und ausgefiltert. Der große Nachteil dieser Methode ist, dass mit dem Spam auch wichtige Email wegsortiert wird, je schärfer der Filter eingestellt ist. Spam Versender füllen ihre Nachrichten mit Textpassagen aus der Literatur auf, um solche Filter zu blenden. Je niedriger also die Toleranz eingestellt ist, desto mehr wirkt normale Email im Verhältnis zu Spam wie unerwünschte Post. Weitere Filtermethoden sind zum Beispiel die Überprüfung der Sender Adresse darauf, ob sie berechtigt ist, Email zu versenden. Leider waren solche Prüfungen im, auf gegenseitigem Vertrauen basierenden, Email System nicht vorgesehen und brechen heute viele sinnvolle Standards, die einfa-

che Kommunikation im Internet ermöglichen sollen. Einen umfassenden Schutz vor Spam gibt es leider ebenso wenig, wie eine absolut sichere Methode, ihn von erwünschter Email zu unterscheiden.

6 Tipps und Tricks im Umgang mit unerwünschter Email

Zum Abschluss noch ein paar Tipps und Kniffe für dem alltäglichen Umgang mit unerwünschter Email:

1. Niemals antworten! Stellen Sie sich tot, reagieren Sie bloß nicht! Sobald der Versender weiß, dass sich hinter Ihrer Adresse ein lebendiger Mensch befindet, steigt der Wert Ihrer Adresse enorm an. Der Versender nimmt Sie, wenn Sie es wünschen zwar aus dem Verteiler, verkauft jedoch Ihre Adresse sofort für klingende Münze an zahllose neue Verteiler. Tragen Sie sich nicht per "Opt-Out" aus angeblichen Verteilern aus, in die Sie sich nicht selbst eingetragen haben.

2. Selbstverständlich darf man natürlich keines der, auf diese Weise beworbenen Produkte erwerben! Dies bestärkt Spam Versender nur in ihrem "Vermarktungskonzept".

3. Stellen Sie in Ihrem Emailprogramm die Darstellung aktiver Inhalte und eingebetteter Bilder ab! Bilder, die in so genannter HTML Email nachgeladen werden, verwenden dazu spezielle Adresse, die schliesslich zu Ihrer Email Adresse zurück verfolgt werden. Auch hier steigert sich der Wert der Adresse durch die Lebenszeichen.

4. Tragen Sie Ihre Email Adresse nicht wahllos in Internet Formulare ein. Prüfen Sie sorgfältig, ob die Nachfrage nach Ihrer Adresse überhaupt für den aktuellen Vorgang nötig ist. Vertrauen Sie nicht blind den Angaben der Webseiten, geben Sie im Zweifel lieber unnütze Daten ein, falls es sich um ein Pflichtfeld handelt.

5. Ihr Bank, Ihre Versicherung, Ihre Kreditkartengesellschaft, Ihr Internet oder Mobilfunk Dienstleister; sie werden alle niemals nach Ihren Kenndaten fragen! Erhalten Sie Eine Email mit der Aufforderung, solche Daten anzupassen, fragen Sie vorher beim (scheinbar) nachfragenden Institut nach. Wählen Sie dazu keine der Nummern, die in der Email angegeben sind, sondern suchen Sie diese aus der vergangenen Korrespondenz!

6. Seien Sie misstrauisch! Wer in der Vergangenheit in deutscher Sprache mit Ihnen kommunizierte, wird sein Verhalten vermutlich nicht einfach ändern. Fragen Sie im Zweifel besser nach.

7. Niemand hat etwas zu verschenken, auch im Internet nicht! Dubiose Geschäftsangebote sollen immer nur einen bereichern, den Versender. Vollmundige Versprechungen über leicht verdientes Geld können nur Betrug bedeuten.

8. Antworten Sie nicht auf Emails mit obskurem Inhalt, mit Virenbenachrichtigungen, mit Rückfragen nach Ihrer Meinung, mit Unterstützungsgesuche für todkranke Kinder, bettelarme Studierende, entzweite Familien

und dergleichen - diese dienen vor allem der Sammlung von Adressen, hinter denen lebendige Menschen stehen.

9. Installieren Sie Spam Filter Programme in Ihrem Email Programm. Diese sortieren vermeintlichen Spam in spezielle Ordner. Löschen Sie die Emails nicht sofort, sondern schauen Sie regelmäßig nach, ob auch nur Spam aussortiert wurde. Trainieren Sie den Filter mit Spam, der nicht entdeckt wurde. Lassen Sie sich bei der Wahl und Installation des geeigneten Filter Systems fachkundig beraten.