E-Mail Adresse missbraucht

Generell

Dieses Merkblatt soll sie darüber aufklären warum sie oder ihre Kunden auf einmal fragwürdige Emails von ihrer E-Mail Adresse erhalten, welche Fälle meistens auftreten und warum wir als Provider nichts dagegen unternehmen können.

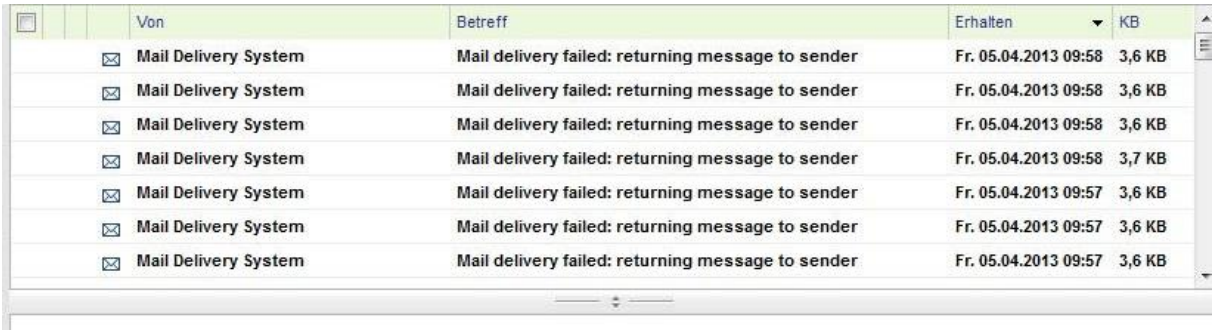
Wie wird ihre E-Mail Adresse missbraucht?

Ihr Konto wurde gehackt und es wird Spam versendet.

In diesem Fall konnte ein Angreifer entweder durch Malware, eine Phishing Seite oder ein zu leichtes Passwort Zugang zu ihrem E-Mail Konto erlangen. Oftmals versuchen Cyberkriminelle dann über die Mailserver Infrastruktur von VTX Spam E-Mails zu versenden. Sobald unsere Systeme ungewöhnliche Aktivitäten auf einer E-Mail Adresse feststellen, wird diese blockiert und sie werden vom Technischen Support informiert.

Ihre E-Mail Adresse wird als Absender missbraucht.

In diesem Fall wurde ihr Konto nicht gehackt. Ein Spammer benutzt lediglich ihre E-Mail Adresse als Absender. Dies können wir als Internet Provider **NICHT** verhindert. Sie können sich dies vergleichsweise mit der normalen Briefpost vorstellen. Falls jemand 1000 Briefe an diverse Schweizer Haushalte versendet und ihre Adresse als Absender missbraucht, werden Sie auf einmal diverse Briefe welche nicht zugestellt werden konnten in ihrem Briefkasten haben. Sie haben jedoch keine Ahnung warum es sich hier handelt. Vergleichsweise ist das mit E-Mail. In diesem Fall wird als Absender ihre E-Mail Adresse benutzt und x-tausend Spam Nachrichten verschickt. Falls eine Nachricht nicht zugestellt werden kann, erhalten sie auf **IHRER** E-Mail Adresse eine Fehlermeldung. In ihrem Postfach häufen sich dann Meldungen wie „**Mail delivery failed: returning message to sender**“



Von	Betreff	Erhalten	KB
Mail Delivery System	Mail delivery failed: returning message to sender	Fr. 05.04.2013 09:58	3,6 KB
Mail Delivery System	Mail delivery failed: returning message to sender	Fr. 05.04.2013 09:58	3,6 KB
Mail Delivery System	Mail delivery failed: returning message to sender	Fr. 05.04.2013 09:58	3,6 KB
Mail Delivery System	Mail delivery failed: returning message to sender	Fr. 05.04.2013 09:58	3,7 KB
Mail Delivery System	Mail delivery failed: returning message to sender	Fr. 05.04.2013 09:57	3,6 KB
Mail Delivery System	Mail delivery failed: returning message to sender	Fr. 05.04.2013 09:57	3,6 KB
Mail Delivery System	Mail delivery failed: returning message to sender	Fr. 05.04.2013 09:57	3,6 KB

Beispiel von Mail delivery failed Meldungen

Was können Sie tun um sich zu schützen?

- Sichern Sie ihre Computer mit einem Virenscanner ab und stellen Sie sicher dass ihr System regelmässig überprüft und der Virenscanner immer aktuell ist. Wenn Sie ihre E-Mail Adresse auf dem Computer zum Beispiel in Outlook eingerichtet haben kann Malware ihr Passwort stehlen.
- Benutzen Sie keine einfachen oder leicht zu erratenden Passwörter. Wechseln Sie ihr Passwort des öfteren.
- Sollten Sie Unregelmässigkeiten bei Ihrem E-Mail Konto feststellen ändern Sie auf jeden Fall das Passwort.

Nachfolgend finden Sie noch diverse Verhaltensregeln zu den Bereichen Passwort und E-Mail

Passwort

Sowohl ihr Rechner wie auch unterschiedliche Online-Dienste verlangen die Vergabe eines Passwortes. Schlecht gewählte oder zu kurze – also schwache – Passwörter stellen ein erhebliches Sicherheitsrisiko dar. Bei der Wahl eines Passwortes sind die folgenden Grundsätze zu beachten:

- **Mindestlänge von 8 Zeichen**
  Die Midestlänge des Passwortes sollte bei 8 Zeichen liegen und sowohl aus Buchstaben, Zahlen wie auch Sonderzeichen bestehen.

- **Einfach zu merken**
  Das Passwort ist so zu wählen, dass man es sich einfach merken kann. Schreiben sie keine Passwörter auf. Gute Passwörter bestehen aus ganzen Sätzen, die ebenfalls Sonderzeichen enthalten. Beispiel: «DiesesP@ssw0rt vergesse1chnie!!»

- **Passwort nicht mehrfach verwenden**
  Verwenden Sie verschiedene Passwörter für verschiedene Zwecke (z.B. für unterschiedliche Benutzerkonten). Bei der Nutzung von Online-Diensten wird dringend empfohlen, jeweils andere Passwörter zu verwenden.

- **Passwort regelmässig ändern**
  Ein Passwort sollte in regelmässigen Abständen (ca. alle 3 Monate) gewechselt werden, jedoch spätestens dann, wenn Sie vermuten, dass es Dritten bekannt sein könnte.

- **Passwort-Checker**
  Prüfen Sie ihr Passwort mit einen Passwort Checker auf dessen stärke. Sie können zum Beispiel folgendes Tool benutzen: https://www.passwortcheck.ch

E-Mail

E-Mail ist eines der beliebtesten Kommunikationsmittel. Allerdings gelangen die meisten elektronischen Schädlinge über E-Mail-Anhänge auf den Rechner. Ein sogrsamer Umgang mit E-Mails trägt erheblich zur Sicherheit ihrer Daten und ihres Rechners bei. Folgende Massnahmen schützen sie gegen Viren, Würmer, Trojaner, Malware und Spam.

Viren, Würmer und Malware

- **Vorsicht bei E-Mails mit unbekanntem Absender**
  Misstrauen sie E-Mails, deren Absenderadresse Sie nicht kennen. Öffnen Sie in diesem Fall keine angefügten Dokumente oder Programme und wählen sie keine darin angegebenen Links aus.

- **Auf Vertrauenswürdigkeit der Quellen achten**
  Öffnen Sie nur Dateien oder Programme aus vertrauenswürdigen Quellen und nur nach vorgängiger Prüfung mit einer aktuellen Antiviren-Software

- **Vorsicht bei Dateinamen mit zwei Endungen**
  Öffnen Sie keine E-Mail-Anhänge, die zwei Endungen aufweisen (z.B. picture.bmp.vbs). Lassen Sie sich nicht durch das Icon einer solchen Datei täuschen.

- **Software-Update des E-Mail-Clients**
  Auch E-Mail-Programme können Sicherheitslücken aufweisen. Vergewissern Sie sich regelmässig, ob ein Software-Update Ihres E-Mail-Programms vorhanden ist und spielen Sie dieses ein.

Spam

- **Vorsichtiger Umgang mit der E-Mail-Adresse**
  Geben Sie Ihre E-Mail-Adresse nur an so wenige Personen wie notwendig weiter und verwenden Sie diese ausschliesslich für wichtige Korrespondenz.

- **Anlegen einer zweiten E-Mail-Adresse**
  Für das Ausfüllen von Webformularen, das Abonnieren von Newslettern, Einträge in Gästebüchern, usw. empfiehlt es sich, eine zweite E-Mail-Adresse zu verwenden. Diese kann bei verschiedenen Anbietern kostenlos beantragt werden. Ist diese Adresse von Spam betroffen, kann sie gelöscht und ersetzt werden.

- **Spam nicht beantworten**
  Wird auf Spam geantwortet, so weiss der Sender, dass die E-Mail-Adresse gültig ist und wird weiter Spam verschicken. Mit Vorsicht ist auch Spam mit «Abbestelloption» zu geniessen. Darin wird versprochen, dass man durch Senden einer E-Mail mit bestimmtem Inhalt von der Verteilerliste gestrichen wird. In diesem Zusammenhang sind auch automatische Antwortmails bei Ferienabwesenheit zu beachten. Sie sollten lediglich bei bekannten Adressen aktiviert werden.