„Sie müssen zahlen!“

Alles hat zwei Seiten: Mail-Kommunikation ist praktisch, gleichzeitig stellen E-Mails in Form von Schad-Spam die größte Bedrohung auch für Vermittlerunternehmen dar. Grundlegende technische und organisatorische Maßnahmen können jedoch schützen. Oft ist der Mensch der Schwachpunkt im System.

Die größte Gefahr lauert oft im scheinbar harmlosen Posteingang. Je nach Studie handelt es sich bei 50 bis 85 Prozent aller E-Mails um unerwünschten und mitunter auch gefährlichen Spam (englisch für Abfall oder Plunder). Dabei sind die Mailaccounts von Unternehmen gleichermaßen wie die von Privatnutzern betroffen. In den meisten Fällen handelt es sich um plumpen Werbe- und Betrugs-Spam, den der Nutzer leicht erkennen kann. Gerade die gefährlichsten Spielarten entgehen den automatisierten Spam-Filtern allerdings häufig.

Und diese Mails führen Böses im Schilde. Bei Angriffen auf Großkonzerne wird solche Schadware gern genutzt, um sensible Daten und Interna auszuspionieren. Am beliebtesten bei Cyber-Kriminellen ist zurzeit allerdings die Spielart der erpresserischen Ransomware. Diese verschlüsselt Daten und Ordner – und das meist so gut, dass selbst Profis sie nicht wieder freilegen können.

Die berüchtigte Schadware wird über Mail-Anhänge transportiert und aktiv, sobald diese geöffnet werden. Oder es befinden sich im Mail-Text Links auf infizierte Webseiten. Werden die Links angeklickt, lädt sich über eine so genannte „Drive by Infektion“ die gefährliche Schadware. Von heute auf morgen lässt sich im schlimmsten Fall dann nicht mehr auf geschäftsrelevante Daten und Prozesse zugreifen. Für die Entschlüsselung verlangen die Täter eine Art Lösegeld – zahlbar in der anonymen virtuellen Hackerwährung Bitcoin. Wurde gezahlt, erhalten die Opfer einen Code für die Entschlüsselung, wobei selbst das nicht immer geschieht. Dann sind sie gleich doppelt geprellt.

Ein Phänomen unserer Zeit

Auch Versicherungsvermittler sind von E-Mail-Gefahren betroffen. „Spam-Mails sind ein bekanntes und weitverbreitetes Problem im Versicherungs- und Finanzbereich. Gerade hier spielt die Kommunikation zwischen Berater und Kunde per E-Mail eine übergeordnete Rolle, da häufig Informationen per E-Mail eingeholt werden“, meint Ludwig-Maximilian Reitinger, Geschäftsführer des IT-Dienstleisters Maklersoftware.com. Es liege in der Natur des Vermittlerberufs, den eigenen Kontakt und somit die E-Mail-Adresse zu verbreiten. Im Laufe der Jahre komme es deshalb häufig zu einem erhöhten Aufkommen problematischer Mails im Postfach. Wie stark das Spam-Aufkommen ist, hänge insgesamt stark vom Verhalten des jeweiligen Nutzers sowie des Providers dahinter ab, der den Spam auffangen soll. Da in größeren Unternehmen meist bessere Sicherheitsvorkehrungen getroffen werden und die Mail-Adressen eher nicht privat genutzt werden, sei hier das Spam-Risiko geringer gegenüber soloselbstständigen Versicherungsmaklern, so Reitinger.

Kompakt

- Am beliebtesten ist bei Cyber-Kriminellen derzeit der Einsatz von Ransomware.
- Diese wird über Mail-Anhänge aktiv, wenn sie geöffnet wird. Für die Entschlüsselung verlangt der Täter Geld.
- Besondere Vorsicht ist bei Links und Mail-Anhängen angebracht.

Es handle sich schlicht um ein Phänomen unserer Zeit, meint Enrico Franz, Mitglied im Arbeitskreis IT des Verbands Deutscher Versicherungsmakler (VDVM). Es gehe den Spammern darum, sich durch Unwissenheit oder Unachtsamkeit von Einzelpersonen Vorteile zu verschaffen. Anders als vor einigen Jahren sei man in den meisten Unternehmen mittlerweile jedoch deutlich weiter: „Die meisten der Kollegen haben IT-Sicherheitskonzepte, die auch gelebt werden, und eigene Datenschutzbeauftragte.“

Generell sei die Branche heute gut aufgestellt. Allerdings könne man die Situation natürlich nicht pauschal beurteilen, zu groß seien die Unterschiede bei den Marktakteuren: „Wir haben kleine und große Maklerunternehmen im Markt, jüngere und ältere Geschäftsführer. Der Grad der technischen Affinität ist in den Unternehmen sehr unterschiedlich, die technische Ausstattung und die genutzte Infrastruktur sind es auch.“

Wer betroffen ist, macht das ungern freiwillig öffentlich, zu groß ist die Angst vor einem Imageverlust oder vor der Häme von Wettbewerbern. Konkrete Zahlen zu Betroffenen gibt es wie in anderen Branchen nicht. Die allgemeinen Angaben zum Spam-Anteil schwanken erheblich. 86 Prozent aller global versendeten Mails sind Spam, meint der große IT-Sicherheitsdienstleister Cisco. Deut-

lich weniger sind es laut Bundesamt für Sicherheit in der Informationstechnik (BSI), das Angaben verschiedener deutscher Mail-Dienstleister zusammengetragen hat. Demnach lag der klassische Verkaufs-Spam in Deutschland bei 40 Prozent, Schad-Spam macht durchschnittlich zehn Prozent aus und besteht zu einem großen Teil aus Ransomware. Der Wert unterliegt aber erheblichen Fluktuationen und erreichte im Dezember letzten Jahres einen Spitzenwert von 30 Prozent.

Foto: © santiago silver/Fotolia

Spam, der gar keiner ist

Versicherungsvermittler sind wie alle Geschäftstreibende darüber hinaus stets doppelt vom Thema Spam betroffen, denn immer wieder sortieren Spam-Filter unbemerkt auch legitime Mails aus. Transaktionsbestätigungen sowie ganz legale Angebots-, Werbe- und Newsletter-Mails verschwinden dann in den Spam-Ordnern von Privatnutzern.

Wie also umgehen mit der zweifachen Zumutung durch das Spam-Unwesen? „E-Mail-Marketing ist extrem komplex geworden. Wenn ich als Makler massenhaft E-Mails verschicke, lande ich schnell auf dem Spam-Index“, meint IT-Experte Franz vom VDVM. Er empfiehlt deswegen, entweder mit einer professionellen Agentur zusammenzuarbeiten, die sich auf den sicheren Versand von Mails spezialisiert hat, oder inhouse in gute und erfahrene Mitarbeiter und Systeme zu investieren.

Anders als in anderen Branchen spiele der Massenversand von Mails allerdings nicht die große Rolle. Und er gibt zu bedenken, dass Kunden solche Mails generell nicht positiv bewerten. Deswegen rät er, behutsam vorzugehen: „Es ist besser, vorher zu klären: Darf ich mit meinem Bestandskunden per E-Mail in Kontakt treten? Viele erlauben eine Kontaktaufnahme per Brief oder Telefon, aber nicht per Mail. Wenn er es erlaubt, dann sollte ich auch die Möglichkeit anbieten, Newsletter abzubestellen.“

Und der mittlerweile essenzielle Kampf gegen Mail-Bedrohungen muss stets auf zwei Gebieten ausgefochten werden: technisch und organisatorisch. Technisch bietet sich der Einsatz etablierter Spam-Filter-Systeme an, deren Algorithmen permanent neuen Bedrohungslagen angepasst werden. Wichtig sind auch regelmäßige Datensicherungen, die am besten physisch getrennt vom sonstigen System aufbewahrt werden. Zudem ist es wichtig, Mitarbeiter für den Umgang mit dem Thema zu sensibilisieren. Im technologischen Wettrüsten gelingt es Spammern immer wieder, an den Filtern vorbei in den normalen Posteingang zu gelangen. Die große Frage ist dann, ob die gefährlichen Mails manuell erkannt werden oder tatsächlich zum Einfallstor für Schadware werden.

Enrico Franz empfiehlt, bei Mails genau hinzuschauen. Zuerst gelte es, den Absender zu prüfen: Kenne ich den? Dabei müsse man auch verifizieren, wer tatsächlich hinter der Mail steht. Spammer geben sich durch Maskierung gern als vermeintlich seriöse Absender aus. Meist ermögliche ein Doppelklick auf das Absenderfeld eine solche Prüfung. Besondere Vorsicht sei bei Links und Anhängen angebracht. Auch hier setzen Spammer gern auf Täuschung. Führt er vermeintlich auf ein bekanntes Angebot wie Amazon oder Paypal, mache es Sinn, nicht direkt über den Link zu gehen, sondern die jeweilige Webseite direkt im Browser aufzurufen und sich dann dort einzuloggen. Und besonderes Gefahrenpotenzial gebe es auch bei Anhängen. Er empfiehlt: „Nicht anklicken, wenn sich im Anhang selbst ausführende Dateien mit einer Endung wie .exe oder .msi befinden, extreme Vorsicht ist auch bei Zip-Archiven angeraten.“ Wenn es sich offensichtlich um einen Betrugsversuch handelt, sollte man die Mail nicht bearbeiten und den internen IT-Beauftragten oder externen IT-Dienstleister um rasche Hilfe bitten.

Eine automatische Erkennung von Gefahren vermag eben nicht alles, so Franz: „Technische Systeme können heutzutage vieles leisten. Wenn aber ein Mitarbeiter aus Unwissenheit oder Unachtsamkeit eine Mail mit verdächtigem oder schädlichem Inhalt öffnet oder nicht bemerkt, dass er Ziel eines Angriffs ist, hat der Angreifer es leicht, sein Ziel zu erreichen.“ ■

Autor: Stefan Mey ist freier Journalist in Berlin.