Phishing-Mails 2.0 sind auch ohne Link gefährlich

Bisher war klar: eine E-Mail mit einem seltsamen Link – Finger weg! Aber jetzt haben die Phishing-Gangster einen neuen Trick ersonnen, um Anwender ganz ohne Links hinters Licht zu führen. Doch auch diese Betrugsattacken lassen sich mit ein bisschen Aufmerksamkeit rechtzeitig erkennen und neutralisieren.

Es ist das ewige “Spiel“ zwischen Security-Spezialisten und Cybergaunern: wer ist schneller, kreativer und hat den längeren Atem. Getreu nach diesem Motto haben sich die Internetschurken wieder etwas Neues einfallen lassen: Phishing-E-Mails ohne Link.

Die meisten Phishing-E-Mails sind auf drei wesentlichen Komponenten aufgebaut:

1. Eine E-Mail mit einem Link, auf den der Anwender klicken soll.
2. Eine Fake-Webseite, auf der sich der Anwender einloggen soll.
3. Eine weiter oder dieselbe Internetseite, welche die Login-Daten an die Gangster übermittelt

Die SophosLabs haben nun zwei außergewöhnliche Phishing-Attacken analysiert, die einen anderen Weg gehen. Bei diesen erfolgt die Aufforderung zum Login nicht über einen Link, sondern über einen HTML-Anhang. Mit diesem „Bring-Your-Own-Website“-Trick verfolgen die Cybergauner zwei Intentionen:

- In der Phishing-E-Mail befindet sich kein Link, den man im Voraus auf gefälschte oder verdächtige Domänennamen prüfen könnte.
- Die URL in der Adressleiste ist ein harmlos aussehender lokaler Dateiname ohne Website-Name oder HTTPS-Zertifikat. Auch hier ist eine Untersuchung auf Anzeichen von Betrug für den Anwender nur schwer möglich.

Mit diesem Vorgehen versuchen die Mail-Versender die Achtsamkeit der Anwender zu unterlaufen. Das wichtigste Ziel ist es, den Anwender von der vermeintlichen Ungefährlichkeit des Anhangs zu überzeugen und damit eine der schwierigsten Hürden für ihre Jagd auf Anmeldedaten zu nehmen, die in diesem Fall über die angehängte Internetseite abgezogen werden sollen. Dabei dies nicht passiert, sollten Nutzer solchen Phishing-Attacken mit den folgenden Tipps vorbeugen:

- HTM- oder HTML-Anhänge möglichst ignorieren
- Nutzung einer Zwei-Faktor-Authentifizierung
- Nutzung einer wirksamen Web-Filterung, wie beispielsweise mit dem kostenlosen Sophos Home

Und natürlich sollte beim Verdacht, einem Phishing-Angriff auf den Leim gegangen zu sein, sofort das Passwort des entsprechenden Services geändert werden. Auf Sophos Naked Security sind weitere Details zu den Phishing-E-Mails 2.0 anschaulich mit vielen Screenshots beschrieben. Zum kompletten englischen Beitrag geht es hier:
https://nakedsecurity.sophos.com/2020/10/02/serious-security-phishing-without-links-when-phishers-bring-along-their-own-web-pages/

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de