

Wirtschaft

E-Mail-Terror als Ablenkungsmanöver

Hintergrund. Hunderte Mails in wenigen Minuten. Was wie harmloser Spam aussieht, ist oft eine Nebelkerze. Dahinter kapern Betrüger Konten und bestellen munter auf Rechnung der Geschädigten

Von Melanie Ptok

Das Smartphone vibriert im Sekundentakt. Das E-Mail-Postfach läuft über. Minütlich treffen neue Newsletter-Bestätigungen ein, die nie angefordert wurden. Was auf den ersten Blick wie lästiger Spam wirkt, kann Teil einer gezielten Betrugsmasche sein: Cyberkriminelle überfluten die Mailbox ihres Opfers, um ihre eigentlichen Aktivitäten im Hintergrund zu verschleiern. Das ist „E-Mail-Bombing“.

Dabei handelt es sich um einen Spam-Angriff, bei dem der Mail-Account mit automatisierten Nachrichten bombardiert wird. „Hier ist ihr Bestätigungscode: 569299“, „Ihre Newsletter-Anmeldung war erfolgreich“. 103 Mails innerhalb von zwei Minuten. Pro Tag können es 2.000 bis 3.000 E-Mails sein.

Ziel der Betrüger ist nicht die Sabotage. Stattdessen wollen sie ihre eigentlichen Aktivitäten vor dem Opfer verbergen. „Hinter einem E-Mail-Bombing steckt häufig der Versuch, Transaktionen oder Sicherheitsbenachrichtigungen in der Flut von E-Mails zu verstecken“, sagen die Experten von BEE SECURE, einer Initiative der Regierung für sicheren Umgang im Netz. Und es funktioniert, wie diverse Schadenfälle belegen. Kein Wunder: In der Flut der Mails den Überblick zu behalten, ist eine echte Herausforderung.

Verstehen, was passiert

Also versenden die Betrüger unzählige automatisierte Nachrichten, um eben zu vertuschen, dass sie tatsächlich gerade das Konto hacken, auf digitale Bezahlstellen zugreifen

und Bestellungen im Namen des Opfers tätigen.

Während Betroffene noch versuchen, die Flut an Nachrichten zu durchschauen, schlagen die Täter zu. Wie das aussehen kann, zeigt ein Fall, der dem „Luxemburger Wort“ von einer Betroffenen geschildert wurde.

● **Hinter E-Mail-Bombing steckt häufig der Versuch, Transaktionen oder Sicherheitsbenachrichtigungen in der Flut von E-Mails zu verstecken.**

BEE SECURE

Bei ihr hatte es der Betrüger auf ihren Account bei einem Online-Shop abgesehen. Über das Konto wurde eine Bestellung von Jogginghosen im Wert von fast 200 Euro aufgegeben. Die Betroffene hatte dies nicht sofort bemerkt. Der Online-Shop hingegen schon, die Betroffene hatte Glück. Zwei Tage nach der Mailbombe auf ihr Postfach erhielt sie eine Nachricht vom Online-Shop: „Ihre Bestellung wurde storniert.“

Dabei ging sie davon aus, gar nichts bestellt zu haben. Doch, als sie ihre Mails durchsuchte, fand sie eine Bestellbestätigung. Just an jenem Abend eingegangen, an dem ihr Mail-Account überflutet wurde. Der Betrüger gab ihre Rechnungsadresse an. Ge-

liefert werden sollte das Paket aber an eine Packstation in Berlin. Der Händler durchschaute dies und die Betroffene änderte sofort alle ihre Passwörter.

Wie sollten Betroffene reagieren?

Das ist längst kein Einzelfall. Wie häufig Mail-Bombing in Luxemburg vorkommt, lässt sich zwar nicht beziffern, doch Cyberbetrug beschwärtigt die Sicherheitsbehörden zunehmend. Und Mail-Bombing als eine bösartige Unterform gehört dazu. Zwischen 2024 und 2025 stieg allein die Zahl der Phishing-Meldungen, die der Polizei gemeldet wurden, von 247 auf 367. Experten warnen, dass die Methoden der Täter immer professioneller werden.

Mail-Bombing ist den Beamten der großherzoglichen Polizei und Experten von BEE SECURE durchaus bekannt. Die Cybersicherheitsexperten haben zu solchen Vorfällen bereits Meldung erhalten. Ob es sich dabei um größeren Betrug handelt, muss noch eruiert werden, wie das „Luxemburger Wort“ erfuhr.

In jedem Fall raten Experten zu einem schnellen Vorgehen, wenn das eigene Postfach plötzlich mit Nachrichten überflutet wird.

„Betroffene sollten zunächst ihre wichtigen Online-Konten überprüfen, insbesondere bei Banken, Zahlungsdiensten und Online-Shops“, so die BEE SECURE-Experten. Anschließend sollte man kontrollieren, ob verdächtige Transaktionen oder unbekannte Anmeldungen bei den eigenen Konten stattgefunden haben. Gleiches gelte für das eigene E-Mail-Konto.

Wie kann man sich davor schützen?

Fest steht: Eine Mailbombe und die daraus resultierende Nachrichtenflut lassen sich nicht vollständig verhindern. „Den Kriminellen reicht häufig bereits die Kenntnis einer E-Mail-Adresse, um automatisiert zahlreiche Anmeldungen auszulösen“, sagen die BEE SECURE-Experten. Daher sollte man bei der Vergabe der E-Mail-Adresse, etwa bei Online-Anmeldungen, sparsam sein. „Einige Anmelddienste bieten die Möglichkeit, die eigentliche E-Mail-Adresse zu verbergen und stattdessen eine zufällig generierte Weiterleitungsadresse zu verwenden“, so BEE SECURE. In der Fachwelt spricht man von einem Alias.

Dadurch könne die persönliche E-Mail-Adresse bei Datenlecks seltener in Umlauf geraten und somit auch seltener für Angriffe wie E-Mail-Bombing verwendet werden. Lässt sich die Nachrichtenflut langfristig nicht eindämmen, oder wird die Adresse immer wieder für Spam missbraucht, kann im Extremfall auch ein Wechsel der E-Mail-Adresse sinnvoll sein.

Um herauszufinden, ob man selbst von einem Datenleck betroffen ist, kann man die persönliche E-Mail-Adresse auf der Webseite haveibeenpwned.com eingeben.

Kontrolle behalten

Hundertprozentig lässt sich eine Mailbombe nicht verhindern. Nutzer können aber das Risiko eines erfolgreichen Angriffs minimieren. BEE SECURE empfiehlt dazu, die Zwei-Faktor-Authentifizierung (2FA) zu aktivieren und, wo möglich, einen sogenann-

ten Passkey einzurichten. „Ein Passkey ersetzt das Passwort und wird per Fingerabdruck oder Gesichtserkennung freigegeben“, erklären die Experten.

Auch Filterfunktionen können helfen, wichtige Nachrichten von Spam zu trennen. „Wurde man bei zahlreichen Newslettern angemeldet, gibt es zudem Möglichkeiten, sich gesammelt von Abonnements abzumelden“, so BEE SECURE. Der „Abmelde-dienst“ ist häufig und je nach Mail-Dienst in die Funktionen des Programms direkt integriert.

● **Wenn persönliche Daten oder finanzielle Mittel betroffen sind oder ein unbefugter Zugriff auf ein Konto festgestellt wurde, sollte zeitnah reagiert werden.**

Police grand-ducale

Laut den Experten bieten mehrere E-Mail-Anbieter solche Funktionen direkt an. Alternativ gibt es spezialisierte Drittanbieter-Tools, die im Mail-Programm installiert werden können. „Bei Letzteren sollte man allerdings genau prüfen, welche Zugriffsrechte diese Anbieter auf das eigene E-Mail-Konto verlangen.“

Spuren zurück zum Täter

Letztlich gilt immer: Wer Opfer eines solchen Angriffs wird, möchte wissen, wer dahintersteckt. Das Herausfinden ist jedoch oft kompliziert. Ein Sprecher der Polizei bestätigt: „Was die Rückverfolgung beziehungsweise Identifizierung möglicher Täter betrifft, hängt dies stark vom jeweiligen Einzelfall und den verfügbaren technischen sowie sonstigen Ermittlungsansätzen ab.“

Zu den konkreten Ermittlungsmethoden können die Beamten allerdings keine Angaben machen. Im Kampf gegen Cyberkriminalität die Nase vorn zu haben, ist für die Ermittler essenziell. Allein die Methoden sind bereits sehr aufwendig und ressourcenintensiv und können sich über einen längeren Zeitraum erstrecken.

Tipps der Polizei

Wer sich vor Betrugsmaschinen schützen möchte, sollte folgende Punkte beachten:

- Keine persönlichen Informationen, Zugangsdaten oder Bankdaten weitergeben, wenn sie per E-Mail, SMS, Telefon oder über andere Nachrichtendienste dazu aufgefordert werden

- Links oder Anhänge aus unbekannten oder verdächtigen Quellen sollten nicht geöffnet werden

- Vorsicht ist geboten, wenn man zu einer schnellen Reaktion gedrängt oder unter Druck gesetzt wird

- Bei Zweifeln an der Herkunft einer Nachricht empfiehlt es sich, die betreffende Organisation oder das Unternehmen ausschließlich über bekannte und offizielle Kontaktwege zu kontaktieren. Sollte festgestellt werden, dass unbefugt auf ein Konto zugegriffen wurde, sollten der jeweilige Anbieter beziehungsweise die Bank umgehend kontaktiert und die betroffenen Zugangsdaten geändert werden.

Betrugsversuche oder tatsächliche Betrugsfälle können jederzeit bei der Polizei angezeigt werden. „Insbesondere wenn persönliche Daten, Zugangsdaten oder finanzielle Mittel betroffen sind oder ein unbefugter Zugriff auf ein Konto festgestellt wurde, sollte zeitnah reagiert werden“, sagt der Polizeisprecher. Auf ihrer Webseite informiert die Polizei über gängige Betrugs-maschinen, und wie Betroffene damit umgehen sollten.



Wer plötzlich mit Hunderten E-Mails bombardiert wird, sollte aufmerksam werden. Denn hinter dem digitalen Chaos können Betrüger versuchen, Bestellungen, Kontozugriffe oder Zahlungsvorgänge zu verschleiern.

Illustration: Sabina Palanca