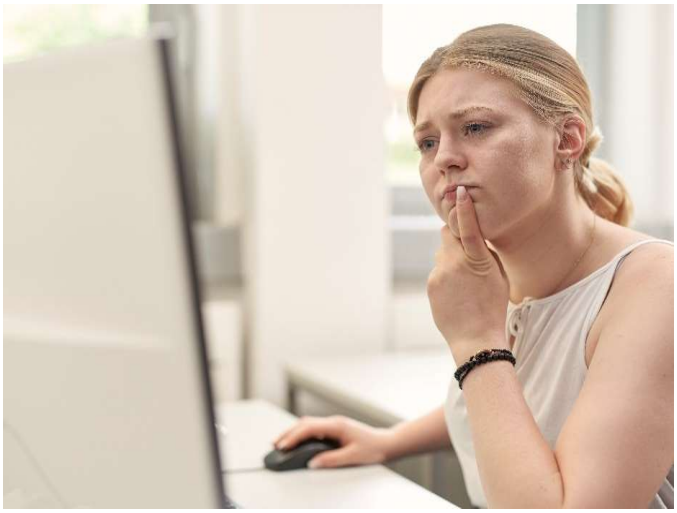
Phishing-Kampagnen und ihre Fallstricke

Forscherinnen des Karlsruher Instituts für Technologie und der Ruhr-Universität Bochum analysieren die Wirkung vorgetäuschter Phishing-Mails zur Sensibilisierung von Angestellten



Öffnen oder nicht? Die Absender von Phishing-Mails geben sich oft als bekannte Dienstleister oder Kollegen aus. (Foto: Amadeus Bramsiepe, KIT)

Gefälschte E-Mails sind der meistgenutzte Weg von Cyberkriminellen, um sich vertrauliche Daten zu erschleichen oder Schadprogramme einzuschleusen. Manche Unternehmen versuchen, die Resistenz ihrer Mitarbeitenden gegen solche Angriffe mit Hilfe von Phishing-Kampagnen zu prüfen und vermeintlich zu verbessern. Dabei werden den Angestellten bewusst simulierte Phishing-Mails geschickt. Der Bericht der Wissenschaftlerinnen des Karlsruher Instituts für Technologie (KIT) und der Ruhr Universität Bochum beleuchtet Phishing-Kampagnen unter den Aspekten „Security, Recht und Faktor Mensch“.

Sie geben sich den Anschein von Glaubwürdigkeit: gefälschte E-Mails, deren Absender sich als bekannte Dienstleister, Kollegen oder Vorgesetzte ausgeben. Ihr Ziel: arglose Empfängerinnen und Empfänger dazu zu verleiten, auf einen Link zu klicken, um in der Folge Kontodaten und Passwörter abzufischen oder Schadprogramme aufzuspielen. Es genügt, dass ein einzelner Angestellter einem Phishing-Angriff Glauben schenkt, um großen

Monika Landgraf
Leiterin Gesamtkommunikation
Pressesprecherin

Kaiserstraße 12
76131 Karlsruhe
Tel.: +49 721 608-21105
E-Mail: presse@kit.edu

Weiterer Pressekontakt:

Carola Mensch
Redakteurin/Pressereferentin
Tel: +49 721 608-21170
E-Mail: carola.mensch@kit.edu

Weitere Materialien:

Zum Bericht:
https://publikationen.bibliothek.kit.edu/1000119662

Schaden zu verursachen. Um zu testen, wie ihre Mitarbeiterinnen und Mitarbeiter auf Phishing-Mails reagieren, nutzen manche Firmen und Institutionen Phishing-Kampagnen externer Dienstleister. Mit Wissen der Unternehmensleitung werden fingierte Phishing-Mails an die Angestellten geschickt.

„Die Kampagnen haben das Ziel, Mitarbeiterinnen und Mitarbeiter bewusst zu täuschen, um sie vor realen Gefahren zu schützen und ein Problembewusstsein zu schaffen, aber es herrschen oft Unsicherheiten darüber, was rechtlich, sicherheitstechnisch und ethisch vertretbar ist“, so die Wissenschaftlerinnen. Diese drei Aspekte beleuchten die beiden Professorinnen Melanie Volkamer, Leiterin der Forschungsgruppe SECUSO – Security, Usability and Society am KIT, und Franziska Boehm vom Zentrum für Angewandte Rechtswissenschaft des KIT gemeinsam mit der Bochumer Professorin für Human-Centred Security am Horst-Görtz-Institut für IT Sicherheit, M. Angela Sasse. Ihr online frei zugänglicher Forschungsbericht beschreibt verschiedene Gestaltungsformen und -ziele von Phishing-Kampagnen und damit verbundene Fragen im Kontext von IT- und Informationssicherheit, Fragen zum Arbeitnehmer- und Datenschutz sowie Fragen der Vertrauenskultur und der Selbstwirksamkeit von Angestellten. Er nimmt die Aussagekraft und Fallstricke der Kampagnen in den Blick und bietet Information unter anderem für IT- und Informationssicherheitsbeauftragte.

„Phishing-Kampagnen bringen eine Reihe von Sicherheitsproblemen mit sich, und sie beeinflussen die Vertrauens- und Fehlerkultur in einem Unternehmen stark; auch rechtlich ist einiges zu berücksichtigen“, sagt Boehm, die neben ihrer Professur am KIT auch Bereichsleiterin für Immaterialgüterrechte in verteilten Informationsinfrastrukturen (IGR) am FIZ Karlsruhe – Leibniz-Institut für Informationsinfrastruktur ist. „Eine Kampagne zu starten ohne die Angestellten vorher darüber aufzuklären, ist schlicht unfair und trägt nicht zum Vertrauen in die Leitung bei“, sagt Sasse, die am Exzellenzcluster Cyber-Sicherheit im Zeitalter großskaliger Angreifer, kurz CASA, forscht und Abschlüsse in Arbeitspsychologie und Informatik hat. Zu erfahren, dass man auf Phishing-Nachrichten hereingefallen ist, wirke sich schlecht auf die Selbstwirksamkeit aus: „Die Angestellten merken, dass sie keine Kontrolle über die Situation haben und reagieren mit Resignation, sie bemühen sich nicht einmal mehr, Phishing-Nachrichten zu erkennen“, stellen die Autorinnen fest.

„Wenn die Mitarbeiter aber wissen, dass die Kampagne läuft, sind sie vielleicht neugierig und klicken eine Mail an, in der Annahme, da kann nichts passieren, die Mail ist ja fingiert. Da aber weiterhin echte Phishing-Mails im Umlauf sind, wird das Schutzniveau herabgesetzt“,

sagt Volkamer, die am Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL) Karlsruhe forscht, einem von deutschlandweit drei Kompetenzzentren für Cybersicherheit. Verstärkt wird das Problem, wenn ein Mitarbeiter merkt, dass er doch einen gefährlichen Link angeklickt hat und sich nicht traut, dies zu melden. Im Unternehmen sollte deshalb vor Start einer Phishing-Kampagne bereits eine Meldepflicht von IT-Sicherheitsvorfällen etabliert sein, betont die Informatikerin.

Bei einer angekündigten Kampagne sei zu erwarten, dass die Mitarbeitenden weitaus mehr Nachrichten kritisch hinterfragen und übervorsichtig sind, dadurch könne sich der Zeit- und Leistungsdruck erhöhen, was sich ebenfalls negativ auf das Vertrauen in die Geschäftsleitung auswirke. „Security wird meist ohnehin als lästig und störend empfunden, aus unserer Sicht ist es ein großes Problem von Phishing-Kampagnen, dass sie das Thema noch negativer belegen, denn letztlich greift dabei die Leitung ihre Angestellten an“, sagt Sasse. Die Autorinnen raten Unternehmen, die ihre IT-Sicherheit stärken wollen, Zeit und Geld in erster Linie in eine Verbesserung der technischen Sicherheitsmaßnahmen zu investieren und erst dann die Angestellten zu schulen, welche Phishing-Nachrichten sie trotz der aktuellsten Sicherheitssoftware und des neuesten Betriebssystems noch erreichen können und wie sie diese erkennen.

Originalpublikation:

Melanie Volkamer (KIT, SECUSO, KASTEL), M. Angela Sasse (RUB, CASA), Franziska Boehm (KIT, FIZ): Phishing-Kampagnen zur Mitarbeiter-Awareness. Analyse aus verschiedenen Blickwinkeln: Security, Recht und Faktor Mensch.

https://publikationen.bibliothek.kit.edu/1000119662

Erhalt unserer natürlichen Lebensgrundlagen. Das KIT ist eine der deutschen Exzellenzuniversitäten.

Diese Presseinformation ist im Internet abrufbar unter: www.sek.kit.edu/presse.php

Das Foto steht in der höchsten uns vorliegenden Qualität auf www.kit.edu zum Download bereit und kann angefordert werden unter: presse@kit.edu oder +49 721 608-21105. Die Verwendung des Bildes ist ausschließlich in dem oben genannten Zusammenhang gestattet.