Dialer & Spam

Inhaltsverzeichnis

1 Was ist Spam?

"Spam" ist der umgangssprachliche Sammelbegriff für unverlangte Werbung. Ursprünglich ist SPAM der Markenname eines Dosenfleischprodukts des amerikanischen Herstellers Hormel. Dieser wurde von der britischen Comedy-Truppe Monty Python in einen Sketch eingebaut, welcher in den Anfangszeiten des Internet bei mutwillig gestörter Kommunikation gerne zitiert wurde.

Die eigentlichen Bezeichnungen "UCE" (unsolicited commercial email) und "UBE" (unsolicited bulk email) können mit unerwünschter Werbe-E-Mail bzw. unerwünschter Massen-E-Mail übersetzt werden. Dabei wird mit "Spam" nicht nur E-Mail bezeichnet, sondern jegliche Art unerwünschter Mitteilungen über elektronische Kommunikationsmittel. Für die meisten Empfänger sind diese Nachrichten wertloser Datenmüll.

Die Spammer geben sich große Mühe, ihre Identität zu verbergen. So benutzen sie via Internet unsichere Server aus dem Ausland (oft in Fernost oder Südamerika), um eine Rückverfolgung unmöglich zu machen. Als E-Mail-Adresse des Absenders wird entweder eine erfundene Adresse genutzt oder ein Eintrag aus der Empfängerliste genommen, deren tatsächlicher Inhaber als vermeintlicher Spammer folglich Tausende verärgerte Antworten erhält. .

Eine Spamwelle kann mehrere Millionen Empfänger treffen. Versendet werden die Spam-Mails dabei nur selten mit herkömmlichen Mailprogrammen wie z. B. Mozilla Mail oder Microsoft Outlook Express, sondern mit spezieller "Bulkmailing"-Software, welche auf den Versand von Massenmail und die üblichen Spammer-Tricks zur Verschleierung ihrer Identität optimiert ist. Der Versand der Spams erfolgt vollautomatisch: neben der Liste der Empfänger und dem Text der Spam-Mail wird eine Auflistung unsicherer ausländischer Proxy-Server benötigt, welche im Internet erhältlich ist oder mit geeigneter Software selbst erstellt werden kann.

Um den Versand zu beschleunigen, werden Spam-Mails sehr kurz gehalten. Über Verweise ("Links") auf WWW-Seiten sind zusätzliche Informationen, Grafiken und Dialer zugänglich. Diese Inhalte liegen oft bei Anbietern kostenloser WWW-Homepages. Bei vielen Internetprovidern werden per Spam beworbene WWW-Seiten jedoch nach Bekanntwerden (meist durch Beschwerden der Opfer an den Provider des Spammers) sehr bald gesperrt. Wenn der Spammer von seinem belästigendem Geschäft profitieren will, muss er seine Inhalte bei einem Provider veröffentlichen, welcher gegen erheblichen Aufpreis (z. B. das Zehnfache des offiziellen Endkundenpreises) einen sogenannten "pink contract" anbietet und als Folge eine per Spam beworbene Internetpräsenz explizit nicht sperrt.

Für den Versand der Spam-Mails werden häufig auch ungesicherte Proxy verwendet. Dies können im Zeitalter des Internet der Dinge auch ungesicherte Kühlschränke bzw. Smart-TV Geräte, Router oder falsch konfigurierte Server sein.

Spam-Mails dienen oft auch als Grundlage für Phishing Attacken. [@]

2 Wie gelangen die Spammer an die Adressen?

Datenträger und Datenbanken mit Tausenden oder Millionen E-Mail-Adressen werden fast täglich auf Internet-Marktplätzen (z. B. Ebay) oder wiederum per Spam angeboten und kosten meist weniger als 100 Euro. Über besondere Einrichtungen im Internet werden gut recherchierte Adresslisten gegen "Mitgliedsbeiträge" vertrieben. Diese CDs enthalten Adressen, welche im Internet an öffentlich zugänglichen Stellen gesammelt wurden: auf WWW-Seiten aller Art, in sozialen Netzwerken, in Foren, in Newsgroups und Chaträumen sowie von "auskunftsfreudigen" E-Mail-Servern, welche die Gültigkeit von geratenen E-Mail-Adressen mitteilen. Auch werden Daten aus bereits gehackten Online Shops und älteren Angriffen verwendet . Alle Adressquellen haben gemeinsam, dass die Inhaber der E-Mail-Adressen einem Empfang von Spam weder zugestimmt haben, noch eine solche Zustimmung gutgläubig vermutet werden kann.

Die Software zum Sammeln von E-Mail-Adressen, als "Spider", "Harvester" oder "Spambot" bezeichnet, wird oft gemeinsam mit den Datenträgern auf Internet-Marktplätzen oder per Spam angeboten. Die Funktionsweise ist dabei einfach, aber effektiv: ein vom Nutzer gewählter Suchbegriff wird an mehrere Suchmaschinen (Google, Bing) weitergeleitet, welche zahlreiche WWW-Seiten zurückliefern, die diesen Begriff sowie E-Mail-Adressen enthalten. Anschließend werden diese Seiten direkt aufgerufen. Das Spider-Programm speichert die gefundenen Adressen in einer Textdatei, welche von der Spam-Software direkt verwendet wird.

[@]

E-Learning Datenschutz

Datenschutz praktische Lektion	https://juristi.de/home/index.php?quiz/