ALARM
Awareness Labor KMU
Informationssicherheit

INFOBLATT – Security kompakt zum Thema Phishing

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 PHISHING/SMISHING 3

1.1 WAS bedeutet Phishing/Smishing? 3

1.2 WARUM sollten Sie sich mit der Angriffsmethode auskennen? 3

1.3 WIE können Sie sich schützen? 3

2 FEHLERKULTUR – Doch geklickt und was dann... 4

1 PHISHING/SMISHING

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.

1.1 WAS bedeutet Phishing/Smishing?

PHISHING ist ein Kunstwort, das sich aus den englischen Begriffen **„password“** und **„fishing“** zusammensetzt und so viel bedeutet wie **„Fischen nach Passwörtern“**.

SMISHING beschreibt ein Phishing-Angriff per SMS.

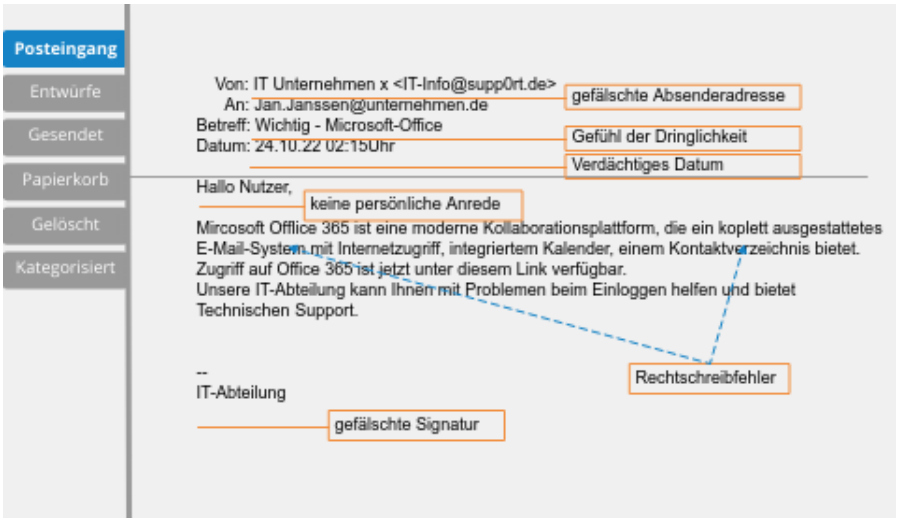
Quelle: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Ver- braucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam- Phishing-Co/Passwortdiebstahl-durch-Phishing/passwortdiebstahl-durch-phi- shing_node.html (19.05.23)

1.2 WARUM sollten Sie sich mit der Angriffsmethode auskennen?

Phishing-E-Mails und Smishing-SMS zählen zu den Haupteinfallstoren von Cyberattacken und können sehr hohe wirtschaftliche und betriebliche Schäden verursachen. Angreifer haben es auf unsere Zugangsdaten zum Unternehmensnetzwerk abgesehen. Deshalb versuchen sie uns Menschen vor den Bildschirmen zu verleiten, auf Links zu klicken oder auf Fake-Webseiten die persönlichen Zugangsdaten einzugeben. Gelingt der Zugriff auf das Unternehmensnetzwerk, können Hacker unbemerkt Systeme lahmlegen oder wichtige Daten stehlen.

1.3 WIE können Sie sich schützen?

Häufige Merkmale einer Phishing-E-Mail



- Achten Sie auf Abweichungen zwischen dem vermeintlichen Absender und der verwendeten E-Mail-Adresse.
- Cyberkriminelle setzen oft auf den Dringlichkeitsfaktor und versuchen so, Handlungsdruck bei der Empfängergruppe aufzubauen.
- Achten Sie auf das Datum und die Uhrzeit.
- Oft wird keine persönliche Anrede genutzt. In offiziellen E-Mails werden Sie grundsätzlich mit Ihrem Namen angesprochen.
- Falsche Rechtschreibung und Grammatik sind häufig ein Indiz für gefälschte Mails.
- Achten Sie auf die Signatur. Oftmals entspricht diese nicht den Signaturvorgaben im Unternehmen.

2 FEHLERKULTUR – Doch geklickt und was dann…

Fehler passieren uns allen!

Bitte informieren Sie umgehend ihren IT-Support und ziehen Sie den Stecker bzw. trennen Sie das Gerät vom Netzwerk. Wenn Sie als Privatperson betroffen sind, dann trennen Sie ihr Gerät ebenfalls von Netzwerk und Internet. Die folgende Checkliste vom BSI zeigt ihnen konkrete Handlungsschritte auf:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/BSI-_ProPK-Checkliste-Phishing.pdf?blob=publicationFile&v=1 (19.05.23)

Weitere Informationen erhalten Sie auch in unseren digitalen Lernszenarios:

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