ALARM
Awareness Labor KMU Informationssicherheit

Niederschwelliges Sicherheitskonzept zum Thema CEO Fraud

für Geschäftsführung und IT-Verantwortliche

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 **niederschwellige Sicherheitskonzept 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 niederschwellige Sicherheitskonzept 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

CEO Fraud ist eine Betrugsmasche, bei der die Beschäftigten von Unternehmen unter Verwendung gefälschter Identitäten dazu veranlasst werden, Geldbeträge an Kriminelle zu überweisen. Für diese Angriffsform hat sich mittlerweile neben dem Begriff „CEO Fraud“ auch die Bezeichnung Business E-Mail Compromise (BEC) etabliert.

In der Regel werden die Angriffe über eine Phishing-Mail gestartet, mittlerweile aber auch im Rahmen von Telefonanrufen oder Messenger-Calls.

Die zugrundeliegende Geschichte ist nahezu immer die, dass sich ein vermeintliches Mitglied der Geschäftsleitung meldet und Hilfe bei einer unangenehmen Lage benötigt. Natürlich möchte man als Mitarbeiter oder Mitarbeiterin hier gerne helfen. Bei einem Unternehmen mit mehreren Hierarchieebenen muss nicht unbedingt jemand aus der Geschäftsführung imitiert werden, es können auch Leitungsfunktionen, wie beispielsweise Leitung Buchhaltung, oder vergleichbare Positionen genutzt werden.

2 Identitäten und Passwörter

Die Anzahl der technischen **Schutzmaßnahmen im Umfeld des CEO Fraud sind begrenzt**, hier entfalten organisatorische Maßnahmen eine deutlich höhere Wirksamkeit.

2.1 Technische Schutzmaßnahmen

Die technischen Schutzmaßnahmen beschränken sich in der Regel auf **E-Mail-Filter**. Dieser verhindert bei korrektem Einsatz die Zustellung von E-Mails mit gefälschten Absendern.

Da E-Mails mit dem Ziel, eine Anweisung der Geschäftsführung vorzutäuschen, in der Regel keine Viren oder Malware enthalten, ist es möglich, dass diese Mails nicht blockiert werden.

Sollten sich die Kriminellen Zugriff zu einem Postfach der Geschäftsleitung verschafft haben, greifen technische Schutzmaßnahmen faktisch gar nicht und es können noch authentischere E-Mails verfasst oder echte E-Mails mit alten Zahlungsaufträgen kopiert und genutzt werden.

2.2 Organisatorische Schutzmaßnahmen

Um einen CEO Fraud vorzubereiten, benötigen die Angreifer Informationen über das Unternehmen. **Bestimmte Informationen über die Geschäftsführung sind öffentlich verfügbar**, andere Informationen beispielsweise über die Leitung der Buchhaltung lassen sich über fingierte Anrufe oder Business-Netzwerke herausfinden.

Der eigentliche Betrug läuft häufig wie folgt ab: Eine gefälschte E-Mail im Namen der Geschäftsführung oder Führungskraft landet im Postfach, mit der dringenden Bitte oder Anweisung, eine Überweisung durchzuführen. Als Vorwand wird eine vermeintliche Notlage oder eine vertrauliche Angelegenheit genutzt, um Druck aufzubauen und eine schnelle Reaktion hervorzurufen. Fällt die angeschriebene Person auf den Betrug herein und tätigt die Überweisung, ist es aufgrund der oft im Ausland befindlichen Zielkonten schwierig bis unmöglich, die Zahlung zu stornieren oder zurückzuverfolgen.

Um sich vor CEO Fraud zu schützen, sollten Unternehmen ihre Beschäftigten regelmäßig über diese Betrugsmasche informieren.

Zudem müssen klare Verfahren für die Überprüfung von Anfragen und die Genehmigung von Zahlungen oder Transaktionen vorliegen. Auch sollte vorab über mögliche Ausnahmesituationen gesprochen werden, und ob hierfür spezielle Prozeduren festgelegt werden, beispielsweise telefonische Rückversicherung.

Im Normalfall sind es die Details in solchen Mails, die die Betrüger entlarven. Wird wie gewohnt „Du“ oder „Sie“ verwendet, sind Schreibstil und Formulierungen unüblich? Die Geschichte ist üblicherweise so aufgebaut, dass es ganz dringend zu vermeiden ist, mit anderen Kolleginnen und Kollegen darüber Kontakt aufzunehmen.

Die Kreativität der Betrüger ist grundsätzlich hoch. In der Urlaubszeit werden E-Mails über öffentliche Maildienste, wie z.B. GMX oder GMAIL, verschickt und darin erklärt, dass es sich um das private E-Mailkonto handelt, da man sich im Urlaub befindet und der Zugang zur Firmenadresse gerade nicht möglich ist. In weniger dramatischen Fällen werden kurzfristig Gutschein-Codes von Internet-Shops für den fast vergessenen Geburtstag des Patenkindes abgefragt.

Varianten dieser Betrugsmasche sind auch Telefonanrufe oder Voice-Calls. In beiden Fällen können gefälschte Rufnummern oder Messenger-Accounts den Namen der Führungskraft anzeigen. Die Betrüger hoffen, dass die persönliche Bekanntschaft der Betroffenen nicht so tiefgehend ist, dass man Stimme und Sprache nicht als Fälschung oder KI-Simuliert nachvollziehen kann. Auch hier gilt wieder: Eine Rückversicherung über einen unabhängigen bekannten Kanal ist notwendig, um sicher zu sein, dass kein Betrüger am Werk ist.

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