Oh nein, ich habe Phishing Mails versandt!

Was ist Phishing überhaupt?

Phishing ist ein Kunstwort aus "Passwort" und "Fishing". Kriminelle versuchen mit gefälschten E-Mails persönliche Daten, insbesondere Login-Daten, von ihren Opfern zu erbeuten, indem sie sie auf ebenfalls gefälschte Webseiten locken und zur Eingabe ihrer Daten verleiten. Dabei ist das Spektrum an nachgeahmten Unternehmen inzwischen vielfältig. Längst nicht mehr nur Banken, sondern auch Online Shops, Social Media, online Spiele und viele andere werden nachgeahmt.

Warum dieser Artikel?

Während es sehr viele Informationen für Endanwender gibt wie man Phishing erkennen kann, z.B. auf https://wiki.botfrei.de/Phishing und https://blog.botfrei.de/?s=phishing und bei den Mailbox Providern gängige Best Practices existieren um eingehende Phishing E-Mails möglichst zu erkennen (z.B. https://www.m3aawg.org/sites/default/files/M3AAWG_AWPG_Anti_Phishing_Best_Practices-2015-06.pdf), konzentriert man sich auf Versender Seite insbesondere darauf die eigenen, legitimen E-Mails mittels Authentifizierungsmaßnahmen - also SPF, DKIM und DMARC - von Phishing E-Mails unterscheidbar zu machen, um den Mailbox Providern wiederum das herausfiltern von Phishing E-Mails zu erleichtern.

Leider ist es nicht ausgeschlossen, dass Kriminelle die Versandplattformen professioneller Versender missbrauchen um Phishing E-Mails zu versenden. Das ist deshalb besonders perfide, da professionelle Versender typischerweise leistungsfähige Versandplattformen haben und gängige Authentifizierungsmaßnahmen implementiert haben. Wie kann man das als Versender vermeiden, und falls es passiert ist, die Folgeschäden minimieren?

Wie verhindere ich ausgehende Phishing E-Mails?

Ein erster Schritt ist mit Sicherheit das Einsetzen eines Spamfilters beim Versender, der ausgehende E-Mails vor dem Versand überprüft und ggf. automatisch stoppt. Dieser Filter kann auch etwas "aggressiver" Filtern als ein typischer eingehender Filter bei Mailbox Providern, denn im Zweifelsfall kann eine E-Mail nach einer manuellen Kontrolle durch einen Mitarbeiter mit etwas Verzögerung doch noch freigegeben und versandt werden.

Darüber hinaus kann es hilfreich sein sämtliche in den E-Mails eingefügten Links gegen gängige Listen wie die Google Safe Browsing List (https://developers.google.com/safe-browsing/v4/lists) oder die Liste von PhishTank (https://www.phishtank.com/) abzugleichen. Auch hier wäre die Aussendung zunächst zu stoppen und durch einen Mitarbeiter zu prüfen. Insbesondere wenn in der Vergangenheit bereits Phishing-Fälle auf der eigenen Plattform aufgetreten sind kann man auch typische Verhaltensmuster der Kriminellen (nutzername, loginorte, loginzeiten, zahlungsdaten, usw.) aus den historischen Daten gewinnen und die eigene Plattform auf eben solche Verhaltensmuster unter den aktuell aktiven Nutzern hin überwachen.

Es ist dennoch passiert, was nun?

Phishing E-Mails zu erkennen ist nicht einfach. Filter und Listen sind oftmals erst dann wirksam, wenn bereits etwas passiert ist. Zeit ist hier ein kritischer Faktor. Je früher der Versand der E-Mails gestoppt werden kann, desto weniger gefährliche E-Mails landen beim Mailbox Provider und damit beim Endnutzer. Das drosseln der Versandgeschwindigkeit bei neuen Accounts kann daher eine Methode sein den Reaktionsspielraum zu vergrößern. Ständiges Monitoring von Blacklisten, Reputationsdaten, Feedbackloops, usw. hilft dabei einen Fall möglichst frühzeitig zu erkennen und den Versand anzuhalten.

Darüber hinaus sollten sämtliche in der als Phishing erkannten E-Mail enthaltenen Weiterleitungen (Trackinglinks) sofort deaktiviert oder auf eine entsprechende Warnungsseite umgeleitet werden. Auch hierbei gilt wieder: eine schnelle Reaktionszeit ist entscheidend! Die bereits versandten E-Mails lassen sich nicht zurückholen, allerdings kann ein Phishingopfer vor weiterem Schaden bewahrt werden, wenn die Links in einer Phishing E-Mail nicht auf eine bösartige Webseite führen.

Eine weitere Möglichkeit die Empfänger von Phishing E-Mails zu warnen besteht darin, dass falls Logos und Grafiken über ein Content Management System beim Versender vorgehalten und vom Empfänger der E-Mail beim Öffnen geladen werden, diese Grafiken auszutauschen und mit deutlichen Warnungen zu versehen, dass es sich um eine betrügerische E-Mail handelt. Es macht einen großen Unterschied, ob der Endnutzer eine täuschend echt aussehende gefälschte E-Mail vorfindet, oder eine die völlig anders aussieht und mit optisch auffälligen Warnungen versehen ist.

Fazit

Phishing ist ein schwerwiegendes Problem, und auch in Zeiten von Authentifizierung mit SPF, DKIM und DMARC nicht gelöst. Das Erkennen von ausgehenden Phishing E-Mails ist nicht einfach, doch durchaus möglich. Insbesondere das Abgleichen mit typischen Verhaltensmustern ist hier vielversprechend. Doch selbst wenn die eigene Plattform für den Versand von Phishing missbraucht wurde kann man als Versender noch immer viel für den Schutz des Endnutzers tun. Allen voran das schnelle deaktivieren, bzw. umleiten von Tracking Links hilft den entstandenen Schaden zu minimieren.

Autoren: Technical Team der Certified Senders Alliance