Forschungsobjekt Phishing

Sophos untersucht, welche Phishing-Typen es gibt, wie sie arbeiten und wie Phishing zu bekämpfen ist

Phishing ist eine der häufigsten und aggressivsten Angriffsmethoden von Hackern. Phishing-Attacken nutzen das Verhalten des Endanwenders als schwächstes Glied in der Cyber-Abwehr eines Unternehmens aus. Dabei gehen Cyberkriminelle immer subtiler und auch gezielter vor und es wird zunehmend schwieriger, wirkungsvolle Schutzmaßnahmen zu ergreifen. Sophos hat das sehr lästige Phishing zum Forschungsobjekt seiner Labs gemacht: Typisierung, Arbeitsweise, aber auch Bekämpfung und vorsorgliche Schutzmaßen wurden in einem eigenen White Paper zusammengetragen. Beste Abwehrstrategie: Prävention durch Mensch und Technik in Verbindung mit fortschrittlichen Sicherheitstechnologien.

Phishing – eine Typisierung
Phishing-Angriffe lassen sich nach Sophos Labs grob in grundsätzlich zwei verschiedene Typen unterteilen:

Massenhaftes-Phishing

- Angriffe auf individuelle Vermögen
- Typischerweise Konsumenten einer Marke oder Dienstleistung
- Entpersonalisierte massenhafte Ausschüttung
- Fokussiert auf den Diebstahl von persönlichen Daten (Log-Ins)

Typisches Beispiel:
Lieber Netflix-Kunde,
wir schicken Ihnen diese Mail, um Ihnen mitzuteilen, dass Ihre Kreditkarte abgelaufen ist. Um Ihre Account-Informationen zu aktualisieren, klicken Sie bitte hier: Ihr Account.
Ihr Netflix-Team

Speerwurf-Phishing

- Angriffe auf Vermögen spezieller Organisationen
- Typischerweise auf Individuen oder spezielle Gruppierungen in der Organisation
- Gefälschte (Look-a-like) Email-Adressen, um eine Konversation zu vermeiden
- Nachahmung von zuverlässigen Quellen bzw. Senior-Entscheidern

Speerwurf-Phishing-Angriffe sind in zunehmendem Maße alltäglich geworden und Cyberkriminelle verbessern stetig ihre Techniken, um effektiver zu werden. Von 330 kürzlich befragten IT-Fachleuten bestätigten 55 Prozent, dass ihre Senior Manager in einer derartigen Attacke nachgeahmt wurden.

Eine noch gezielter anvisierte Teilmenge nutzt Social Engineering, um bestimmte Daten zu bekommen und die Umwandlung zu verbessern – ein Sonderfall der Speerwurf-Typologie. Auch bekannt als CEO-Betrug, dem originell klingenden Whaling (also große Meerestiere angeln) oder Business Email Compromise (BEC).

Unterschied zwischen Massen- und Speerwurf-Angriffen: Der Köder
Der Köder von Speerwurf-Attacken ist spezifischer als bei Massen-Angriffen.

Beispiel:
Massen-Phishing: „Lieber Kunde, …..“
Speerwurf-Phishing: „Lieber Herr xy,…“
BEC-Phishing: Adressat ist der Chef mit seiner korrekten Adresse

Leider ist es in der Realität nicht so einfach wie im obigen Fall, denn die Kriminellen sind sehr gut vorbereitet und bei ihren Angriffen äußerst geschickt. Sie kennen sich erschreckend gut aus mit den Jobtiteln, beliebten Mittagspausentreffs, dem Freundeskreis, Historie der Vorgesetzten und möglicherweise sogar dem Lieferanten von Büromaterial und Kaffeebohnen. Und je mehr die Betrüger über den Betriebsalltag erfahren, desto gezielter setzen sie diese Informationen für ihre täuschend echten Konversationen ein. Die Anzahl der Phishing-Angriffe auf das Unternehmen wird daher stetig zunehmen. Bereits jetzt werden nach Sophos Labs 30 Prozent von Phishing-Emails geöffnet.

Doch woher kommen diese detaillierten Informationen?

- Vorherige erfolgreiche Angriffe, wie Datenklau-Schadsoftware
- Private Unternehmens-Dokumente, wie Telefondurchwahlen, oder Organigramme, aufzufinden via Suchmaschinen
- Soziale Netzwerk-Seiten von Mitarbeitern und Unternehmen
- Verärgerte Ex-Mitarbeiter
- Daten, die von anderen Betrügern im Dark Web gekauft wurden
- Plus unzählige weitere Möglichkeiten, an geheime Informationen zu gelangen

Was kann man gegen Phishing tun?

Phishing-Angriffe treten in allen Größen und Formen auf, und wie immer existiert kein Allheilmittel. Aus den gesammelten Labs-Erkenntnissen und -Erfahrungen empfiehlt sich aber eine duale präventive Verteidigungsstrategie:

1. Geschulte Mitarbeiter
   Durchschnittlich 16 Minuten dauert es, bis jemand auf eine Phishing-Email klickt (Verizon 2018 Data Breach Investigation Report). Mit einem individuellen oder Tool-basierten Simulations und Trainings Programm lernen Mitarbeit typische Fallen kennen und werden im sicheren Umgang geschult.

2. Fortschrittliche Sicherheitstechnologie
   Pre-Delivery: 58 Prozent der Emails ist Spam, 77 Prozent des Spams trägt schadhafte Daten in sich. Das sichere Email-Gateway ist eine elementare Maßnahme, um Phishing erst gar nicht hereinzulassen.
   Post-Delivery greift als letzte Verteidigungslinie, wenn die obigen präventiven Schutzmaßnahmen nicht funktionierten: Ist das System durch einen schadhaften Klick infiziert, begrenzt eine Endpoint-Sicherheitslösung inklusive Deep Learning, Anti-Exploit und Anti-Ransomware den Schaden.

„Die Kombination von hoch modernen technischen Abwehr- und Erkennungs-Maßnahmen und dem sensibilisierten Mitarbeiter, der mit Hilfestellung und einem einfach zu handhabenden Leitfaden die Situationen schnell und individuell entscheiden kann, nützt sowohl dem Schutz des Unternehmens als auch den ungestörten Arbeitsabläufen“, erklärt Michael Veit, Security Experte bei Sophos.

Über Sophos

Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos‘ Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.
Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. 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 +49-172-4536839
sophos@tc-communications.de