Probleme mit dem Mailversand

Meike Pfefferkorn - 2024-03-13 - Newsletter

Egal ob per Newsletter, Einfach-Mail oder im Rechnungsversand: Wenn Sie E-Mails verschicken, insbesondere an viele Empfänger, kann es aufgrund immer strengerer Filterregeln der Mailbetreiber sein, dass Sie unter Spam-Verdacht geraten.

Als privater E-Mail-Nutzer kennen Sie das Problem: Natürlich möchten Sie E-Mails erhalten, aber natürlich keinen Spam. Deswegen wurden Spam-Filter erfunden und die E-Mailanbieter haben viele Anstrengungen unternommen, dass Sie nicht mehr von Spam-Nachrichten überflutet werden.

Aber wie unterscheidet der Server eigentlich Spam von „richtigen“ E-Mails?
Auf der inhaltlichen Ebene sieht es für das menschliche Auge recht einfach aus: Ein Prinz, der Ihnen zigmillionen schenken will, ist kein gewollter Kontakt. Aber diese Arbeit müssen Computer erledigen -einerseits aufgrund des Aufwands, andererseits sollen ihre E-Mails ja nicht von anderen Leuten gelesen werden. Für einen Computer ist aber „Mein kleiner Prinz wurde geboren“ und „Ich bin ein Prinz“ kein so grosser Unterschied. Deswegen wird vieles von einer deutlich technischeren Seite eingeschätzt.

Jede E-Mail kommt von einer E-Mailadresse und über einen Mailserver. Sie wird zu einer E-Mailadresse gesendet, die ebenso auf einem Mailserver liegt. Der Mailserver des Adressaten schätzt also beides ein: Ist die Absender-E-Mailadresse in Ordnung? Verhält sich der andere Mailserver auffällig? Passen die E-Mailadresse und der Mailserver zusammen?

Fairgate unternimmt vieles, um richtig eingeschätzt zu werden. Deswegen werden z.B. die Einfach-Mails und Newsletter nicht auf einen Schlag rausgeschickt, sondern über ca. 1 Stunde verteilt. Wenn andere Mailserver „sehen“, dass ein andere mit tausenden E-Mails in derselben Minute „schiesst“, werten diese das als sehr schlechtes Zeichen bzw. Spamversuch. Auch kann ein Versandversuch temporär fehlschlagen, also versuchen wir ca. 30 Mal innert eines Tages die Mail wieter zu verschicken bis Sie erfolgreich angenommen wurde, abgelehnt wurde oder wenn keines von beidem, dann brechen wir den Versand als permantenten Fehler ab.

Dennoch sind Spam-Verschicker erstmal genauso klug wie wir. Daher ist es ein beständiger Kampf, des Nachrüstens, Nachjustierens usw. – sowohl in der Blockade von Spam-Nachrichten, als auch beim Überspringen der Barrikaden für die „gewollten“ E-Mails. Manchmal verlieren wir, aber immer nur kurzzeitig.

Es gibt ein paar Konstellationen, die immer besonders schwierig sind. Apple und Microsoft sind besonders eifrig im Barrikaden-Bauen und daher kommt es hier häufiger zu Problemen.

Banken, Versicherungen und andere Unternehmen mit hohem Sicherheitsbedarf sind häufig schwer durchdringbar, weit über Spam-Filter hinaus. Bedenken Sie aber folgendes: *Nicht alles was Mailserverbetreiber als Spam klassifizieren ist auch wirklich Spam, es gibt aufgrund immer strengerer Regeln häufig Falschdeklarationen die dann nur verwirren*.

Was Sie tun können
Es gibt ein paar Dinge, die Ihre E-Mails besser aussehen lassen bzw. was Sie machen können:

- Verwenden Sie für jedes Login ein eigenes, langes und nicht einfach zu erratendes Passwort das Sie auch mit niemandem teilen: Wie man ein sicheres Passwort auswählt und behält
- Nutzen Sie als Versandadresse eine E-Mailadresse Ihres Vereins-Mailservers, z.B. news@beispielverein.ch.
- Massenversände: Halten Sie Ihre Newsletter/Einfachmails kurz und ohne grosse Bilder, das vergrössert die Chance nicht geblockt zu werden (ideal wäre 20-50 KB).
- Tragen Sie bekannte Mailadressen denen Sie trauen in die "White-List" Ihres Mailprogramms ein, damit sie nicht geblockt oder als Spam eingestuft werden.
- Bitten Sie Ihre Kontakte und Mitglieder, Ihre E-Mailadresse(n) in ihr Adressbuch aufzunehmen – dann sehen Sie eher aus wie ein „Freund“.
- Bitten Sie Ihre Kontakte und Mitglieder, dass falls Ihre E-Mails im Spam-Ordner landen, Sie dort wieder herauszuholen und als „kein Spam“ zu markieren – dann können die Spam-Filter lernen, dass Sie zu den Guten gehören.
- Checken Sie, ob Ihre E-Mailadresse gehackt wurde und Ihr Passwort im Umlauf ist: https://haveibeenpwned.com/
- Wenn Sie mit externen Web- und Mailservern arbeiten, ergänzen Sie Ihren SPF-Eintrag in Ihrem DNS mit den folgenden Punkten (bitte vorher mit Ihrem Provider absprechen):
    - ip4:5.148.183.20 include:mailgun.org include:spf.fairgate.ch ~all
- Manchmal hilft es bei besonders schwierigen Mailanbietern beim Support um Gnade zu bitten.
- Falls möglich, bitten Sie Kontakte und Mitglieder mit beruflichen E-Mailadressen von Banken und Co. Ihnen eine private andere E-Mailadresse zu geben. Meistens wissen diese um das Problem der „Unerreichbarkeit“ von Aussen.
- Melden Sie Phishing-eMails über diese Website um die Verbreitung zu stoppen: https://www.antiphishing.ch/de/
- Überprüfen und korrigieren Sie regelmässig Ihre Maillisten damit Sie sich nicht Mails aus SpamTraps (SpamFallen) einheimsen: SpamTraps Erklärungen + SpamTraps

Explanation

Checklisten für E-Mails

- Checkliste: Mails so verschicken, dass man Ihnen vertraut https://www.heise.de/news/Checkliste-Mails-so-verschicken-dass-man-Ihnen-vertraut-7238158.html
- Tips zum Mailversand von Mailjet: https://www.mailjet.com/de/blog/zustellbarkeit/spam-ordner-vermeiden/
- Erklärungen zur Domainreputation: https://kinsta.com/de/blog/domain-reputation/