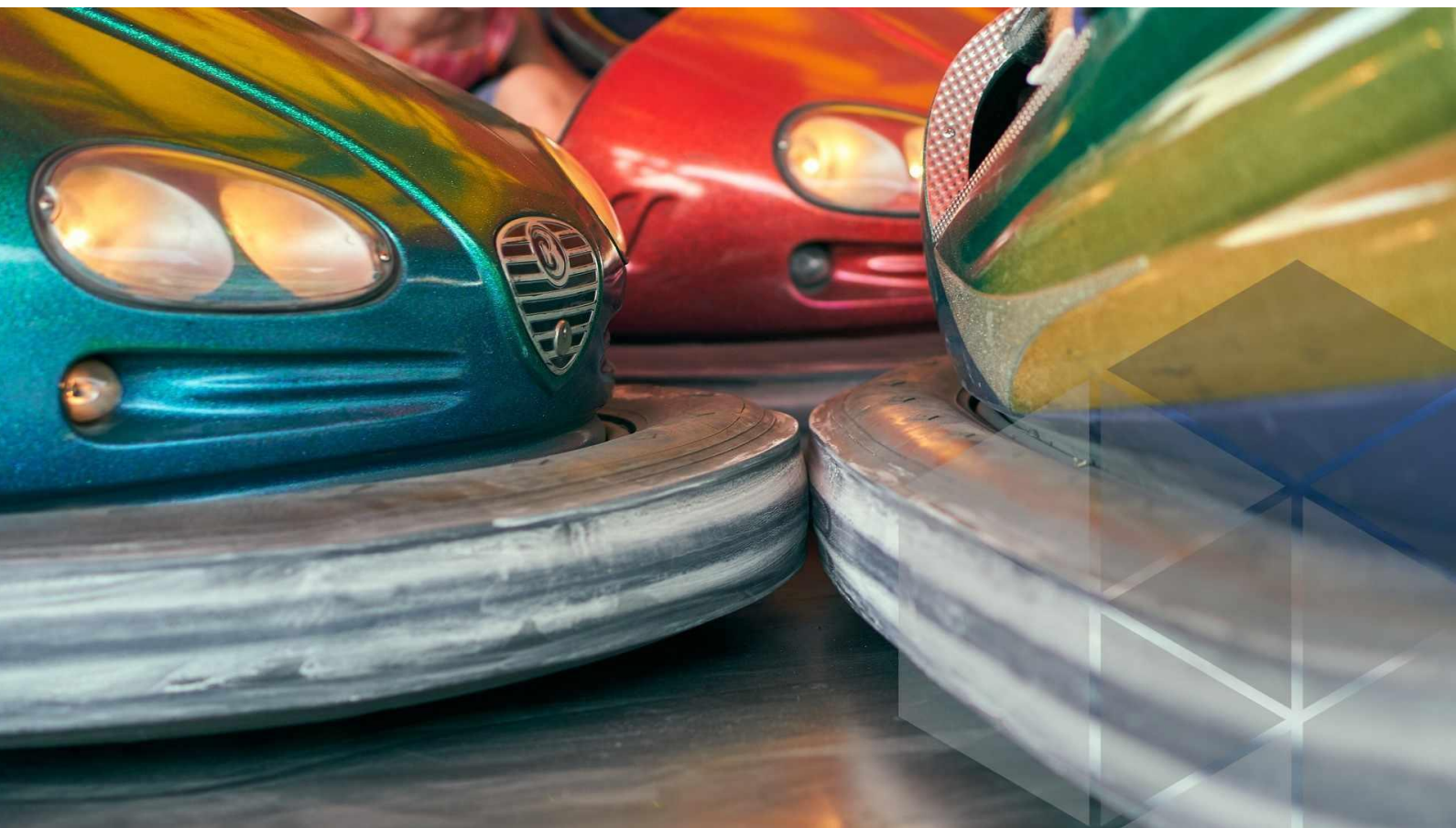


WHITEPAPER

Messfehler bei Newsletter-KPI

Wie Privacy- und Sicherheits-Initiativen
die Marketing-KPI unter Druck setzen



Die Privacy-Initiativen von Apple & Co. sowie neue Features von Sicherheitssoftware machen die Newsletter-KPIs – welche jahrelang feste Messgrößen waren – zunichte. Dieses Whitepaper erklärt die neusten Herausforderungen und gibt praktische Tipps.

Ausgangslage

Für E-Mail-Newsletter konnten bisher in der Regel gute und weitgehend korrekte Statistiken der Nutzung erstellt werden. Die wichtigsten Kennzahlen lauten:

- **Zustellrate:** wie viele der versandten Newsletter konnten zugestellt bzw. nicht zugestellt werden – die sogenannte «**Bounce Rate**».
- **Öffnungsrate** oder **Open Rate:** in Prozent zu den versandten bzw. zugestellten Mails.
- **Klickrate:** wie viele Links wurden geklickt. Diese ist sowohl bei redaktionellen Inhalten für den Absender, aber natürlich auch und vor allem bei Banner Ads für den Werbekunden von Interesse.

Eine Erläuterung der verschiedenen Newsletter-KPI finden Sie in unserem Whitepaper «[KPIs im E-Mail-Marketing](#)».

Diese Zählungen werden technisch unterschiedlich umgesetzt:

Links in E-Mail-Newslettern sind in der Regel durch eine **Folge von Redirects** umgesetzt, die beim Aufruf des Links den User weiterleiten und zugleich eine **Zählung auslösen**. Bei Banner Ads, die über einen Ad-Server eingebunden sind, sind oft zwei Redirects hintereinander geschaltet: einer von der Mailsoftware, einer vom Ad Server. Die Zahlen der beiden Systeme lassen sich also theoretisch vergleichen, wobei zwei verschiedene Zählungen praktisch nie zum exakt gleichen Ergebnis kommen.

Grundsätzlich ist das Thema von ungenauen/falschen Auswertungsdaten ebenso alt wie die Online-Werbung.

Diverse Faktoren können das Ergebnis verzerren, so etwa:

- das Ein- oder Ausschalten des automatischen Ladens von Bildern,
- lokale Blocker der Zählpixel beim Empfänger,
- die Nutzung einer Vorschau z. B. in Outlook (die zu einer «Open»-Zählung führen kann oder nicht),
- Details der konkreten technischen Umsetzung,
- Einstellungen zu Datenschutz und Privatsphäre
- oder andere Sicherheitseinstellungen beim Empfänger und dessen Software-Setup, durch dessen Firma und/oder den technischen Provider.

Diese Ungenauigkeiten werden bisher notgedrungen immer in Kauf genommen.

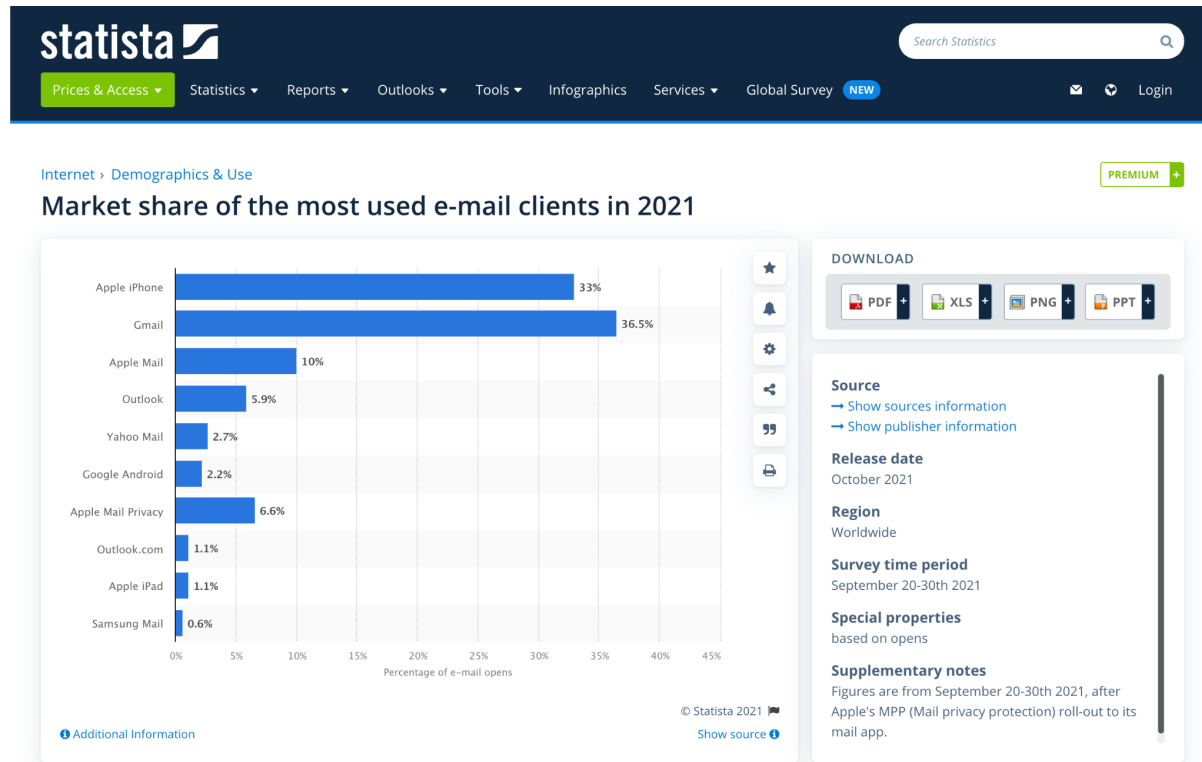
Wie auch bei anderen Online-Themen (wie Spam-Protection oder bei Web-Analytics dem Schutz gegen Klickbetrug und Fake Sessions) gibt es auch hier ein andauerndes Wettrüsten zwischen Betrügern und den Anbietern von Schutzmechanismen. Diese führen zu einem Katz-und-Maus-Spiel, das voraussichtlich ewig weitergehen wird.

Apples Mail Privacy Protection zerstört Open Rate

Ein interessanter Player in diesem Markt ist Apple, der sich Privacy gross auf die Fahnen geschrieben hat, um sich von den Konkurrenten Google und Facebook klar abzugrenzen (siehe auch [hier](#)). Apple hat mit dem neuen iOS15, das seit Ende September 2021 auf iPhones installiert wird, sowie mit macOS Monterey (seit Oktober 2021 auf Mac-Rechnern) diverse weitreichende Änderungen eingeführt, die insbesondere die Open Rates als verlässliche Masszahl in Gefahr bringen.

Apple «öffnet» im Hintergrund alle Mails vorab, die mit den Apple Mail Apps (auf dem Mac oder auf iOS/iPadOS) empfangen werden, bevor diese an den eigentlichen Empfänger gehen. Dadurch wird die Öffnungsrate aufgeblasen und die Messung an sich entwertet. Zusätzlich versteckt Apple dabei auch die IP-Adresse des E-Mail-Empfängers; somit kann auch die Geolocation nicht mehr nachvollzogen werden. Diese Änderung ist so fundamental, und Apples Marktanteil ist auf mobilen Geräten so hoch, dass die **Open Rate als KPI in Zukunft womöglich komplett hinfällig** werden könnte.

Gemäss einer Auswertung bei Statista lag der Anteil der mit der neuen Einstellung von Apple geöffneten Mails («Apple Mail Privacy») zehn Tage nach der Lancierung von iOS15 schon bei 6,6 %:



Sicherheitssoftware verfälscht Klick-Rate

Durch die zunehmende Verbreitung von Malware, Phishing etc., die u. a. wegen der immer stärker zunehmenden Ransomware-Attacken (z. B. [Funke Mediengruppe von Erpressersoftware befallen](#)) hat das Thema eine neue Dringlichkeit bekommen. Manche Unternehmen installieren Sicherheitssysteme, die alle Links nachverfolgen, um die Zielseiten auf mögliche Gefahren zu scannen.

Beispielsweise [Kaspersky Endpoint Security](#), von dem eine Cloud-Version (für kleinere Firmen) und eine Enterprise-Version (für grosse Unternehmen mit eigenen Mailservern) existiert. Diese Lösung wirbt mit «Sicherheitslösungen, die in der Lage sind, Phishing-E-Mails auf dem Mail-Server zu erkennen und die Weiterleitung auf Phishing-Sites zu verhindern». Dies beinhaltet vermutlich, dass Mails vom Sicherheitssystem «geöffnet» und Redirects ausgelöst werden, bevor der Empfänger die Mail auf seinem lokalen Gerät öffnet.

Das heisst es werden vor der Zustellung an den Empfänger bereits alle Links geöffnet. Der Empfänger hat das Mail noch gar nicht gesehen, im Reporting werden aber alle Link-Öffnungen als Klicks gezählt.

Derzeit sind solche Systeme noch nicht sehr weit verbreitet, sodass sie noch nicht zu substantiellen Verzerrungen aller Analytics führen. Allerdings dürfte der Einsatz in Zukunft insbesondere wegen der erwähnten Malware- und Ransomware-Bedrohungen deutlich zunehmen.

Es ist gut vorstellbar, dass andere grosse Anbieter demnächst nachziehen werden. Google mit Gmail/Google Workspace oder Microsoft mit Outlook/Office 365 scannen bereits heute per Default Dateianhänge, aber noch keine Links. Wenn diese beiden Player ähnliche Malware-Protection-Funktionen einsetzen wie oben beschrieben, könnten damit sämtliche Klick-Statistiken weitgehend unbrauchbar werden.

Da das Thema noch relativ neu ist, ist noch nicht absehbar, wie die Anbieter von Mess-Systemen, also vor allem die Newsletter-Versender und Adserver-Betreiber, reagieren werden. Einerseits wäre es möglich, viele fast gleichzeitig ausgeführte automatisierte Klicks zu erkennen; andererseits ist nicht klar, ob diese automatischen Aktionen bei allen Sicherheitssystemen ähnliche Muster ergeben, die daran erkannt und ausgefiltert werden können. Somit sind wir wieder beim Katz-und-Maus-Spiel.

Alternative für Klick-Zählungen

Klicks können an zwei Orten gezählt werden, bisher wurden Klicks vom Newsletter aus gehend gemessen. Was effizienter und praktischer war. Stattdessen könnten neu die **eingehenden Seitenaufrufe** über Analytics-Tools (z.B. Google Analytics, Piwik bzw. Matomo, etc.) gemessen werden. Diese Messungen werden voraussichtlich verlässlicher sein, da Sicherheits-Bots auf einer Website leichter zu erkennen sein werden als beim Auflösen eines Redirects.

Deshalb erwarten wir, dass diese Messung in Zukunft an Bedeutung gewinnen und womöglich sogar zu der relevanten KPI werden wird.

Fazit & Tipps

Insgesamt gehen wir davon aus, dass in den nächsten Monaten und Jahren das Thema **Analytics im E-Mail-Bereich stark unter Druck** kommen wird. Aktuell ist es besser Ruhe zu bewahren und zu schauen, wie sich die Zahlen entwickeln. Es ist davon auszugehen, dass die Hersteller der Newsletter-Versandssysteme handeln und mit neuen Messarten aufwarten werden.

Was ist zu tun?

Ruhe bewahren und schauen, wie sich die Öffnungsraten entwickeln. Wenn diese über die nächsten Versände ansteigen, sind Sie zumindest nicht überrascht. Die gute Nachricht ist: Ihre Mails werden weiterhin zugestellt und deswegen nicht weniger angeschaut, sie können es nur weniger gut messen.

Für B2C:

Die Klickraten sind bei privaten Anwendern noch ziemlich robust. Sie können weiterhin die Klickzahlen messen und vergleichen. Es ist allerdings damit zu rechnen, dass auch Sicherheitssoftware für Privatanwender früher oder später die Links vorab prüfen wird.

Für B2B:

Wenn Sie in Ihrem Newsletter auf Seiten Ihrer eigenen Website verlinken, vergleichen Sie die Klickzahlen auch mit den eingehenden Seitenaufrufen (Web-Analytics).

Falls Sie mit Content auf anderen Webseiten arbeiten, können Sie filtern, wie viele Personen

alles angeklickt haben und diese bei der Anzahl Klicks abzählen. (Sie werden damit aber geringere Zahlen erhalten, da gewisse dieser Personen ja tatsächlich geklickt haben.)

Qualität und Nutzwert als Maxime

Konzentrieren Sie sich anstatt auf die Zahlen auf die Qualität Ihres Newsletters. Bietet dieser hoher Nutzwert für Ihre Empfänger? Könnten Sie Ihre Empfänger sinnvoll Clustern (bspw. nach B2C/B2B, Frau/Mann, Produktgruppe) und diesen Zielgruppen unterschiedliche Newsletter zustellen?

Mit Scope können Sie sehr einfach und schnell zielgruppenspezifische Newsletter erstellen und einen viel grösseren Aufwand zu haben. Finden Sie direkt in der Scope Plattform passende Artikel zu Ihren Themen und erstellen Sie daraus kombiniert mit Ihren eigenen Inhalten zielgruppenspezifische Newsletter, die hohen Nutzwert bringen.

Sind Sie interessiert zu sehen, wie dies funktioniert? [Vereinbaren Sie einen Termin für eine unverbindliche Demo von Scope.](#) Alternativ erreichen Sie uns unter untenstehenden Koordinaten.

Peter Hogenkamp

CEO Scope Content AG

peter.hogenkamp@thescope.com

direkt: +41 44 533 00 50



Impressum

Scope Content AG

Weinbergstrasse 137

CH-8006 Zürich

www.thescope.com

hello@thescope.com

+41 44 533 00 55

CHE-307.434.909

Geschäftsführung:

Dr. Peter Hogenkamp

Redaktion:

Reto Kleeb, Peter Hogenkamp, Lea Lutz

Erstellt:

25. November 2021