ALARM
Awareness Labor KMU Informationssicherheit

INFOBLATT – Security kompakt zum Thema CEO Fraud

für Endanwender:innen

Thinking Objects GmbH

Stand: Mai 2023

IT-Sicherheit
IN DER WIRTSCHAFT

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Das vorliegende **INFOBLATT – Security kompakt für KMU** ist eines von insgesamt sieben Sicherheitskonzepten, die im dreijährigen Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“ der Technischen Hochschule (TH) Wildau verfasst werden.

Das Projekt „ALARM Informationssicherheit“ wird vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) gefördert.

Projektlaufzeit

01.10.2020 – 30.09.2023

Das INFOBLATT – Security kompakt für KMU basiert auf Ergebnissen der im Projekt „ALARM Informationssicherheit“ durch den Unterauftragnehmer Thinking Objects (TO) GmbH in Pilotunternehmen durchgeführten „Vor-Ort-Angriffen“.

Das diesem Sicherheitskonzept zugrundeliegende Vorhaben wird mit Mitteln des Bundesministeriums für Wirtschaft und Klimaschutz unter dem Förderkennzeichen 01MS19002A gefördert.

Das Mittelstand-Digital Netzwerk bietet mit den *Mittelstand-Digital Zentren*, der Initiative *IT-Sicherheit in der Wirtschaft* und *Digital Jetzt* umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit. Weitere Informationen finden Sie unter www.it-sicherheit-in-der-wirtschaft.de.

Inhaltsverzeichnis

1 Einleitung

Cyberangriffe gehen uns alle an und auch Sie können einen wichtigen Beitrag dazu leisten, dass Ihr Arbeitgeber, Ihr Unternehmen oder Sie persönlich nicht Opfer eines Cyberangriffs werden.

Alles, was Sie dazu wissen müssen, finden Sie kurz und kompakt in diesem Infoblatt.

2 WAS bedeutet CEO-Fraud?

CEO-Betrug, auch bekannt als CEO-Fraud oder Business E-Mail Compromise (BEC), ist eine Form des Betrugs, bei dem Angreifende versuchen, sich als CEO oder andere hochrangige Führungskräfte eines Unternehmens auszugeben, um Geld oder vertrauliche Informationen zu stehlen.

Der Angreifer sendet eine gefälschte E-Mail an eine Person des Unternehmens, meistens an jemanden in der Finanzabteilung oder Buchhaltung. Die E-Mail sieht so aus, als käme sie von einem CEO oder einer anderen Führungsperson und fordert die Person auf, eine finanzielle Transaktion durchzuführen. Der Grund für die Transaktion wird oft als dringlich oder geheim dargestellt, um den Mitarbeiter unter Druck zu setzen.

Die gefälschten E-Mails sind oft sehr überzeugend gestaltet und können offiziell aussehen, indem sie das Unternehmenslogo, die Sprache und den Schreibstil der tatsächlichen Führungskräfte imitieren.

2.1 WARUM sollten Sie sich mit der Angriffsmethode auskennen?

Es ist wichtig, sich mit CEO-Fraud vertraut zu machen, um die eigene Sicherheit und die Sicherheit der Organisation zu gewährleisten. Indem Sie sich über diese Betrugsmethode informieren, können Sie Risiken minimieren, Betrugsversuche erkennen und geeignete Maßnahmen zum Schutz ergreifen.

- **Erhöhte Sicherheit:** Wenn Sie die Taktiken und Methoden von CEO-Fraud verstehen, sind Sie besser darauf vorbereitet, potenzielle Betrugsversuche zu erkennen und entsprechende Sicherheitsvorkehrungen zu treffen.

- **Schutz Ihrer Organisation:** Als MitarbeiterIn oder Führungskraft können Sie dazu beitragen, Ihre Organisation vor CEO-Fraud zu schützen, indem Sie das Bewusstsein und das Wissen darüber in Ihrem Team oder Unternehmen fördern. Je mehr Menschen über diese Betrugsmethode Bescheid wissen, desto besser können potenzielle Angriffe erkannt und gemeldet werden, bevor es zu finanziellen Schäden kommt.

- **Frühzeitige Erkennung:** CEO-Fraud kann oft sehr raffiniert und überzeugend sein. Indem Sie sich mit den gängigen Betrugstaktiken vertraut machen, können Sie verdächtige E-Mails oder Anfragen erkennen und angemessen darauf reagieren. Eine frühzeitige Erkennung ermöglicht es Ihnen, Betrugsversuche zu stoppen, bevor Schaden angerichtet wird.

2.2 WIE können Sie sich schützen?

- **Überprüfen von E-Mails:** Achten Sie genau auf die Details von E-Mails, insbesondere wenn es um finanzielle Transaktionen oder vertrauliche Informationen geht. Überprüfen Sie die E-Mail-Adresse des Absenders sorgfältig, um sicherzustellen, dass sie der tatsächlichen Adresse des CEOs oder der Führungskraft entspricht. Seien Sie vorsichtig bei E-Mails, die Druck auf Sie ausüben, Geheimhaltung verlangen oder ungewöhnliche Anfragen stellen.

- **Authentifizierungsmethoden nutzen:** Implementieren Sie Authentifizierungsmethoden wie Zwei-Faktor-Authentifizierung (2FA) für E-Mail-Konten und andere sensible Systeme. Dadurch wird die Wahrscheinlichkeit verringert, dass Betrüger Zugriff auf die Konten von Führungskräften erhalten.

- **Vertraulichkeit und Sicherheit:** Behandeln Sie vertrauliche Informationen mit Vorsicht. Geben Sie niemals sensible Daten oder Unternehmensgeheimnisse aufgrund einer einfachen E-Mail-Anfrage preis. Überprüfen Sie die Anfrage mit anderen verifizierten Kanälen wie persönlichen Treffen oder Telefonanrufen.

- **Interne Überprüfung:** Implementieren Sie interne Überprüfungsprozesse für finanzielle Transaktionen. Stellen Sie sicher, dass zwei Personen unabhängig voneinander eine Transaktion überprüfen, insbesondere wenn es um große Geldbeträge geht. Kommunizieren Sie diese Richtlinien und stellen Sie sicher, dass sie von allen im Unternehmen befolgt werden.

- **Kontakte verifizieren:** Bestätigen Sie finanzielle Anfragen oder Transaktionen persönlich oder telefonisch bei der angeblichen Führungskraft, bevor Sie Maßnahmen ergreifen. Verwenden Sie dabei jedoch keine Kontaktdaten aus der verdächtigen E-Mail, sondern verwenden Sie bereits bekannte und verifizierte Kontaktdaten.

3 FEHLERKULTUR – Doch geklickt und was dann…

Fehler passieren uns allen!

Wenn eine Person auf die gefälschte E-Mail hereinfällt, führt sie die angeforderte Transaktion durch, ohne zu bemerken, dass es sich um einen Betrug handelt. Das Geld wird dann normalerweise auf ein Konto transferiert, das von den Betrügern kontrolliert wird. In einigen Fällen werden auch vertrauliche Informationen wie Unternehmensgeheimnisse oder Mitarbeiterdaten gestohlen.

LINKS zu weiteren Infos: https://alarm.wildau.biz/#learningScenarios

Technische Hochschule Wildau
Technical University of Applied Sciences

Thinking Objects

Thinking Objects GmbH
Lilienthalstraße 2/1
70825 Korntal-Münchingen

Tel. +49 711 88770400
Fax. +49 711 88770449
www.to.com