Reaktion nach Sperrung der Mail-Domain ct.de von Google

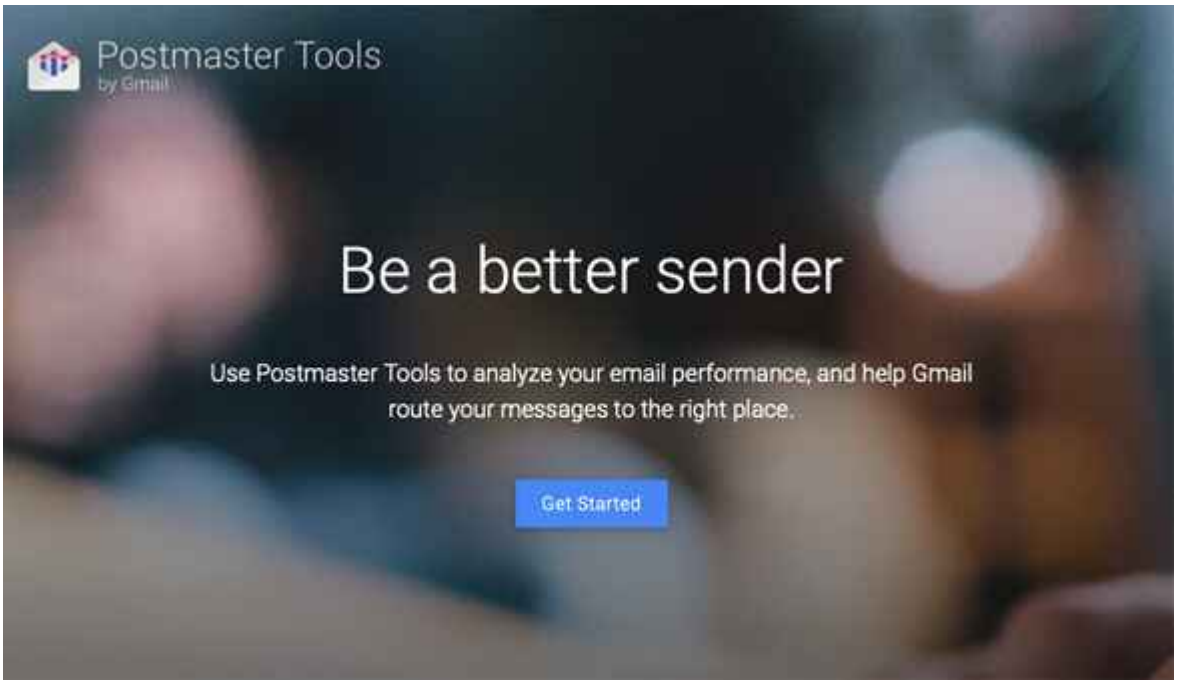
Google sagt: Microsoft ist schuld

Mitte Juni nahm Google plötzlich keine Mails von ct.de mehr an, die Reputation der Domain sei zu gering. Jetzt hat sich das Unternehmen geäußert und zeigt mit dem Finger auf Microsoft.
Mitte Juni nahm Google plötzlich keine Mails von ct.de mehr an, die Reputation der Domain sei zu gering. Jetzt hat sich das Unternehmen geäußert und zeigt mit dem Finger auf Microsoft.

Von Michael Fischer von Mollard und Jan Mahn

Fast einen Monat lang konnten Mitarbeiter der c’t mit einer

@ct.de-Adresse nicht an Server von Google mailen – weder an @gmail.com noch an die zahlreichen Unternehmen, die ihre Mails bei Google verwalten lassen. In der Fehlermeldung beklagten sich die Server über mangelnde Reputation der Domain ct.de [1]. Die Postmaster-Tools, die Google für solche Fälle für Mail-Admins bereitstellt, halfen nicht weiter. In seinen FAQ spricht Google selbst davon, dass die Informationen erst bei einer Größenordnung von Hunderten Mails pro Tag aussagekräftig sind – und diese Grenze erreicht die Domain nicht. Im Juli war das Problem dann so plötzlich verschwunden, wie es gekommen war.



Postmaster-Tools von Google: Die Anlaufstelle für Mailserverbetreiber liefert nicht immer aussagekräftige Informationen, wenn es bei der Zustellung Probleme gibt.

Mit einer Erklärung ließ sich Google bis Ende August Zeit, doch die hatte es in sich: Schuld sei Microsoft. Weil der Verlag für Videotelefonie Teams einsetzt, enthielt der SPF-Eintrag (Sender Policy Framework) im DNS für ct.de den Eintrag: include:spf.protection.outlook.com

Empfangende Mailserver können diesen Eintrag auswerten und ihm entnehmen, wer Mails im Namen einer Domain versenden darf. Dass Microsofts Server berechtigt wurden, ist Standard für Unternehmen, die Teams nutzen und das System zum Beispiel

Termineinladungen verschicken lassen wollen. Zum Problem wurde der SPF-Eintrag, weil Microsofts Server eine extrem ungewöhnliche Art der direkten Weiterleitung einsetzen, die Spammer ausnutzen können. Beschrieben wird das Problem auch in einem wissenschaftlichen Paper aus dem April [2].

Um das Problem zu verstehen, muss man wissen, dass es auf Ebene des Mailprotokolls SMTP einen für die Nutzer meist unsichtbaren Envelope-Absender gibt, der von dem Absender abweichen kann, den Sender und Empfänger in ihren Mailprogrammen sehen (dem From-Header). Für SPF ist der Envelope-Absender entscheidend.

Offene Weiterleitung

Die Spammer nutzen aus, dass Microsofts Mailserver sogenanntes Open Forwarding erlauben – als Nutzer kann man eine dauerhafte Weiterleitung einrichten. Bei Accounts von Privatnutzern, die über outlook.com senden, setzt Microsoft in dem Fall den Envelope-Absender auf die Domain outlook.com, bei Geschäftskunden jedoch nicht. Bei ihnen wird beim Weiterleiten der Absender aus dem From-Header als Envelope-Absender übernommen und die Mail so an die eingestellte Adresse gesendet. Spammer brauchen also Zugriff auf ein Geschäftskundenkonto, hinterlegen dort die Adresse ihres Spam-Opfers (in diesem Fall ein Konto bei Google) als Weiterleitungsadresse.

Dann müssen sie sich nur eine beliebige Domain aussuchen, die den gängigen SPF-Eintrag für Microsoft-Server enthält. Von ihrer eigenen Adresse senden sie Mails an das Konto bei Microsoft, setzen aber als From-Header zum Beispiel eine ct.de-Adresse. Microsoft nimmt die Mail an, ändert den Envelope-Absender und leitet sie direkt an das Opfer weiter. Genau das ist laut Google mit der Domain ct.de passiert: Am 15. Juni stieg das Mailvolumen von der Domain um rund den Faktor 2000, alle problematischen Mails kamen über Microsoft-Server. Anstatt diese Server auszubremsen, entschied sich

Google dafür, die Reputation der Domain zu senken.

Googles Reaktion ist teilweise verständlich, die nicht funktionierenden Postmaster-Tools, die Reaktionszeiten und das Kommunikationsverhalten sind für Mail-Admins jedoch extrem unbefriedigend. Microsofts Vorgehen dagegen ist ein echtes Sicherheitsproblem: Weil Teams-Admins den entsprechenden SPF-Eintrag massenhaft setzen, haben Microsofts Mailserver eine exponierte Rolle – die spammerfreundliche Weiterleitung ist dann schlicht unangemessen. Mitte August erfuhren wir über DMARC-Reports von einem ähnlichen Vorfall – diesmal schickten die Microsoft-Server im Namen von ct.de an Yahoo-Adressen. Der SPF-Eintrag für ct.de ist seitdem geändert und Microsofts Server sind entfernt.

Der Vorfall macht aber auch deutlich, dass SPF aus einer anderen Zeit stammt, in der es noch üblich war, dass Mailserver dezentral von Organisationen betrieben werden. Heute ist es dagegen üblich, dass große Provider die Mails für ihre Kunden abwickeln und mit dem dann unvermeidlichen include: im SPF-Eintrag gibt man als Admin die Kontrolle über die ausgehenden Server aus der Hand – das verwässert den Wert eines SPF-Eintrags.

1. Literatur
2. Jan Mahn, Google stufte ct.de als Spamschleuder ein, c’t 19/2023, S. 35
3. E. Liu et al., Forward Pass: Onthe Security Implications of Email Forwarding Mechanism and Policy, arXiv, 19. April 2023, https://arxiv.org/pdf/2302.07287.pdf