ALARM
Awareness Labor KMU
Informationssicherheit

INFOBLATT – Security kompakt zum Thema Smishing

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 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 Cyber- angriffs werden.

Alles, was sie zum Thema Smishing wissen müssen, finden Sie kurz und kompakt in diesem Infoblatt.

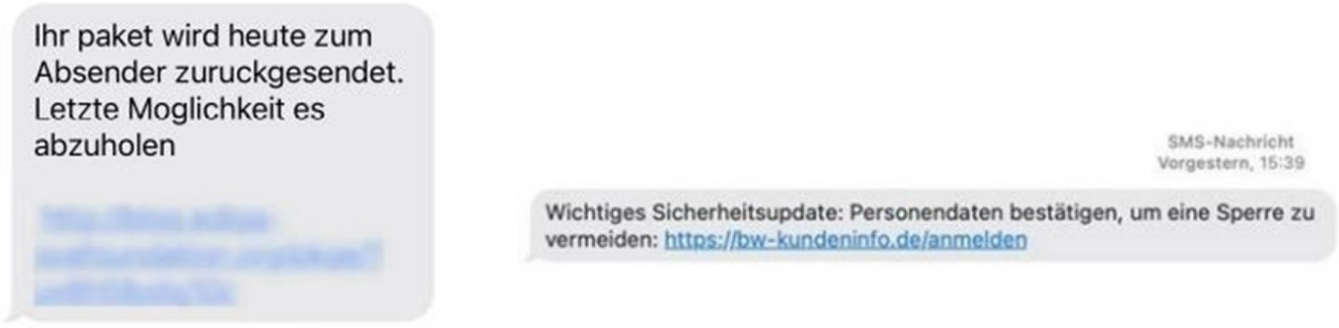
1.1 WAS bedeutet Phishing/Smishing?

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/Service-Navi/Presse/Alle-Meldungen- News/Meldungen/Smishing_SMS-Phishing_141021.html (19.05.23)

Beispiele:



1.2 WARUM sollten Sie sich mit der Angriffsmethode Smishing auskennen?

Smishing-SMS zählen neben Phishing-Angriffen per E-Mail zu den Haupteinfallstoren von Cyberattacken und können sehr hohe wirtschaftliche und betriebliche Schäden verursachen. Die Angreifer haben es darauf abgesehen, dass wir Menschen vor den Bildschirmen sie über das Klicken auf Links oder durch die Eingabe von persönlichen Zugangsdaten auf Fake-Webseiten in unser Unternehmensnetzwerk lassen. Wenn der Zugriff auf das Unternehmensnetzwerk gelingt, sind sie für uns unsichtbar und können alles lahmlegen oder unbemerkt wichtige Daten stehlen.

- Achten Sie auf Abweichungen zwischen dem vermeintlichen Absender und der verwendeten E-Mail-Adresse.
- Klicken Sie nicht auf enthaltene Links.
- Laden Sie keine Dateien aus unbekannter Quelle herunter.
- Löschen Sie die verdächtige SMS-Nachricht unverzüglich.

Quelle: https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Mel- dungen/Smishing_SMS-Phishing_141021.html (19.05.23)

2 FEHLERKULTUR – Doch geklickt und was dann…

Fehler passieren allen von uns!

Wenn das Diensthandy betroffen ist:

- Flugmodus aktivieren, um das Gerät vom Netz zu nehmen
- Informieren Sie Ihre IT-Abteilung

Wenn das private Handy betroffen ist:

- Flugmodus aktivieren, um das Gerät vom Netz zu nehmen
- Informieren Sie Ihren Mobilfunkprovider
- Erstatten Sie Strafanzeige bei der örtlichen Polizeidienst- stelle. Nehmen Sie dazu Ihr Smartphone zur Beweissicherung mit
- Setzen Sie Ihr Smartphone auf Werkseinstellungen zu- rück (nachdem Sie Anzeige erstattet haben). Sichern Sie vorher alle wichtigen Daten wie Fotos, Dokumente usw. lokal (zum Beispiel über eine USB-Verbindung). Mit dem Zurücksetzen auf die Werkseinstellungen gehen alle gespeicherten und installierten Daten verloren. Dieser Schritt ist allerdings notwendig, um die über die aktuel- len SMS-Spam-Nachrichten verteilten Android-Schadpro- gramme vollständig zu entfernen.

Quelle: BSI https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen- News/Meldungen/Smishing_SMS-Phishing_141021.html (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