Sophos X-Ops nimmt Quishing unter die Lupe

Cybercrime-Trend im Aufwind: Phishing mit QR-Codes

In Anlehnung an Albert Einstein ließe sich wohl sagen, dass der kriminelle Einfallsreichtum der Menschen unendlich ist. Der neueste Trend Quishing beweist jedenfalls einmal wieder, dass die Cyberkriminellen keine Möglichkeit auslassen. Die Experten von Sophos X-Ops haben sich den neuesten Hype der Infiltration über QR-Codes genauer angesehen.

Wenn Cyberkriminelle ihre Phishing-Methoden mit eigentlich ganz harmlosen QR-Codes kombinieren, ist von „Quishing“ die Rede. Mittlerweile ist diese neue Taktik so populär geworden, dass es schon ganze Kampagnen dazu gibt.

Die Analysten von Sophos X-Ops haben gerade einen Coup aufgedeckt, bei dem ein Sophos-Mitarbeiter ein PDF-Dokument mit einem QR-Code als E-Mail-Anhang erhielt. Dieser QR-Code war ein Phishing-Köder, um Zugang zu den Anmeldeinformationen des Nutzers inklusive des MFA-Tokens (Multi-Faktor-Authentifizierung) zu ergaunern. Die Sophos-Experten waren in der Lage, die Angreifer daran zu hindern, Zugang zu jeglichen internen Anwendungen zu erhalten – doch andere Unternehmen hatten vielleicht weniger Glück, den Angriff zu erkennen und abzuwehren.

Seit Juni 2024 haben die Spezialisten von Sophos eine wachsende Anzahl dieser Quishing-E-Mails registriert, mit stetig ausgefeilteren Grafiken und gefälschtem Docusign-Branding. Es erscheint, dass die Angreifer Vorteile von „Quishing as a Service“ nutzen und sich eine bekannte Phishing-as-a-service-Plattform zu eigen machen.

Andrew Brandt, Principal Threat Researcher bei Sophos, ordnet die Situation so ein: „Als die QR-Codes während der COVID-Pandemie populärer wurden, war man zwar besorgt, das Risiko für die meisten Menschen blieb jedoch eher gering. Jetzt sehen wir, wie Angreifer die QR-Codes für gezielte Phishing-Attacken sehr effektiv nutzen. QR-Codes sind ungemein flexibel und mit Quishing-Bausätzen können die Kriminellen ganze Serien von gezielten Quishing-Massen-E-Mails entwickeln. Und wenn es den Angreifern gelingt, sowohl das Login als auch die Multifaktorauthentifikation eines Mitarbeiters zu stehlen, haben sie sich in vielen Fällen Zugang zu hoch privilegierten Bereichen verschafft.“

Selbst unter besten Bedingungen und mit gut geschulten Mitarbeitern ist Phishing beziehungsweise Quishing eine zunehmend gefährliche Bedrohung. Mit einem mehrschichtigen Schutz ist es heute allerdings möglich, einen erfolgreichen Phishing-Angriff zu entschärfen. Genauso wichtig ist aber auch eine Unternehmenskultur, in der die Mitarbeiter ermutigt werden, verdächtige Aktivitäten umgehend zu melden. Das schnelle Eingreifen kann den Unterschied zwischen einem bloßen Phishing-Versuch und einem erfolgreichen Angriff ausmachen.

Wie genau Quishing-Attacken funktionieren und weshalb sie eine zunehmende Gefahr darstellen, wird in diesem Artikel ausgeführt:
https://news.sophos.com/en-us/2024/10/16/attackers-leverage-qr-codes-in-pdf-email-attachments-for-phishing-on-mobile-devices/

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, Senior PR-Manager EMEA Central
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