Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Nationales Zentrum für Cybersicherheit (NCSC)
Expertenpool NCSC

Phishing-Prävention

durch Sensibilisierung- und Befähigung der Mitarbeitenden

Stand: Mai 2023

1 Einleitung

Die Phishing-Prävention umfasst Massnahmen zum Schutz vor Phishing-Angriffen. Technische Hilfsmittel wie SPAM Filter reichen nicht aus, um böswillige E-Mails von E-Mail Postfächern fernzuhalten. Aus diesem Grund hängt die Sicherheit massgebend von unserem Sicherheitsverständnis und von unserem Verhalten im Umgang mit E-Mails und dem Internet ab.

Interne Phishing-Kampagnen sind ein verlockendes Instrument zur Phishing-Prävention. Die folgende Analyse zeigt, dass interne Phishing-Kampagnen **Unsicherheit** und **Frustration** hervorrufen können und das Sicherheitsniveau Einbussen erfahren kann. Auch der finanzielle und technische Aufwand für die Durchführung von internen Phishing Kampagnen ist – gemessen am Mehrwert für die Unternehmung - hoch.

Wirksame Massnahmen der Phishing-Prävention sind die Definition und die Kommunikation von Vorgaben zum Umgang mit verdächtigen E-Mails und Internetseiten, sowie der Betrieb eines Melde- und Analyseprozesses für verdächtige E-Mails.

2 Cyberbedrohung Phishing

Der Begriff «Phishing[1]» umfasst Social-Engineering-Angriffe, die darauf abzielen, vertrauliche Informationen zu stehlen oder Schadcode einzuschleusen. Der effektive Schaden entsteht nachträglich, wenn die preisgegebenen Informationen für böswillige Zwecke missbraucht werden.

Folgende **Beispiele** zeigen, wie Cyberkriminelle bei Phishing-Kampagnen vorgehen:

Für den Betrieb von Phishing-Kampagnen nutzen Cyberkriminelle unter anderem:
- kompromittierte oder dedizierte IKT-Infrastrukturen
- illegale Tools (beispielsweise «Phishing-Kits»)

Um technische Schutzmassnahmen zu umgehen, wenden die Absender folgende Tricks an:
- Einbetten von Instruktionen in einem E-Mail Anhang
- Täuschung der technischen Sicherheitsmechanismen durch bewusste Anwendung

[1] https://www.ncsc.admin.ch/ncsc/de/home/cyberbedrohungen/phishing.html

gestalterischer Tricks beim Inhalt der E-Mail

Für eine erfolgreiche Manipulation des Empfängers greifen die Absender von böswilligen E-Mails auf folgende Tricks zurück:

- Missbrauch von Emotionen wie Gier, Neugier, Mitleid und Angst
- Imitation von bekannten Unternehmen

Zu den **möglichen Konsequenzen eines Phishing-Angriffs** gehören beispielsweise:

- Identitätsmissbrauch
- der Missbrauch von Kreditkartendaten
- der Einbruch in IT-Systeme
- die Veröffentlichung der gestohlenen Informationen

3 Massnahmen zur Phishing-Prävention

Phishing-Prävention ist ein untergeordnetes Thema der **Sicherheit im Umgang mit E-Mail- und dem Internet**, welche sich unter anderem auch mit dem Schutz vor Schadcode befasst.

Weil Phishing-Angriffe aus dem Missbrauch von IT-Diensten und der Manipulation von Personen resultieren, erfordert die **Phishing-Prävention** ein **mehrschichtiges Schutzkonzept** bestehend aus dem Einsatz von technischen Hilfsmitteln, einer gezielten Parametrierung der IT-Systeme sowie der Sensibilisierung und Befähigung der potenziellen Zielpersonen (siehe Kapitel 4).

Das folgende Beispiel zeigt vier Themenbereiche, mit denen die Phishing-Prävention in einem Schutzkonzept adressiert werden kann:

- **Schutz der eigenen Infrastruktur vor Missbrauch durch Cyberkriminelle:**
  - Härtung der Internet Domäne (beispielsweise mit Sender Policy Framework)
  - Schutz der Webmail Zugänge (beispielsweise mit Multifaktor Authentisierung)
  - Einrichtung von DomainKeys Identified Mail (DKIM[2])

- **Aussonderung von eingehenden, verdächtigen E-Mails**
  - Einsatz von SPAM Filter;
  - Einrichtung eines DomainKeys Identified Mail Check (DKIM);

- **Minderung der Gefahr im Umgang mit zugestellten E-Mails**:
  - Bereitstellung einer Quarantäne für verdächtige E-Mails
  - Bereitstellung einer Funktion zur Meldung von verdächtigen E-Mails
  - Internet Proxy
  - Betrieb eines *Data Leakage Prevention* Systems

- **Sensibilisierung- und Befähigung der Mitarbeitenden**:
  - Vorgaben zum Umgang mit E-Mails und dem Internet im Unternehmen
  - Durchführung von Sensibilisierungskampagnen

Weitere Massnahmen zur Senkung der Gefahren im Umgang mit E-Mails und dem Internet sind:

- Blockliste für gefährliche Anhänge (https://www.govcert.ch/downloads/blocked-filetypes.txt)

[2] https://www.rfc-editor.org/rfc/rfc6376

- Berechtigungsvergabe nach dem Need-to-have Prinzip (keine privilegierten Berechtigungen (admin) für Endanwender)
- Ausführung von nicht vertrauenswürdigen Makros sperren
- Installation und Ausführung von nicht freigegebener Software sperren

4 Phishing-Prävention durch Sensibilisierung- und Befähigung der Mitarbeitenden

4.1 Zusammenhang zwischen Sensibilisierung und Befähigung

Technische Hilfsmittel bieten in der Regel einen guten Schutz vor unerwünschten E-Mails. Sie sind leider nicht immer in der Lage, Phishing-E-Mails von unseren Postfächern fernzuhalten.

Die **Sensibilisierung** und die **Befähigung** der Mitarbeitenden sollen diese Lücke schliessen, indem sie unser Beurteilungsvermögen und letztendlich unser Verhalten im Umgang mit E-Mails und beim Besuch von Internetseiten positiv beeinflussen sollen.

Abbildung 1 zeigt wie sich die **Sensibilisierung** und die **Befähigung** als Teil der präventiven Massnahmen ergänzen:

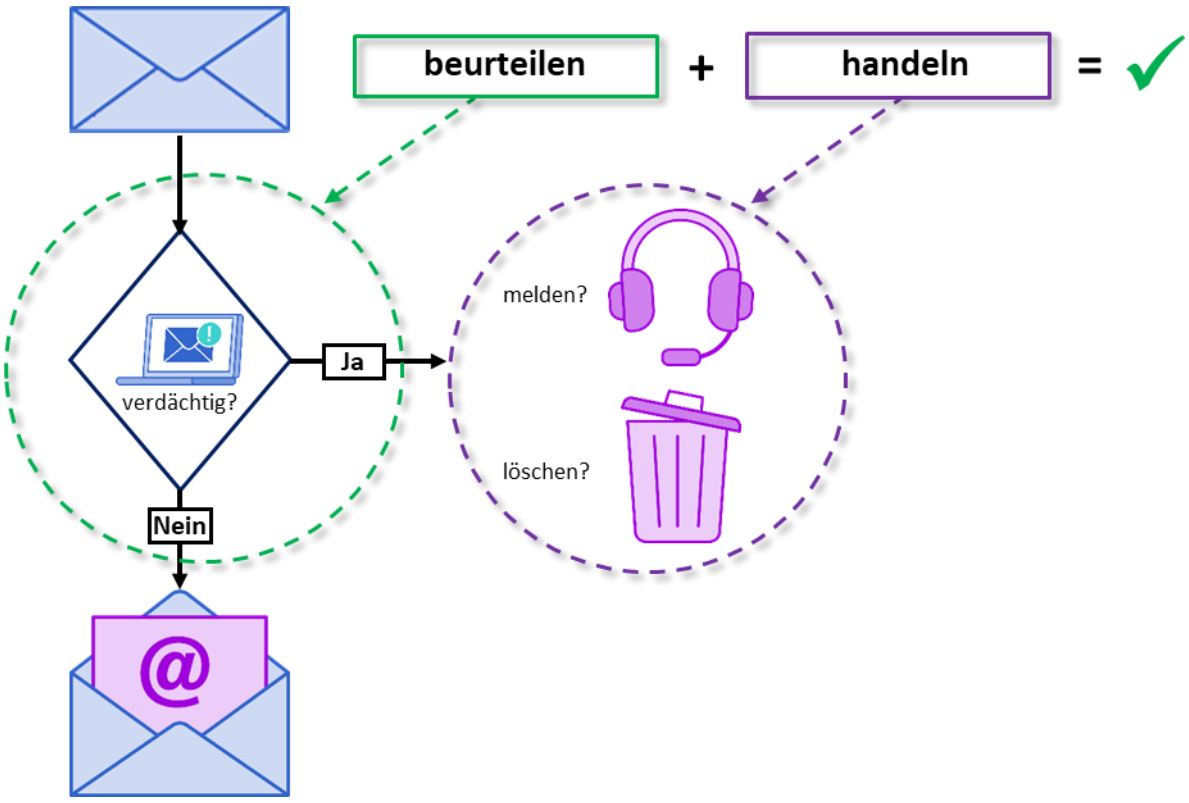

Abbildung 1: E-Mails beurteilen und richtig handeln

4.2 Umgang mit E-Mails

Letztendlich entscheidet unser Verhalten über den Erfolg eines Phishing-Angriffs. Abbildung 2 zeigt die möglichen Szenarien im Umgang mit E-Mails:

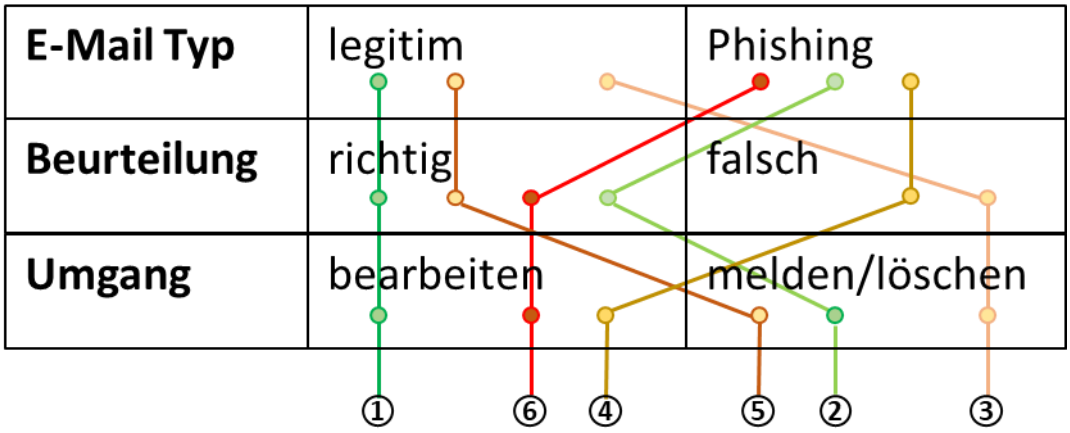

Abbildung 2: Szenarien zum Umgang mit E-Mails

Szenarien:

(1) Der Empfänger erkennt eine legitime E-Mail als solche und bearbeitet sie
(2) Der Empfänger erkennt eine böswillige E-Mail und hält sich an die internen Vorgaben
(3) Der Empfänger stuft eine legitime E-Mail als böswillige E-Mail ein und hält sich an die internen Vorgaben
(4) Der Empfänger stuft eine böswillige E-Mail falsch ein und bearbeitet diese als wäre sie eine legitime Nachricht
(5) Der Empfänger erkennt eine legitime E-Mail und behandelt diese absichtlich als handle es sich um eine böswillige E-Mail
(6) Der Empfänger erkennt eine böswillige E-Mail und behandelt diese absichtlich, als handle es sich um eine legitime E-Mail

Die Szenarien (1) und (2) bilden das ideale Verhalten im Umgang mit E-Mails. Die Szenarien (3) und (4) deuten wegen der falschen Beurteilung auf Defizite in der Sensibilisierung hin. Die Szenarien (5) und (6) zeigen ein bewusstes, falsches Verhalten des Mitarbeitenden.

Die 6 Szenarien zeigen, dass eine **wirksame Sensibilisierung** und die **Bereitstellung klarer Richtlinien** zum Umgang mit E-Mail und dem Internet wesentlich zur Phishing-Prävention beitragen.

4.3 Risiken bei der Sensibilisierung- und Befähigung der Mitarbeitenden durch Phishing-Kampagnen

Eine einzige Phishing-Email kann bei einem falschen Verhalten erheblichen Schaden anrichten. Der falsche Umgang mit E-Mails kann durch **Unsicherheit** und **Frustration** ausgelöst werden.

Mögliche Ursachen für **Unsicherheit** und **Frustration**:

- **Unsicherheit**: Überforderung wegen fehlenden, unklaren oder komplizierten Vorgaben und Abläufen, Zeitdruck, Angst vor Sanktionen
- **Frustration**: Zu viele SPAM Nachrichten im Postfach, anhaltende Unsicherheit, schlechte Erfahrung mit Sicherheitsmassnahmen (beispielsweise Sanktionen)

Mögliche Konsequenzen von **Unsicherheit** und **Frustration**:

- **Unsicherheit**: die Mitarbeitenden erkennen böswillige E-Mails nicht als solche und reagieren deshalb falsch (Szenarien (3) und (4))
- **Frustration**: die Mitarbeitenden resignieren und halten sich nicht mehr an die Vorgaben, falls welche existieren (Szenarien (5) und (6))

Mögliche Massnahmen zur Vermeidung von **Unsicherheit** und **Frustration**:

- Rücksicht auf den Aufgabenbereich und die Arbeitslast der Zielpersonen
- Strikte Trennung zwischen Wissensvermittlung und Testmassnahmen
- Wertschätzung gegenüber pflichtbewussten Mitarbeitenden (z.B. wenn diese eine verdächtige E-Mail melden)

Die Kenntnis dieser Ursachen, Konsequenzen und Massnahmen ist bei der Auswahl von Sensibilisierungmassnahmen und Befähigung der Mitarbeitenden wichtig.

4.4 Beurteilung von internen Phishing-Kampagnen

Viele Unternehmen führen interne Phishing-Kampagnen durch (oder kaufen diese ein) mit dem Ziel, die Phishing-Awareness ihrer Mitarbeitenden zu evaluieren. Eine beliebte Kennzahl ist die **Klickrate**. Eine sinkende Klickrate wird oft als Fortschritt bezüglich Sicherheit interpretiert. Im Wissen, dass eine einzige Phishing-E-Mail ausreicht, um erheblichen Schaden anzurichten, lohnt es sich, die Vorteile und Risiken interner Phishing-Kampagnen abzuwägen.

Die folgenden Überlegungen zeigen **Grenzen** und **Risiken** bei der Durchführung von internen Phishing-Kampagnen:

- Je nach Phishing-Szenario müssen die Schutzmassnahmen der Organisation während der Phishing-Kampagne zum Nachteil der Sicherheit der Unternehmung gelockert werden (zum Beispiel durch Whitelisting von potenziell gefährlichen Anhängen wie .doc, .xls, …).
- Die fehlende Akzeptanz für interne Phishing-Kampagnen kann frustrierte Mitarbeitende dazu verleiten, bewusst falsch zu reagieren und als Folge davon auch bei echten Phishing-E-Mails falsch zu reagieren.
- Nicht personifizierte E-Mail-Adressen (zum Beispiel *kreditoren@meinefirma.ch*) oder externe Dienstleister mit Remote Zugang zu den IT-Systemen sind auch im Visier von Cyberkriminellen. In der Regel sind nur personifizierte E-Mail-Adressen im Scope von internen Phishing-Kampagnen. Die Aussagekraft solcher Kampagnen kann deshalb in Frage gestellt werden.
- Für Unternehmen, welche die Klickrate als Benchmarking-Instrument verwenden, stellt sich die Frage, ob eine Verringerung der Klickrate effektiv eine Erhöhung des Sicherheitsniveaus bedeutet: Selbst wenn die Klickrate sinkt, besteht das Risiko eines erfolgreichen Phishing-Angriffs immer noch.
- Beim Imitieren von bekannten Unternehmen müssen Urheber- und Markenrechte eingehalten werden.
- Sensibilisierung verträgt sich nicht mit dem Sammeln von negativen Erfahrungen. Das Gefühl bei einer internen Phishing-E-Mail «ausgetrickst» worden zu sein, trägt also nicht nachhaltig zum Sicherheitsverständnis der Mitarbeitenden bei.
- Cyberkriminelle sind bei ihren Phishing-Kampagnen rücksichtslos. Bei internen Kampagnen ist der Handlungsspielraum begrenzt.
- Bedrohungen wie Phishing in sozialen Medien oder per SMS lassen sich nur schwer und zeitaufwändig in internen Kampagnen abbilden.
- Gewisse Unternehmen sanktionieren ihre Mitarbeitenden, wenn diese auf eine interne Kampagne reinfallen. Unter solchen Umständen bleibt die Sicherheit eine

Glückssache.
- Das grundlegende Problem bei Phishing liegt nicht beim Verhalten der Mitarbeitenden, sondern bei den unzuverlässigen technischen Massnahmen.

4.5 Fazit

Interne Phishing-Kampagnen können zu Frustration bei den Mitarbeitenden und damit zu einem Vertrauensverlust in die Unternehmung führen. Das Sicherheitsniveau wird dadurch geschwächt.

Wirksame Massnahme der Phishing-Prävention sind:
- die Definition und Bekanntgabe von Vorgaben zum Umgang mit verdächtigen E-Mails und Internetseiten.
- der Betrieb eines Melde- und Analyseprozesses für die Mitarbeitenden.
- der Einsatz von technischen Sicherheitsmechanismen, damit ein erfolgreicher Phishing-Angriff in seiner Wirkung eingegrenzt wird.

5 Berichte zum Thema «Phishing-Kampagnen»

- Simulierte Phishing-Kampagnen: Analyse aus verschiedenen Blickwinkeln https://digitaleweltmagazin.de/simulierte-phishing-kampagnen-ziele-formen-und-ihre-probleme/
- Warum simulierte Phishing-Kampagnen keine gute Idee sind https://www.vdz.org/oeffentliche-it/Security-Awareness-durch-simulierte-Phishing-Kampagnen
- Simulierte Phishing-Kampagnen – Ziele, Formen und ihre Probleme https://digitaleweltmagazin.de/simulierte-phishing-kampagnen-ziele-formen-und-ihre-probleme/
- Phishing for Awareness https://www.kes.info/archiv/leseproben/2020/phishing-for-awareness/
- Lain/Kostiainen/Capkun 2021: Phishing in Organizations: Findings from a Large-Scale and Long-Term Study https://arxiv.org/pdf/2112.07498.pdf
- Telling users to ‘avoid clicking bad links’ still isn’t working https://www.ncsc.gov.uk/blog-post/telling-users-to-avoid-clicking-bad-links-still-isnt-working
- Volkamer/Sasse/Boehm 2020: Phishing-Kampagnen zur Mitarbeiter-Awareness. Analyse aus verschiedenen Blickwinkeln: Security, Recht und Faktor Mensch. Karlsruher Institut für Technologie.