Komm her, du Wurm! Google Docs-Attacke – weit mehr als ein Phishing-Angriff

Ist der aktuelle Angriff auf Google Docs wirklich nur ein weiteres Phishing-Beispiel? Weit mehr als das, sind sich die Sophos Experten einig.

Wiesbaden, 9. Mai 2017. Auf den ersten Blick erscheint die aktuelle Google Docs Attacke ein weiteres Phishing-Beispiel zu sein. Tatsächlich aber handelt es sich laut Michael Veit, Technology Evangelist bei Sophos, um etwas ganz anderes:

„Zuallererst muss man diese Attacke als Missbrauch von Googles APIs verstehen, also der Schnittstelle, die die Google-Funktionalität sicherstellt – auch wenn der Angriff zunächst als Phishing erscheint: man erhält eine Email mit einer Gmail-Endung, die einen auf eine Authentifizierungsseite von Google locken will. Durch die Autorisierung nutzt die schadhafte App den Email Account und die Kontakte für seine eigenen Zwecke. Damit kann diese zunächst relativ harmlose Google-Attacke weit mehr: sie hat das Zeug, zum Virus zu werden, wie der Love Bug Virus aus dem Jahr 2000 oder die schädliche FriendGreeting Adware (Software, die zusätzlich Werbung anzeigt). Technisch gesehen macht das die Google Docs Attacke sogar zum Wurm – also einer speziellen Art von Virus, der sich selbst verbreitet, ohne auf Host-Dateien als Wirt angewiesen zu sein. Ein Relikt vergangener Zeit sozusagen.

Seit Langem wissen wir um die Verletzbarkeit von Systemen, auf die sich jeder als Entwickler, der OAuth nutzt, einloggen kann. Und die Überprüfung der App-Entwickler liegt hier eindeutig bei den Plattformen selbst. Kürzlich wurde ein Missbrauch beim Google Play Store aufgedeckt – auch hier wieder durch Malware-Autoren.

Wie funktioniert die Attacke:
1. Der Anwender bekommt eine Email – sehr wahrscheinlich von einer bekannten Person, die selbst gar nicht weiß, dass diese Email von ihrem Account kommt. Tückisch, denn man geht davon aus, dass derjenige wirklich auf Google Docs Dateien mit einem teilen möchte.

2. Klickt man auf den „Open in Docs“-Link, landet man auf einer Webseite, die einen auffordert, eine Gmail App herunterzuladen und den Zugang zu Email und Kontakten zu gewähren. Hier schon sollte man misstrauisch sein, denn man benötigt keine App, um Google Docs-Dateien zu öffnen. Besonders heimtückisch: die App zum Herunterladen nennt sich natürlich nicht Gmail App sondern „Google Docs“. Man fühlt sich also auf der sicheren Seite.

3. Ein Versuch, herauszufinden, ob es wirklich eine Mail von Google ist, geht so: auf „Google Docs“ klicken und den aktuellen Account sehen, der die Anfrage stellt. Aber auch da könnten glaubhafte Angaben stehen, es gibt keine spezifischen Hinweise, nach denen man Ausschau halten könnte.

Wie kann man sich schützen?
1. Der einzig verlässliche Weg: niemals Apps akzeptieren, die mit dem Account verbunden sind, und Zugang zu Email und Kontakten anfordern bzw. sonstigen Zugang erfragen, es sei denn man will gerade einen neuen Service dazu schalten. Aber auch hier hilft der gesunde Menschenverstand. Hat man kein gutes Gefühl, lieber lassen.

2. Generell misstrauisch gegenüber Legitimationsabfragen durch Services von Google, Twitter, Facebook und anderen Online-Seiten sein, die OAuth mit einem nicht-geprüften Application-Entwicklerprogramm verwenden. Alle Provider von OAuth tragen die Verantwortung, die Nutzung ihrer Plattform zu kontrollieren, damit User nicht durch offizielle Anfragen durch die Plattformbetreiber wie Google, Twitter, etc. in eine Falle gelockt werden.

3. Überprüfen aller Apps in den Social-Media-Kanälen, die Zugangsrechte zu den Accounts haben.

4. Apps löschen, bei denen man sich nicht sicher ist, ob sie auf OAuth-basierten Plattformen laufen. Bei Google findet man diese Einstellungen unter seinem Account-→ Sign-in & Security → Connected Apps & Sites. Bei Twitter und Facebook in die Settings & Pricavy → Apps schauen.

Und ganz wichtig: Hat man bereits auf den Link geklickt, werden wahrscheinlich sämtliche Kontakte diese Aufforderung erhalten. Deshalb: schnell Freunde und Kollegen informieren, dass der eigene Account gehackt wurde und welches Ausmaß hinter der vermeintlichen Phishing-Attacke steckt: ein waschechter Virus!“

Über Sophos
Sophos ist führender Anbieter von Endpoint- und Network-Security-Lösungen der nächsten Generation. Als Pionier der Synchronized Security entwickelt Sophos sein innovatives Portfolio an Endpoint-, Netzwerk-, Verschlüsselungs-, Web-, E-Mail- und mobilen Security-Lösungen, die miteinander kommunizieren. Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Lösungen von Sophos mit hervorragendem Schutz vor anspruchsvollen Bedrohungen und Datenverlust. Sophos Produkte sind exklusiv über den weltweiten Channel mit mehr als 26.000 registrierten Partnern erhältlich. Sophos hat seinen Hauptsitz in Oxford, Großbritannien, und wird an der Londoner Börse unter dem Symbol "SOPH" öffentlich gehandelt. Weitere Informationen unter www.sophos.de

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
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 +172 4536839
sophos@tc-communications.de