Inhalt

STEFANIE HEYDUCK

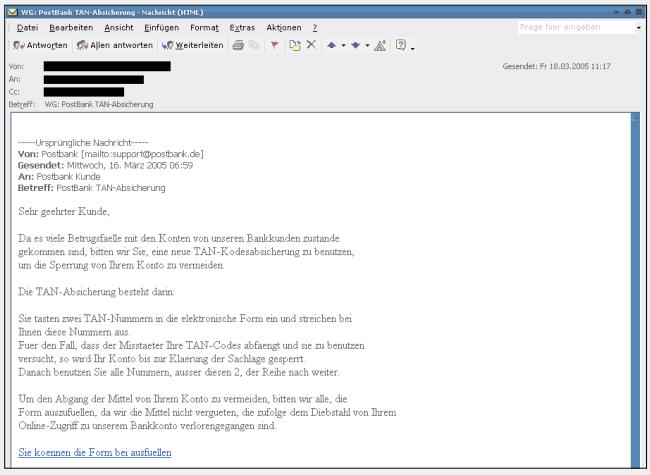
DIGITALER MÜLLBERG

Spam ist die digitale Pest. Trotz fortgeschrittener Filtertechniken reißt die Flut nicht ab und verursacht jährlich Schäden in Milliardenhöhe. Business&IT sprach mit Experten über Entwicklung und Gegenwehr.

Charles Booher droht mit Anthrax-Post, Folter mit Schlagbohrer und Eispickel, erbarmungsloser Jagd, Kastration und Mord: keine Szene aus *Falling Down* mit Michael Douglas, sondern der verzweifelte Kampf eines Programmierers aus Kalifornien gegen Spam. Nachdem er monatelang mit E-Mails zum Thema Penisverlängerung bombardiert wurde, ist er ausgeflippt. Ihm drohten fünf Jahre Gefängnis und eine Geldstrafe von 250000 US-Dollar – vor der Urteilsverkündung nahm er sich das Leben. Ein tragisches Beispiel für die erschreckenden Ausmaße, die Spam annehmen kann. MessageLabs gibt an, dass mittlerweile fast 70 Prozent aller E-Mails Spam sind.

Die digitalen Postwurfsendungen werden häufig auch als Junk-Mail, Bulk-Mail oder Unsolicited Commercial E-Mail (UCE) bezeichnet. Spam ist immer anonym und unerwünscht – im Unterschied zu Mailing-Listen und Newsletter, die zwar werblich sein können, aber legitim sind.

In den letzten Jahren hat Spam eine bedrohliche Entwicklung vollzogen. In einem aktuellen Bericht von Ferris Research gehen Analysten davon aus, dass Spam in diesem Jahr weltweit Schäden in Höhe von 50 Milliarden US-Dollar verursachen wird. Allein in Deutschland sollen es 4,5 Milliarden US-Dollar sein. Diese Summe resultiert daraus, dass Spam Speicher und Bandbreiten verbraucht und das tägliche Durch-


WG: PostBank TAN-Absicherung - Nachricht (HTML)

Datei Bearbeiten Ansicht Einfügen Format Extras Aktionen ?

Antworten Allen antworten Weiterleiten

Von:
An:
Cc:
Betreff: WG: PostBank TAN-Absicherung

Gesendet: Fr 18.03.2005 11:17

-----Ursprüngliche Nachricht-----
Von: Postbank [mailto:support@postbank.de]
Gesendet: Mittwoch, 16. März 2005 06:59
An: Postbank Kunde
Betreff: PostBank TAN-Absicherung

Sehr geehrter Kunde,

Da es viele Betrugsfaelle mit den Konten von unseren Bankkunden zustande gekommen sind, bitten wir Sie, eine neue TAN-Kodesabsicherung zu benutzen, um die Sperrung von Ihrem Konto zu vermeiden.

Die TAN-Absicherung besteht darin:

Sie tasten zwei TAN-Nummern in die elektronische Form ein und streichen bei Ihnen diese Nummern aus.
Fuer den Fall, dass der Misstaeter Ihre TAN-Codes abfaengt und sie zu benutzen versucht, so wird Ihr Konto bis zur Klaerung der Sachlage gesperrt.
Danach benutzen Sie alle Nummern, ausser diesen 2, der Reihe nach weiter.

Um den Abgang der Mittel von Ihrem Konto zu vermeiden, bitten wir alle, die Form auszufuellen, da wir die Mittel nicht vergueten, die zufolge dem Diebstahl von Ihrem Online-Zugriff zu unserem Bankkonto verlorengegangen sind.

Sie koennen die Form bei ausfuellen

Phishen im Trüben: Hier versucht ein Phisher, Angst zu schüren, um an TAN-Nummern zu gelangen. Das gebrochene Deutsch verrät die betrügerischen Absichten in dieser Mail.

SPAM-FREIE POSTFÄCHER

1. Bestellen Sie nie etwas über unerwünschte E-Mails.
2. Wenn Sie den Sender einer nicht angeforderten E-Mail nicht kennen, löschen Sie die E-Mail.
3. Antworten Sie nie auf Spam-Mails und klicken Sie nicht auf die in der E-Mail enthaltenen Links.
4. Vermeiden Sie die Vorschau-Funktion in Ihrer E-Mail-Client-Software.
5. Wenn Sie E-Mails an zahlreiche Empfänger senden, verwenden Sie das Feld *Blind Copy (BCC)*, um die E-Mail-Adressen zu verbergen.
6. Geben Sie Ihre E-Mail-Adresse nie auf Websites, Newsgroups-Listen oder öffentlichen Online-Foren an.
7. Geben Sie Ihre primäre E-Mail-Adresse niemals einer Person oder auf einer Webseite an, der Sie nicht vertrauen.
8. Legen Sie sich ein oder zwei sekundäre E-Mail-Adressen zu und benutzen Sie diese.

Quelle: Sophos

forsten des Postfachs und der Quarantäne-Ordner Zeit sowie Produktivität kostet. Mittlerweile müssen sich die Hersteller auch auf Mobile Spam (etwa Werbe-SMS) und Spam over Internet Telephony (Spit) vorbereiten.

Wie es begann...

Die erste Massenmail wurde 1978 versendet, als das Internet noch Arpanet hieß und nur wenigen Nutzern zur Verfügung stand. Gary Thuerk, Marketing-Leiter von DEC, verschickte 400 E-Mails, in denen er einen neuen Computer ankündigte. Schon damals rief dieser „Massenversand" wütende Reaktionen und scharfe Kritik hervor.

Der Begriff *Spam* wurde erst 1994 eingeführt, nachdem Rechtsanwalt Laurence Canter ein Posting an alle Newsgroups schickte, um für den Immigrationsservice seiner Kanzlei zu werben. Dadurch erwirtschaftete er einen Mehrumsatz zwischen 100000 und 200000 US-Dollar. „Canter gilt als Vater des modernen Spam, weil sein unerwünschtes Posting in den Reaktionen erstmals explizit als Spam bezeichnet wurde", erklärt Rainer Link von Trend Micro (www.trendmicro.de).

Meistens geht es inhaltlich um Pornografie, Gesundheit und Medizin, IT, Finanzen und Bildung. Klassische Themen sind Viagra, Penisverlängerung und fingierte Aufrufe zu Spenden, die auf einem Privatkonto landen. Letztere sind unter dem Namen *Nigeria Mails* bekannt geworden.

Mittlerweile ist das Versenden von Spam zu einer lukrativen Industrie geworden. Günther Fuhrmann, General Manager Germany von Blackspider (www.blackspider.de) gibt ein Beispiel: „Spammer arbeiten inzwischen saisonal und marktorientiert. So drehte sich vor Weihnachten ein Großteil des Spam um Geschenke und Kredite, wohingegen nach Weihnachen nur noch Diätprodukte und Fitnessgeräte angeboten wurden. In den Wochen vor dem Valentinstag läuft die Spam-Maschine dann wieder Richtung alles was rot und mit Herz ist."

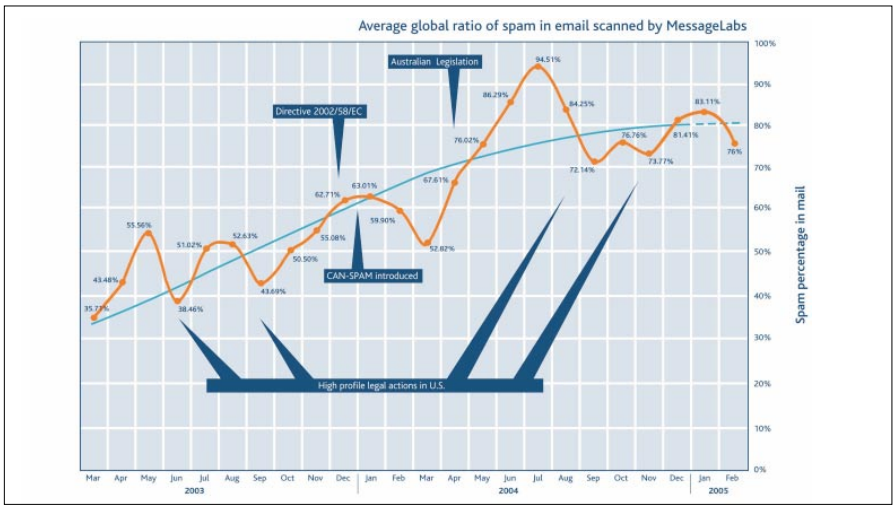
Zu dieser finanzstarken Industrie gehören seit *MyDoom* und *Sobig.F* auch Hacker und Virenschreiber. „Der Trend einer Verschmelzung von Spam und Virus mit der *Sobig.F*-Epidemie ist erkennbar. Ziel dieses Schädlings war das Installieren einer Komponente, die den Zugriff auf Server ermöglicht. Das weit verbreitete Phänomen des Computer Kidnapping erschwert die zweifelsfreie Identifizierung der Spammer", kommentiert Anette Mayr von Xpedite Systems (www.xpedite.de).

Ein Beweis dafür ist die drastische Vermehrung der Botnets. Diese Zombie-Netzwerke umfassen bis zu 100000 von Trojanern annektierte Rechner, die sich für weitere Angriffe und Spamming nutzen lassen. So verdient auch der Virenautor Geld, wenn er diese Ressourcen an Spammer vermietet.

Auch der Handel mit E-Mail-Adressen boomt. Für 150 Millionen validierte Adressen zahlt ein Spammer 100 Euro. Den Trend, dass die Unterscheidung zwischen Hackern, Virenautoren und Spammern allmählich überflüssig wird, bestätigt auch Michael Hoos, Technischer Direktor bei Symantec (www.symantec.de): „Es wird nicht mehr den klassischen Virus und den klassischen Wurm geben, sondern die verschiedenen Technologien werden beliebig gemixt."

Im letzten Jahr waren Phishing-Mails eine besonder Bedrohung: E-Mails, die versuchen, den Empfänger zum Herausgeben seiner Kontoverbindung, PIN- und TAN-Nummern oder Login-Daten zu verleiten. Phisher geben sich dabei die größte Mühe, die Briefe mit Firmenlogos und Design der Bank oder Firma zu gestalten. Auch die eingefügten Links scheinen authentisch (etwa www.postbank.de). Dies lässt sich über das so genannte Spoofing realisieren. Die tatsächliche URL, auf die der Link weist, ist tief im HTML-Code und für den Nutzer nicht erkennbar versteckt.

Toralv Dirro, Security Lead Sales Engineer bei McAfee (www.mcafee.de), analysiert: „Hinter Spam stecken verschiedenste Gruppen, von SexWebseiten bis hin zu organisierten Kreisen, die mit gefälschten Medikamenten handeln. Bei Phishing scheint es eine ähnlich breite Täterschicht zu geben, vom Kleinkriminellen bis hin zur organisier-



MessageLabs scannt täglich Millionen von E-Mails und meldete im Februar eine Spam-Rate von 70 Prozent weltweit.

ten Kriminalität." Gemeinsam mit der Anti-Phishing Working Group ermittelte Websense (www.websense.de) einen Anstieg aktiver Phishing-Seiten von 50 Prozent seit Ende 2004.

Die Trickkiste

Mit dieser finanziellen Motivation haben sich die Methoden der Spammer verändert. Andrew Graydon, Vice President Technology bei BorderWare Technologies (www.borderware.de), beschreibt, wie einfach es ist, ins Spamming-Geschäft einzusteigen: „Die technischen Voraussetzungen, um auch große Mengen von Nachrichten zu verschicken, bietet heute jede Highspeed-Internet-Verbindung. Software, um Massenmails zu generieren und zu versenden, ist als Freeware erhältlich, und Listen mit E-Mail-Adressen können vergleichsweise günstig gekauft werden."

Die Adressen beschafften sich Spammer früher durch das einfache Ausprobieren der gängigsten Kombinationen (z.B. *Lieschen.Mueller@gmx.de*) oder durch legalen/illegalen Adresshandel. Dies übernahmen später *Harvester-Programme*: Software, die auf Knopfdruck das Internet scannt und alle verfügbaren E-Mail-Adressen „aberntet".

Für den Versand braucht der Spammer keine aufwändige, teure Infrastruktur. Botnets (manipulierte Rechner) kann er von Hackern mieten, ungesicherte WLAN Access Points nutzen oder unsichere Mail-Server, wie etwa offene Relais (open relays) missbrauchen. Noch in den 90er Jahren waren alle Mail-Server offene Relais – und sie existieren heute immer noch. Das heißt, jeder beliebige Nutzer konnte beliebig viele E-Mails an beliebig viele Adressen verschicken. Wo es früher genügte, statt *Viagra* einfach *V1agra* zu schreiben, um einen Spam-Filter zu überlisten, ist heute mehr Ideenreichtum nötig. Inhalte lassen sich in HTML-Code, JavaScripts oder Bildern verstecken.

Dass der Massenversand profitabel ist, garantieren zwei Faktoren:

- Selbst wenn nur 0,1 Prozent von einer Million E-Mails beantwortet werden, ist das eine Trefferquote von 1000 Aufträgen.
- Der zweite heißt „Social Engineering": Spammer wählen die Betreffzeile so, dass der Empfänger glaubt, die E-Mail sei tatsächlich für ihn bestimmt.

Und damit lässt sich richtig viel Geld verdienen. Exakte Gewinnsummen eines Spammers lassen sich zwar nur schwer beziffern, dennoch gibt Rainer Link von Trend Micro eine Einschätzung:

- geöffnete E-Mail (verifizierte Adresse): ein US-Dollar pro 1000 Mails,
- erfolgreiche Spyware-Installation: 15 US-Dollar pro 1000 Mails,
- der User klickt auf einen Link: 50 US-Dollar pro 1000 Mails,
- Hypothekenanmeldung: 12 bis 16 US-Dollar,
- Anmeldung für einen gefälschten akademischen Titel: 12 US-Dollar.

Andrew Graydon gibt ein aktuelles Beispiel aus den USA: „Ein Mann bewarb eine Abhör-Software zum Preis von 40 US-Dollar. Er schickte zehn Millionen Nachrichten pro Tag, mit einem durchschnittlichen Ergebnis-Volumen von 50 Aufträgen pro Tag, das macht durchschnittlich 700000 US-Dollar pro Jahr."

Die Müllabfuhr im Einsatz

Bei derartigen Gewinnmargen ist die Motivation der Spammer klar. Deshalb gestaltet sich der Kampf gegen Spam besonders schwierig. Hersteller setzen auf die Kombination verschiedener Techniken:

- Signaturen: Ähnlich wie bei Antiviren-Programmen lassen sich bekannte Spam-Mails mit Signaturen erkennen.
- URL-Filter: Internet-Adressen, die Spammer verwenden, lassen sich automatisch filtern.
- Spracherkennung: E-Mails etwa in kyrillischer Schrift werden blockiert.
- Heuristische (Bayes-)Filter: Sie rechnen mit Wahrscheinlichkeiten und sind lernfähig. Spam wird nach Worthäufigkeiten und Kriterien (z.B. Aufbau der Mail) klassifiziert.
- Black-/Whitelisting: Unerwünschte und erwünschte Absender werden in diesen Listen verwaltet.

Diese forensischen Regelwerke sind intelligent und effektiv. Christopher Hardy von Sophos (www.sophos.de) erklärt die Wir-

PHISH-FREIE ZONE

1. Banken versenden keine E-Mails, in denen persönliche Daten erfragt werden. Antworten Sie nicht auf solche E-Mails, ohne sich bei Ihrer Bank erkundigt zu haben.
2. Anstatt Links über eine E-Mail aufzurufen, tippen Sie sie direkt im Browser ein.
3. Füllen Sie kein Formular in einer E-Mail aus.
4. Übertragen Sie persönliche Daten nur über verschlüsselte Internet-Seiten. Die URL sollte mit *https://* beginnen. Überprüfen Sie die Gültigkeit des digitalen Zertifikats.
5. Prüfen Sie die Transaktionen über Ihre Konten auf Richtigkeit.
6. Halten Sie Programme wie Betriebssystem und Browser mit Updates immer aktuell.
7. Informieren Sie Ihre Bank über Auffälligkeiten.

Quelle: Kaspersky

KOMMENTAR

Rainer Link, Assistant to the President of European Operations bei Trend Micro

Ist das Kommunikationsmedium E-Mail am Ende?

Eine endgültige Lösung des Spam-Problems ist für die nächsten Jahre nicht zu erwarten. Um die Effizienz des Kommunikationsmediums E-Mail zu erhalten, müssen Technologie-Anbieter, staatliche Stellen und Anwender zukünftig noch stärker zusammenarbeiten. Durch die kontinuierliche Weiterentwicklung technischer Lösungen kann Spam bereits heute in großem Umfang blockiert werden.

Rein technisch wird das Problem aber nicht zu lösen sein, sodass wirksame rechtliche Regelungen zu begrüßen sind. Schlussendlich können auch Anwender einen großen Teil zur Entschärfung der Situation beitragen, indem sie ihr Sicherheitsbewusstsein schärfen und vor allem für den umfassenden Schutz ihrer Systeme sorgen.

kungsweise am Beispiel eines Playmobil-Männchens: „Nehme ich ihm den Hut weg, erkenne ich immer noch, dass es sich um Playmobil handelt."

Anti-Spam-Hersteller haben den Wirkungskreis ihrer Spam-Lösungen erweitert und setzen auf primären Schutz am Gateway. E-Mails werden direkt am Zugang zum Internet gescannt und die Firmenserver entlastet. Um Unternehmensnetze frei von Spam zu halten, kommen immer häufiger Managed Security Services zum Einsatz. Hier übernehmen externe Dienstleister wie MessageLabs und Blackspider die Filterarbeit.

AOL, Microsoft und Yahoo! gründeten zum Kampf gegen Werbemüll die Anti Spam Technical Alliance und entwickelten drei Lösungsmodelle:

- SPF (Sender Policy Framework): Im DNS werden Regeln gespeichert, die beschreiben, welche Server E-Mails mit einer bestimmten Absender-Domain verschicken dürfen.
- SMTP-Authentifizierung (Domain Key): Die E-Mail erhält eine digitale Signatur. Der empfangende Server verifiziert die Mail mit einem öffentlichen Schlüssel, der im DNS der Domäne verfügbar ist.
- Sender-ID: der Standardisierungsversuch, das Prinzip von SPF und Caller-ID zu kombinieren.

Die Allianz fand zu keiner Einigung und die Initiative gegen Spam scheiterte. AOL propagierte SPF, Yahoo! die Domain Keys und Microsoft mit AOL später die Sender-ID als Lösung. Alle Technologien haben ihre Lücken. Gekaperte Rechner machen SPF unwirksam und das Prinzip der Domain Keys erfordert große Modifikationen am Mailserver und Verschlüsselungs-Know-how von den Nutzern.

Die Schattenseite der vielseitigen Filtertechniken: Auch abonnierte Newsletter oder sogar wichtige E-Mails kommen nicht mehr an. Solche Mails werden als *false positives* (fälschlicherweise als Spam identifizierte Post) bezeichnet. Verdächtige E-Mails sollten deshalb zum Beispiel in einem eigenen Quarantäne-Ordner gesichert werden. Hier können Anwender nochmals sicherstellen, dass keine E-Mail irrtümlich als Spam markiert wurde. Hersteller geben die Fehlerquote der Spam-Filter zwar mit weniger als ein bis maximal zwei Prozent an, doch kann auch nicht zugestellte Post Schaden verursachen, zum Beispiel für seriöse Marketingfirmen. Deshalb hat eco (Verband der deutschen Internetwirtschaft e.V., www.eco.de) in Zusammenarbeit mit dem Deutschen Direktmarketing Verband e.V. das Positivlistenprojekt ins Leben gerufen. Wer die Aufnahmekriterien erfüllt und es auf die Liste schafft, darf Massenmails versenden und sicher sein, dass Internet Service Provider die Mails nicht abfangen.

Was tut Justitia?

Auch Justitia wirft Gesetze in die Waagschale, um Spammern das Leben zu erschweren. Bislang leider nicht sehr erfolgreich. Nationale Gesetzgebungen wie der Can-Spam-Act, der 2004 in den USA verabschiedet wurde, sorgten zwar für einige medienwirksame Verurteilungen; dennoch stehen die Vereinigten Staaten weiter ganz oben auf der Liste der Spam versendenden Länder.

Gernot Huber von SurfControl (www.surfcontrol.de): „Ein durchschlagender Erfolg war dem Gesetz in den USA bislang nicht beschieden. Vielmehr zeigte sich, dass Spammer beinahe täglich neue Tricks entdecken, um Schlupflöcher und rechtliche Grauzonen zu nutzen und somit ihre Botschaften weiterhin an den Mann zu bringen."

Kritische Stimmen beklagen sogar die Legalisierung von Spam durch das Gesetz. Durch Botnets haben Spammer weltweit Zugriff auf Rechner, über die sie massenweise E-Mails versenden. Damit kommt der Werbemüll nicht mehr direkt aus den USA, die Spammer gehen straffrei aus.

Anfang 2005 legte auch die deutsche Legislative einen Anti-Spam-Gesetzentwurf vor, der für Absender, die ihre Identität verschleiern, ein Bußgeld bis zu 50000 Euro vorsieht. Spam wurde als unzulässig und wettbewerbswidrig eingestuft. Das Spam-Volumen minimieren kann das Gesetz allerdings nicht, denn Spam direkt am Gateway zu löschen, ist in Betrieben, in denen die private Nutzung von E-Mail erlaubt ist, unzulässig. Das regelt das Fernmelde- und Telekommunikationsgesetz, das E-Mails unter das Briefgeheimnis stellt.

Diesen Umstand kommentiert Mirco Rohr, Technical Manager bei Kaspersky (www.kaspersky.de): „Gerade dieses Gesetz macht uns das Leben schwer. Es muss dringend novelliert werden."

Bevor nicht entsprechend verschärfte Gesetze in Deutschland wirksam sind und ein international gültiger Gesetzentwurf vorliegt, müssen wir weiter mit Spam leben. Was nützt ein deutsches Gesetz, wenn sich Spammer oder ihre Rechner auf einer einsamen Insel befinden? Selbstjustiz wie im tragischen Fall des Charles Booher kann keine Lösung sein, denn in diesem Fall ist die Gesetzeslage eindeutig. *hey*

KOMMENTAR

Henning Ogberg, Director Sales DACH bei MessageLabs

Anti-Spam-Gesetze sind wirkungslos

Spam ist weltweit ein großes Problem, daran können auch Anti-Spam-Gesetze nichts ändern. Vor allem in den USA, in Großbritannien, Deutschland, Australien und Hongkong lassen sich auffällige Spam-HotSpots lokalisieren, wo 97 Prozent des weltweiten Spam-Aufkommens die Postfächer verstopfen. Mittlerweile sind über 50 Prozent aller Nachrichten, die deutsche E-Mail-Empfänger erreichen, Spam. Hinzu kommt, dass Spam-Attacken immer häufiger im Vorfeld zu Virenattacken auftreten. Spammer und Virenschreiber arbeiten zusammen, um die Kontrolle über Computer an sich zu reißen (Hijacking), sowie Identitäten und Online-Accounts zu stehlen (Phishing).

Spam ist also zu einer wirklichen Gefahr für sämtliche Unternehmensressourcen geworden. Um diese Bedrohungen in den Griff zu bekommen, reichen internes Personal und IT-Budgets nicht mehr aus. Der Ansatz von Managed E-Mail Security Services stellt gebündelte Fachkompetenz zur Verfügung und entlastet gleichzeitig die unternehmenseigene IT-Infrastruktur, da sämtliche Gefahren bereits auf Internet-Ebene abgefangen werden. Für Unternehmen ist das deshalb die praktikabelste Methode, gefährlichen oder unerwünschten Inhalten Einhalt zu gebieten und auch mit den gesetzlichen Entwicklungen in Deutschland konform zu gehen.