Newsletter von Dr. Héctor B. Epelbaum #38 / 2. August 2007

Guten Tag!

Im August befassen wir uns mit den Risiken von Spam. Ich präsentiere Ihnen 2 aktuelle Beispiele, die meine Kunden im Juli 2007 erlebt haben. Wie immer erhalten Sie nützliche Erkenntnisse, praktische Schlussfolgerungen und umsetzbare Lösungen. Viel Vergnügen!

Spam im Alltag: 2 Beispiele.

Beispiel 1: Der Geburtstagsangriff

Am Tag seines Geburtstags bekommt Hans S. eine digitale Glückwunschkarte. Er ist in guter Stimmung, freut sich über die vielen Freunde, die an ihn denken … Er kennt den Absender der Glückwunschkarte zwar nicht, aber das ist nicht ungewöhnlich: Er hat schließlich viele Bekannte. Und er wundert sich auch nicht über diese E-Mail, warum sollte er: Sein Geburtsdatum ist an mehreren Stellen veröffentlicht, zum Beispiel bei Xing, und lässt sich auch über eine Suchmaschine ohne große Umstände ermitteln.

Er will also vor dem Prüfen des Absenders erst mal die Greeting Card lesen, die diese E-Mail ankündigt. Noch bevor er irgendwelche Hintergedanken hegt, klickt er auf den Link und landet auf einer Adresse, die seinen Computer sofort mit Viren infiziert und seinen PC ausschaltet. Mehrere Versuche, den PC wieder zu starten, scheitern.

Er überlegt sich verschiedene Maßnahmen, versucht, seinen PC zu retten. Vergeblich. Zwei Tage später gibt er auf. Die Firma, die für Vernetzung und Wartung der EDV in seinem Geschäft zuständig ist, wird mit der Reparatur seines privaten PCs beauftragt. Fünf Tage später ist sein Computer wieder einsatzfähig. Die Festplatte musste vollständig formatiert, alle Programme mussten neu installiert werden. Hans S. ist froh, immerhin regelmässige Backups seiner Daten gemacht zu haben …

Diese Geschichte ist nicht erfunden. Hans S. ist ein Kunde von mir. Er ist dipl. Ingenieur und kein PC-Neuling. Sowohl Antiviren-Software als auch Spam-Filter sind auf seinem privaten Rechner und Laptop installiert, aber auch in seiner Firma eingesetzt. Seine E-Mail-Adresse erscheint auf seiner Website. Dadurch bekommt er täglich ca. 80 Mails – und natürlich viel Spam.

Fazit: Hans S. hat – richtigerweise – Schadensbegrenzung betrieben. Mit dem Einsatz von Software-Programmen gegen Viren und Spam hat er richtig gehandelt. Doch hat er vorbeugende Massnahmen unterlassen: Sein Computer bekam viel Spam. Regelmäßig musste er die eingegangenen E-Mails analysieren, um nichts Wesentliches ohne Absicht zu löschen. Mit der Viren- und Spam-Software wurden damit allerdings lediglich die Symptome bekämpft. Denn selbst die beste Spam-Software ist letztlich Symptombekämpfung und stellt keine grundsätzliche Lösung des Spam-Problems dar.

Beispiel 2: Der Angriff der „Arbeitskollegen“

Claudia N. erhält täglich mehrere E-Mails von Kollegen Ihrer Firma. Die E-Mail-Adressen dieser Kollegen sind öffentlich zugänglich, sie erscheinen auch auf der Firmen-Website. Nun erhält Claudia N. plötzlich eine spezielle Art von Spam: Dieses Spam sieht aus, als ob ihre Kollegen die Absender wären! Obwohl diese E-Mails durch den Spam-Filter entdeckt werden, prüft Claudia N. grundsätzlich alle empfangenen E-Mails, bevor sie sie löscht. Eine Mail von Ihrer Kollegin Beate R. fällt ihr dabei auf, weil die Mail lediglich ein PDF-Icon enthält. Claudia N. klickt drauf – und Ihr Computer ist sogleich infiziert. Das vertrauenswürdig wirkende PDF-Icon war eine Täuschung, die den Glauben von Claudia N. in die Sicherheit eines PDF-Dokuments missbrauchte. Denn in Tat und Wahrheit verbarg sich hinter dem Icon ein Link, der Viren importierte.

Abb. 1: Claudia N, hier KollegeB, hat diese E-Mail erhalten und anschliessend auf das PDF-Icon geklickt.

Fazit: Die Software-Tools zur Schadensbegrenzung sind gut, aber nicht perfekt. Menschliches Verhalten ist eine Fehlerquelle. Das Vertrauen in halbautomatische Software-Lösungen kann sehr teuer werden. E-Mails sollten erst geöffnet bzw. Links angeklickt werden, wenn man weiss, wer oder was sich wirklich dahinter verbirgt.

Die richtige Lösung gegen Spam

Die einzig richtige Lösung gegen Spam ist eine vorbeugende Vorgehensweise, die dazu führt, dass man überhaupt kein Spam mehr erhält. Doch wie ist das möglich?

Was ist zu tun?

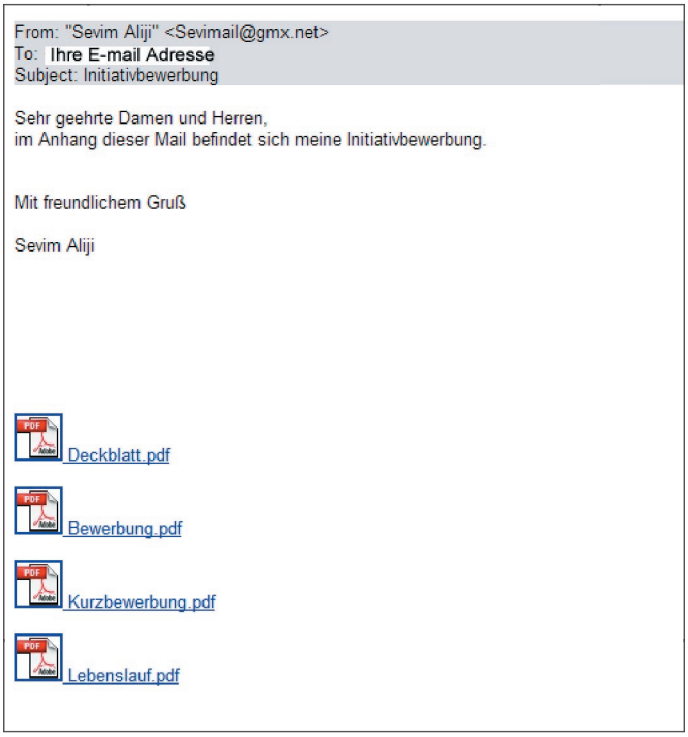
Die E-Mail-Kommunikation muss zur Vorbeugung gegen Spam ein einziges Mal richtig organisiert werden. Anschliessend brauchen Sie lediglich einige Verhaltensregeln zu beachten – und Sie sind spamfrei!

Um spamfrei zu bleiben, sind mehrere E-Mail-Adressen sowie ein adäquater Umgang mit den Absender-Adressen erforderlich, beispielsweise beim privaten Gebrauch oder bei Publikationen im WWW (Foren, Visitenkarten usw.). Diese neuen Adressen sind ein Mix aus provisorischen und permanenten Adressen. Keine Angst: Jeder, der eine E-Mail auf eine „alte" Adresse schreibt, erfährt sogleich die neue Anschrift. Es gehen also bei diesem Verfahren weder private noch geschäftliche Kontakte verloren. Zudem bleibt die Arbeitsweise im Alltag dieselbe. Mehraufwand gibt es keinen, im Gegenteil: Das regelmässige und oft zeitraubende Überprüfen des Junk-Ordners entfällt, die Datensicherheit ist um ein Vielfaches höher, die Arbeit entspannter.

Die präventive Lösung, die ich anbiete, ist dabei auf meine Auftraggeber angepasst: Die Anzahl Mitarbeiter mit E-Mail-Einsatz, externe und interne Mitarbeiter, Arbeitsprozesse, spezifische Bedürfnisse und Anforderungen werden berücksichtigt.

Haben Sie Interesse an einer professionellen Anti-Spam-Lösung für Ihre Firma?
Einfach Kontakt per E-Mail aufnehmen und einen Termin für ein Telefonat vorschlagen!

PS: Wie hätten Sie auf diese E-Mail (Abb. 2) reagiert? Und wie Ihre Mitarbeiter?


From: "Sevim Aliji" <Sevimail@gmx.net>
To: Ihre E-mail Adresse
Subject: Initiativbewerbung

Sehr geehrte Damen und Herren,
im Anhang dieser Mail befindet sich meine Initiativbewerbung.

Mit freundlichem Gruß

Sevim Aliji

Deckblatt.pdf
Bewerbung.pdf
Kurzbewerbung.pdf
Lebenslauf.pdf

Abb. 2: Hinter jedem Icon der (Pseudo-)PDF-Dateien stecken infizierende Programme.