ALARM
Awareness Labor KMU Informationssicherheit

# Niederschwelliges Sicherheitskonzept zum Thema Phishing

## 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

Phishing ist heute einer der gängigsten und weit verbreitetsten Wege, Kontrolle über fremde Benutzer-Accounts oder Systeme zu erlangen.

Angreifende versuchen hierbei auf unterschiedlichste Art und Weise Benutzerinnen und Benutzer eines Computer-Systems in eine Falle zu locken, um ihnen ihr Kennwort zu entlocken oder sie zur Ausführung einer bösartigen Software zu verleiten.

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

Neben den direkten Schutzmaßnamen gegen Phishing ist es besonders wichtig, weitere Sicherheitsmaßnahmen aufzubauen, 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.

# 2 Technische Maßnahmen

Die beschriebenen technische Maßnahmen erschweren Angreifenden die Durchführung des Angriffes und können helfen, Schäden zu reduzieren und Auswirkungen zu mindern.

## 2.1 E-Mail-Filter

Ein wichtiger Teil der Sicherheitskette sind E-Mail-Filter. In der Regel versucht ein Filter zu verhindern, dass Mails mit Viren, Malware oder Spam-Mails überhaupt zugestellt werden. Wenn die bösartigen E-Mails jedoch ins Postfach gelangen, hilft nur noch die Aufmerksamkeit der Anwender. Für manche Angriffsmethoden, wenn weitere Komponenten der Angriffssoftware nachgeladen werden sollen, können wieder andere technische Komponenten helfen. Wenn es jedoch darum geht, eine Überweisung zu tätigen oder Dokumente zurückzuschicken, können technische Komponenten kaum Schutz liefern.

## 2.2 Antivirus und Endpoint-Protection

Soweit möglich, sollte auf allen Systemen, sowohl Clients aber auch Servern, eine aktuelle Antiviren-Lösung (AV) eingesetzt werden. Hier können Systeme mit zentraler Managementfunktion helfen, die AV aktuell zu halten.

Auch hierzu gehören begleitend organisatorische Überlegungen, wie mit Meldungen der AV umgegangen wird. Welche Ereignisse lösen automatisierte oder manuelle Prozesse zur Isolation betroffener Systeme aus. Wie wird vor allem mit Fehlalarmen (sog. False-Positives) umgegangen. Diese führen erfahrungsgemäß dazu, dass die Meldungen der AV irgendwann ignoriert werden und im Ernstfall so zu spät reagiert wird.

## 2.3 Web-Filter

Web-Filter helfen, Kommunikation mit dem Internet zu unterbinden, wenn sie potentiell gefährlich, riskant oder unerwünscht ist. Dazu zählen nicht nur die Webseiten die Benutzerinnern und Benutzer im Browser aufrufen, sondern beispielsweise auch die von einer Malware initiierte Kommunikation mit einem System der Angreifenden. Diese versucht sich ebenfalls als Webseiten-Aufruf zu tarnen, um durch diese Filter-Systeme schlüpfen zu können. In der Regel sind diese Filter heute in die Firewall integriert, müssen aber zusätzlich lizensiert werden. Die Konfiguration erfolgt in der Regel auf Basis von Kategorien.

Wenn ein System zur Endpoint-Protection auf den Endgeräten installiert ist, macht dies den Filter auf der Firewall nicht unnötig, denn in der Regel existieren viele weitere Geräte innerhalb des Netzwerkes, die auf den Schutz des zentralen Web-Filters angewiesen sind.

## 2.4 Passwörter

Für die Erstellung und den Umgang mit Passwöorten existieren zahlreiche Empfehlungen. Für die üblichen Anwenderinnen und Anwender verweisen wir hier auf die Richtlinien und Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI).

**Ansatz 1: ein langes und wenig komplexes Passwort**

Für ein Passwort dieser Art verwenden sie eine Aneinanderreihung von Worten, gerne auch getrennt durch Sonderzeichen oder Zahlen. Ziel ist es, mindestens eine Länge von 25 Zeichen zu erreichen, dafür darf der Einsatz von besonderen Zeichen reduziert werden.

**Beispiel:** tisch!himmel!kenia!blau!pfannkuchenteig!lachen

**Ansatz 2: ein kürzeres und komplexes Passwort**

Für ein Passwort dieser Art verwenden sie alle vier Zeichenarten (Großbuchstaben, Kleinbuchstaben, Sonderzeichen, Zahlen) um eine hohe Komplexität zu erreichen.

**Beispiel:** x§uP3?e0aA

**Wichtig ist auch der Umgang mit Passwörtern:** für keine zwei Accounts sollten sie das gleiche Passwort verwenden. Angreifende nutzen Passwörter, von denen sie Kenntnis erlangt haben, bei allen bekannten und weniger bekannten Diensten, um Zugriff zu erlangen. Das gilt sowohl für firmenbezogene als auch private Accounts. Hilfreich in diesem Zusammenhang ist ein Passwort-Manager, also eine Software, die alle Passwörter sicher verwahrt. Nebenbei erlangt man so auch Überblick über alle Accounts, die man bei unterschiedlichen Unternehmen und Diensten angelegt hat.

Wenn der Verdacht besteht, dass Dritte Kenntnis von einem Passwort erlangt haben, ist dieses schnellstmöglich zu ändern. Dieser Verdacht kann zum Beispiel durch unerklärliche Aktivitäten in Accounts oder durch Benachrichtigungen zu Anmeldungen, die man nicht selbst initiiert hat, entstehen.

## 2.5 Multi-Faktor-Authentifzierung

Gegen Passwort-Diebstahl oder das Raten von Passwörtern hilft eine Multi-Faktor-Anmeldung (MFA). Diese ist für alle Systeme notwendig, die direkt aus dem Internet erreichbar sind. Dazu zählen exponierte eigene Systeme oder auch Systeme, die in der Cloud stehen. Moderne Lösungen zur MFA benötigen in der Regel nur noch bei ungewöhnlichen Aktivitäten oder neuen Endgeräten eine Eingabe des sogenannten Tokens durch die Anwenderinnen und Anwender. Damit wird diese nicht als besonders störend empfunden.

Der Token muss nicht zwingen ein Hardware-Token oder eine App auf dem Unternehmens-Smartphone sein. Ein Token kann, wenn keine besonderen Anforderungen an das Schutzniveau vorliegen, auch auf dem privaten Smartphone der Nutzerinnen und Nutzer mittels eigener App generiert werden. Diese App benötigt in der Regel nur minimalen Datenverkehr und ist deutlich komfortabler als ein Hardware-Token. Auf dieser Basis kann eine entsprechende Betriebsvereinbarung geschlossen werden. Ein Token auf einem vermeintlich unsicheren Gerät ist in jedem Fall besser als gar kein Token.

## 2.6 Patch-Management

Eingesetzte Software muss immer auf dem aktuellen Stand gehalten werden.

Patch-Management bezeichnet den Prozess, die Software-Stände aller Systeme des Unternehmens, sowohl auf Servern als auch auf Clients, zu kennen und auf einem aktuellen Stand zu halten.

Organisatorisch bedeutet das für ein Unternehmen

a) die Inventarisierung eingesetzter Software und

b) die Überwachung der vom Hersteller zur Verfügung gestellten Updates sicherzustellen.

Updates beheben oft bis dahin noch nicht öffentlich bekannte Sicherheitslücken, die dem Hersteller zum Beispiel durch IT-Sicherheitsforschende gemeldet wurden. Mit Erscheinen des Updates werden diese Sicherheitslücken zumeist öffentlich gemacht. Angreifende reagieren hierauf sehr schnell und versuchen, diese Lücken auf noch nicht aktualisierten Systemen auszunutzen.

## 2.7 Backup

Regelmäßige Backups der wichtigen Daten und Systeme müssen stattfinden. Hierzu gehört zunächst eine Bewertung, welche Daten/Systeme als kritisch einzustufen sind.

Gerade bei Spezialsoftware reicht es oft nicht aus, nur die Daten zu sichern, da diese nur mit der Software wieder gelesen werden können.

An der Kritikalität sollte sich die Backuphäufigkeit und Methode orientieren.

Eine etablierte Methode ist die sog. 3-2-1-Backup-Regel. Diese besagt, dass von den zu sichernden Daten drei Kopien angefertigt werden, diese auf zwei verschiedenen Speichermedien gesichert werden und eine dieser Sicherung an einem anderen Standort aufbewahrt werden soll.

Zu einem ganzheitlichen Backupkonzept gehören zwingend Tests zur Wiederherstellung der Backups. Je nach Kritikalität sollten hier auch in regelmäßigen Abständen sog. Desaster Recoverys durchgeführt werden. Dabei wird der Komplettausfall der betroffenen Systeme (inkl. Ausfall/Defekt der Hardware) simuliert und das Backup auf neuen Systemen eingespielt.

## 2.8 Festplatten-Verschlüsselung

Alle mobilen Arbeitsplätze wie beispielsweise Laptops oder Notebooks können, im Gegensatz zu den Arbeitsplätzen im Unternehmen, sehr viel leichter gestohlen oder verloren werden. Darum sollten alle diese Geräte mit einer Festplattenverschlüsselung versehen sein. Diese wird in der Regel vom Betriebssystem oder der Endpoint-Protection mitgeliefert. Wichtig ist hierbei darauf zu achten, dass eine Mechanik existiert, mit der vergesse Passwörte nicht zu einem vollständigen Datenverlust führen. Die IT-Abteilung sollte für den Fall der Fälle eine Recovery-Möglichkeit haben.

## 2.9 Smartphones

Smartphones werden in ihrer Kritikalität oftmals unterschätzt, und können genauso wie Laptops leicht gestohlen oder verloren werden. Um als Firma die eigenen Daten schützen zu können, ist ein Mobile Device Management notwendig. Hierdurch können beispielsweise die Daten von verlorenen oder gestohlen Geräten gelöscht werden.

## 2.10 Cloud

Daten in der Cloud sind in der Regel direkt im Internet und auch von überall verfügbar. Mit dem Cloud-Anbieter wird üblicherweise ein Vertrag geschlossen, dass hier keinerlei Zugriff auf die Daten erfolgt, auch wenn das durch den Anbieter in den meisten Fällen technisch möglich wäre. Die Gefahr geht von einem Zugriff durch Unbefugte aus, wenn keine entsprechenden Maßnahmen wie Multi-Faktor-Authentifizierung genutzt werden. Dann können schwache oder gestohlene Passwörte dazu genutzt werden, Daten aus der Cloud zu stehlen. Je nach Inhalt ergeben sich für die Angreifenden weitere Möglichkeiten, wie beispielsweise Erpressung mit der Drohung, die Daten zu veröffentlichen.

## 2.11 Ausgetrickst

Mit einer entsprechend hinterhältig aufgebauten Falle lassen sich auch Personen mit IT-Erfahrung austricksen. Wichtig ist, dass die Beschäftigten angemessen reagieren. Wenn sie eine ungewöhnliche Mail bekommen und sie möglicherweise erst nach dem „Klick“ der Verdacht beschleicht, dass etwas faul war, sollte es einen klar definierten und kommunizierten Meldeweg geben. Der Helpdesk sollte eine zentrale Anlaufstation sein und geeignete Maßnahmen anhand einer Checkliste vorliegen haben, wie weiter zu verfahren ist. Vorwürfe und Schuldzuweisungen führen in einem solchen Fall schnell dazu, dass Benutzerinnern und Benutzer beim nächsten Vorfall nicht mehr nachfragen oder sich nicht melden. Nicht nur in einem solchen Fall ist eine positive Fehlerkultur im Unternehmen sehr wertvoll.

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**