ALARM
Awareness Labor KMU Informationssicherheit

Niederschwelliges Sicherheitskonzept zum Thema Smishing

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

Smishing beschreibt einen Phishing-Angriff per SMS. Angreifende versuchen hierbei auf unterschiedlichste Art und Weise Benutzerinnen und Benutzer eines Smartphones oder Computer-Systems in eine Falle zu locken, um ihnen ihr Kennwort zu entlocken oder sie zur Installation einer bösartigen Software zu verleiten.

Ziel der Angreifenden ist es, mit dieser gestohlenen Identität des Anwenders oder der Anwenderin weitere Aktionen durchzuführen, um sich selbst zu bereichern.

Der Eingangskanal für Smishing ist üblicherweise SMS, aber mittlerweile auch Messenger-Nachrichten wie beispielsweise WhatsApp.

Diese Kanäle sind im Gegensatz zu E-Mail auch im Unternehmensumfeld nicht mit besonderen Schutzmaßnahmen versehen. Auch hier ist die Notwendigkeit gegeben, weitere Sicherheitsmaßnahmen zu implementieren, um Angreifenden nach der Übernahme des Kontos die Durchführung des Beutezuges soweit es geht zu erschweren und sie oder ihn bei der Umgehung dieser Maßnahmen möglicherweise auch zu entdecken.

Für die privat genutzten Smartphones der Beschäftigten stellen Banking-Trojaner noch ein hohes Risiko dar. Hier geht es in der Regel darum, Zugriff auf Bankkonten zu erhalten und den TAN-Schutz für Überweisungen auszuhebeln.

2 Die Welt der Smartphones

Aus Sicht von Hackern und Hackerinnen sind Smartphones nichts anderes als kleine tragbare Computer, die einige spezielle Eigenschaften haben.

Es gibt praktisch keine technischen Maßnahmen für Smartphones, die vor gefälschten SMS oder Messenger Nachrichten schützen, ebenso wenig vor Spam. Auch der Zugriff auf unerwünschte URLs sind von den Unternehmens-Smartphones aus in der Regel nicht blockiert, von privaten Geräten ebenfalls nicht.

In vielen Fällen tarnen sich Smishing Nachrichten als Links von Paket-Dienstleistern mit dem Ziel, dass User auf ihrem Smartphone die entsprechende Fake-Seite öffnen. Dort werden entweder persönliche Daten oder Logins abgefragt, oder es wird versucht eine Malware oder einen Trojaner auf dem Smartphone zu installieren.

In manchen Bereichen werden auch heute noch einfache Mobiltelefone ohne Smartphone-Funktionalität eingesetzt. Die per SMS verschickten Links sind oftmals bewusst kurze Web-Adressen, um sie auch einfach auf dem PC eintippen zu können. Speziell im Bereich des Identitätsdiebstahls kann hier keinerlei Entwarnung gegeben werden, das Risiko in gefälschte Anmeldemasken Anmeldedaten einzugeben besteht hier ebenfalls.

2.1 Schutzmaßnahmen

Sofern das Gerät über eine Mobilfunkverbindung verfügt, befindet es sich damit in der Regel im Internet. Damit sollten alle notwendigen Funktionen möglich sein. Daher muss es auch vor Ort im Unternehmen nicht Teil des internen Netzwerkes sein. Ein WLAN, das lediglich Internetzugang zur Verfügung stellt, ist hier der passendere Weg. Damit kann ein infiziertes Smartphone nicht direkt im internen Netz als Zugang für Angriffe dienen.

2.2 Verwaltung der Smartphones

Die Unternehmensgeräte müssen zentral verwaltet und reguliert werden. Ein sogenanntes Mobile Device Management (MDM) hilft hierbei, zentrale Richtlinien durchzusetzen und beispielsweise den Stand des Betriebssystems zu kontrollieren. Auch können hierbei sogenannte Container-Systeme für verschiedene Schutzzonen auf dem Gerät sorgen. Manche Lösungen bieten einen abgesicherten Zugriff auf Unternehmens-E-Mails. Im Falle eines Verlustes eines Gerätes ist die Löschung aller Daten möglich.

2.3 Updates und Gerätetausch

Die Hersteller von Smartphones liefern über einen bestimmten Zeitraum hinweg Updates und Sicherheitsupdates für ihr Smartphone-Modelle. Diese sind umgehend einzuspielen.

Wenn es für ein Smartphone keine Updates mehr gibt, muss es zwingend ausgetauscht werden. Nicht geschlossene Sicherheitslücken sind der häufigste Weg für Schadsoftware, auf einem Smartphone Hintertüren einzurichten.

2.4 Im Falle eines Falles

Wenn man auf einen Link geklickt hat, sind zwei Angriffsszenarien verbreitet: Der Versuch Zugangsdaten zu stehlen, indem man eine nachgemachte Webseite präsentiert bekommt oder die Installation einer Malware auf dem Endgerät. In ersten Fall ist genau zu prüfen, wofür Zugangsdaten abgefragt werden und im Zweifelsfall keine Daten einzugeben.

Wenn man geklickt hat und bemerkt, es geschehen ungewöhnliche Dinge auf dem Gerät, ist der wichtigste Punkt, das System so schnell wie möglich vom Netz zu trennen. Dazu gibt es folgende Checkliste:

Wenn das **Geschäftshandy** betroffen ist:

- Flugmodus aktivieren, um das Gerät vom Netz zu nehmen
- Informieren Sie umgehend 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 Polizeidienststelle. Nehmen Sie dazu Ihr Smartphone zur Beweissicherung mit

Setzen Sie Ihr Smartphone auf Werkseinstellungen zurück (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 aktuellen SMS-Spam-Nachrichten verteilten Android-Schadprogramme vollständig zu entfernen.

Quelle: **BSI**

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