ALTHAMMER & KILL

Leitfaden

Zur Verhinderung von Phishing-Attacken und CEO-Fraud

Im Homeoffice unterliegen Sie einer erhöhten Gefahr, Opfer von Phishing-Attacken und ähnlichem zu werden. Sie arbeiten möglicherweise mit Ihren privaten Geräten (BYOD) und haben nicht dieselbe IT-Sicherheitsstruktur, wie Sie sie im Unternehmen vorfinden würden. Wir möchten mit diesem Kurzpapier praxisnah die Gefahren von möglichen Phishing-Attacken und CEO-Fraud kurz beschreiben.

Phishing

Phishing bezeichnet das Abfangen von Daten in der Absicht, sie missbräuchlich zu nutzen. Phishing findet im Alltag in unterschiedlichen Facetten statt. Wir betrachten an dieser Stelle leidglich die typischste Art und Weise, welche einem Nutzer von internetfähigen Endgeräten begegnen kann.
Das klassische Beispiel ist eine im Browser dargestellte Webseite, welche bei Ihnen den Anschein von Echtheit erweckt und Sie dazu auffordert, z.B. Ihre Zugangsdaten einzugeben. Auf eine solche Seite werden Sie typischerweise durch einen Link in einer nicht vertrauenswürdigen E-Mail geleitet.
Allerdings besteht aber auch immer die Gefahr, dass Sie einen solchen Link von einer Ihnen eigentlich bekannten und als vertrauenswürdig eingestuften E-Mail-Absenderadresse erhalten. Falls nämlich dieser Absender die Zugangsdaten für sein E-Mail-Postfach hat „phishen" lassen, werden über dieses Postfach oftmals an alle im Adressbuch befindlichen und sonstigen E-Mail-Adressen Nachrichten mit einem Link verschickt, um weitere Opfer zu generieren. Auf diese Weise kann natürlich auch leicht andere Malware auf Ihrem Endgerät installiert werden.
Auch wenn es trivial klingt: Öffnen sie keine Links in E-Mails Ihnen unbekannter Herkunft. Achten Sie auch bei Ihnen bekannten E-Mail-Adressen auf Ungewöhnlichkeiten – z.B. würde Ihnen Ihr Chef wahrscheinlich keine kurze Nachricht mit „Schau dir mal das an." schreiben. Achten Sie auf die Sprache – sind ungewöhnliche Rechtschreibfehler enthalten? Nutzt das Gegenüber plötzlich das „Sie", obwohl Sie sich sonst immer duzen?
Kein seriöser Anbieter wird Zugangsdaten von Ihnen per E-Mail abfragen. Insbesondere Microsoft wird Sie nicht per E-Mail kontaktieren, um beispielsweise Ihr Postfach zu verifizieren. Nutzen Sie keine Links aus E-Mails, die Sie zu scheinbar echten Seiten führen und Ihre Zugangsdaten abfragen. Vielmehr rufen Sie Webseiten, auf denen Sie sich üblicherweise einloggen, immer direkt über Ihren Browser auf.

CEO-Fraud

CEO-Fraud zielt darauf ab, typischerweise die Buchhaltung zu einer unberechtigten Überweisung zu verleiten. Dieses kann per Telefon passieren – in großen Unternehmen sind sich beispielsweise Geschäftsführung und Buchhaltung nicht unbedingt persönlich bekannt¬ ¬– oder eben per E-Mail. Hierbei geht gerne ein Phishing-Angriff voraus, um dann folgend über den Account eines Geschäftsführenden eine Konversation mit der Buchhaltung zu beginnen. Hierbei werden dann Regeln innerhalb des Accounts angelegt, so dass der Account-Inhaber nichts von der Konversation mitbekommt. Achten Sie wieder auf Ungewöhnlichkeiten innerhalb der Nachrichten. Dies können sprachliche Fehler sein, eine alte Signatur und vor allem ein ungewöhnliches Überweisungsziel. Halten Sie unbedingt Rücksprache, falls Ihnen etwas komisch vorkommt und lassen Sie sich nicht unter Druck setzen.