Bundesamt für Verfassungsschutz

Info Blatt

Informationsblätter zum Wirtschaftsschutz

Schutz vor Phishing

Die deutsche Wirtschaft und Wissenschaft, aber auch Politik und Verwaltung, sind lohnende Ziele für Cyberangriffe. Eine der häufigsten Angriffsmethoden ist dabei das sogenannte Phishing. Auch fremde Nachrichtendienste nutzen Cyber- und Phishingangriffe für Spionage und Sabotage.

Mögliche Gefährdungen lassen sich jedoch minimieren. Dabei können auch die Sicherheitsbehörden hinzugezogen werden. Der Verfassungsschutz ist für die Abwehr von Spionage und Sabotage durch ausländische Nachrichtendienste zuständig und steht als vertraulicher Ansprechpartner zur Verfügung.

Die meisten Cyberangriffe beginnen mit einer E-Mail.

1 Was ist Phishing und warum ist es so gefährlich?

DEFINITION

- Beim Phishing erhält der Adressat eine vermeintlich authentische E-Mail. Der E-Mail ist häufig ein Dokument als Anhang beigefügt oder sie enthält Verlinkungen auf
  - ***andere Webseiten***.
- Angreifer nutzen absichtlich **Neugier, Stress oder Angst**. Ziel ist es, Sie dazu zu bringen, auf schadhafte Dokumente zu klicken oder vertrauliche Informationen, wie z. B. Passwörter, preiszugeben.

PHISHING

- *Phishing setzt sich aus „Password“ und „Fishing“ zusammen, zu Deutsch „nach Passwörtern angeln“.*

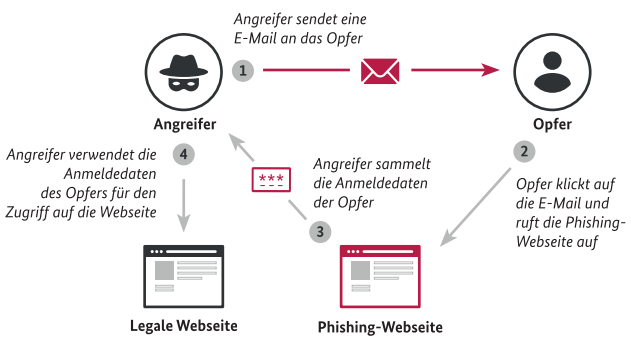
- ***Andere Webseiten***
  *Angreifer bauen z. B. **Login-Webseiten** nahezu identisch nach. Die Daten, die das Opfer hier eingibt, werden vom Angreifer unbemerkt abgegriffen. Danach folgt meist die Weiterleitung auf die korrekte Webseite, damit das Opfer keinen Verdacht schöpft.*

GEFAHR

*Durch Phishing **erbeutete Zugangsdaten** können in vielfältiger Art und Weise gegen Sie verwendet werden.*

- *Zugriff auf andere von Ihnen genutzte **Dienste und Konten***
- *Auslesen Ihrer **Korrespondenzen und Kontakte***
- ***Versand gefälschter E-Mails** mit schädlichen Anhängen oder Links an z. B. Kolleginnen und Kollegen*
- ***Erpressung oder Rufschädigung** mittels erbeuteter persönlicher Informationen oder Bilder*
- ***Verbreiten von Falschnachrichten** in Ihrem Namen z. B. in sozialen Medien*

Ablauf eines typischen Phishing-Angriffs



*Besonders **E-Mail-Konten** sind für Angreifer interessant, lassen sich hier doch viele persönliche Informationen finden.*

- *Bilder/Videos, Kontaktdaten und Kalendereinträge*
- *E-Mails und Dokumente*
- *Informationen über genutzte Social-Media-Konten und andere Onlinedienste*

Viele Onlinedienste sind mit einem E-Mail-Konto verknüpft. Durch die „Passwort vergessen“-Funktion können Angreifer somit auch andere Konten kapern.

2 So erkennen Sie Phishing-Mails.

- Die **Absenderadresse** ist zumeist mittels ➔ ***E-Mail-Spoofing* manipuliert**. Phishing-Mails stammen dann häufig angeblich von Ihrem E-Mail-Provider, von Social-Media-Plattformen oder einer Bank.

➔ ***E-Mail-Spoofing***
Dabei wird Ihnen durch Manipulation der Kopfzeile (E-Mail-Header) eine gefälschte Absenderadresse angezeigt. Schauen Sie sich diese daher im Zweifel genauer an. Mehr Informationen dazu, wie Sie den Mail-Header auslesen, finden Sie auf ***www.verbraucherzentrale.de*** *(„Header“).*

- Ihnen wird **dringender Handlungsbedarf** suggeriert, z. B. „Abschaltung Ihres E-Mail-Kontos in 2 Tagen“. Durch **Drohungen** wird der Druck zusätzlich erhöht, z. B. „Wenn Sie jetzt nicht aktiv werden, dann …“.
- Es sind **Links oder Dateien enthalten**, welche durch Sie geöffnet werden sollen. Dabei werden **vertrauliche Daten abgefragt**, z. B. PINs, TANs oder Passwörter.
- Häufig lassen sich **Rechtschreibfehler oder auch sprachliche Unstimmigkeiten** im Text finden, wie z. B. Formulierungen, die nicht zum Absender passen. Die **Anrede** ist oft unpersönlich, z. B. „Sehr geehrter Kunde“. Ein **Impressum** ist nicht vorhanden oder unvollständig.

SPEAR-PHISHING

➔ *Spear-Phishing ist vom Vorgehen her ähnlich (schadhafter Link oder Anhang, Abgreifen von Anmeldedaten etc.). Der Angriff richtet sich in der Regel jedoch gegen eine bestimmte Organisation oder einen bestimmten Personenkreis bzw. sogar Einzelpersonen. Die Angriffs-E-Mail ist dabei individuell auf das konkrete Ziel zugeschnitten und der häufigste Infektionsweg für gezielte Cyberangriffe.*

3 So schützen Sie sich.

PERSÖNLICHE SCHUTZMASSNAHMEN

- Misstrauen Sie allen E-Mails, die Sie zu dringenden Handlungen auffordern. **Geben Sie niemals Ihre Passwörter an.** Dies gilt auch für E-Mails von Familie, Freunden oder dem Arbeitgeber. Deren **E-Mail-Konten könnten ebenfalls gehackt** worden sein.
- Hinterfragen Sie bei verdächtigen E-Mails, welche **Verbindung Sie tatsächlich zum Absender** haben und ob die **Handlungsaufforderung** wirklich **plausibel** sein kann.
- Klicken Sie **niemals auf Links oder Anhänge** verdächtiger E-Mails. Seien Sie besonders vorsichtig bei Anhängen mit Formaten wie .exe oder .scr. Nutzen Sie Ihren **Browser**, um eine Webseite zu suchen und sich dort ggf. zu authentifizieren.
- Aktivieren Sie – wann immer möglich – bei Online-Konten die **Zwei-Faktor-Authentifizierung**.
- Überprüfen Sie durch einen Mouseover die in der E-Mail **enthaltenen Verlinkungen**. Welche **Webseitenadresse** (URL) wird dort angezeigt?
- Lassen Sie sich ggf. den Versand der E-Mail **vom Absender bestätigen**, z. B. telefonisch.
- Sie können mit dem **E-Mail-Inhalt** auch eine **Internetsuche durchführen**. So können Sie prüfen, ob andere Personen ebenfalls diese E-Mail erhalten und bereits gemeldet haben.
- Installieren Sie **Antivirenprogramme und aktualisieren Sie Software und Betriebssystem** immer umgehend.
- Verwenden Sie **verschiedene und starke Passwörter** (➔ ***sichere Passwörter***).

Sichere Passwörter

➔ *Passwörter wie „12345“ oder „passwort“ können von Angreifern schnell geknackt werden. Sichere Passwörter bestehen aus mindestens 8 Zeichen, beinhalten Groß- und Kleinschreibung sowie mindestens 1 Sonderzeichen und eine Zahl.*

➔ *Verwenden Sie für unterschiedliche Onlinekonten verschiedene Passwörter. So schützen Sie diese besser vor fremden Zugriff. Nutzen Sie ggf. das „Passwort-Merkblatt“ des Bundesamts für Sicherheit in der Informationstechnik (BSI).*

➔ *Weitere Tipps zum Erstellen und Verwalten sicherer Passwörter bieten neben dem BSI auch die Verbraucherzentralen:*
www.bsi-fuer-buerger.de
www.verbraucherzentrale.de

3

SO KÖNNEN SIE DAS RISIKO IM UNTERNEHMEN SENKEN.

- Minimieren Sie **potentielle Zugriffsmöglichkeiten** (sog. Angriffsvektoren) auf das System. Wägen Sie sorgfältig ab, welche digitalen Vorgänge und Systeme für die tägliche Arbeit unbedingt erforderlich sind oder ggf. **vom Netz getrennt** werden können.
- Fertigen Sie in regelmäßigen Abständen **Sicherheitskopien/ Backups** an und bewahren Sie diese anschließend von den betroffenen Systemen getrennt auf.
- Schließen sie bekannte Sicherheitslücken durch das **Einspielen vorhandener Patches** und installieren Sie regelmäßig die **neuesten Updates**.
- Verwenden Sie **aktuelle Betriebssysteme und Programme**. Ziehen Sie den Einsatz von **Anti-Spam und Anti-Phishing-Programmen** in Betracht.
- Überprüfen Sie regelmäßig Nutzerkonten, Berechtigungen und Nutzer auf Systemen. Entfernen Sie **unbekannte oder nicht mehr verwendete Nutzer** (bspw. ehemalige Mitarbeitende) und reduzieren Sie **Nutzungsberechtigungen auf ein Minimum**.
- Erwägen Sie den Einsatz eines sogenannten **Intrusion Detection Systems (IDS)** bzw. **Intrusion Prevention Systems (IPS)**. Dadurch können eine Vielzahl von Schadsoftware erkannt und blockiert werden.
- Setzen Sie zur besseren Absicherung Ihres E-Mail-Verkehrs eine **Transport- oder eine Ende-zu-Ende-Verschlüsselung** ein. Durch die Verwendung **digitaler Signaturen** stellen Sie die Integrität der Daten und der Absender von E-Mails sicher.

BESCHÄFTIGTE ALS „MENSCHLICHE FIREWALL“

Mittels Phishing wollen Angreifer die zunehmenden technischen Sicherheitsmaßnahmen wie Firewall oder Spamfilter überwinden. Daher kommt Ihnen als Beschäftigte eine besondere Verantwortung zu. Seien Sie stets wachsam und öffnen Sie niemals leichtfertig verdächtige E-Mails oder Anhänge.

SO SCHÜTZEN SIE IHRE BESCHÄFTIGTEN.

- **Sensibilisieren Sie regelmäßig alle Mitarbeitenden**, sich an Sicherheitsvorkehrungen zu halten. Informieren Sie diese auch umgehend über **neue Angriffsmethoden**.
- Erleichtern Sie Ihren Beschäftigten den Umgang mit potentiell gefährlichen E-Mails und stellen Sie **klare E-Mail-Richtlinien mit Checklisten** auf.
- Mittels **Phishing-Tests** lässt sich eventuell weiterhin bestehender Schulungs- und Sensibilisierungsbedarf erkennen. Dabei werden simulierte Phishing-E-Mails an die Beschäftigten versendet.

HOMEOFFICE

Im Homeoffice ist die Gefahr von Cyberangriffen besonders groß: klare Verhaltensregeln, Schulungen und die notwendige technische Ausstattung sind hier unerlässlich.

Wirtschaft & Wissenschaft.
Zukunftssicher.
Verfassungsschutzverbund des Bundes und der Länder

*Das Bundesamt für Verfassungsschutz und die 16 Landesbehörden für Verfassungsschutz bilden gemeinsam den Verfassungsschutzverbund. Auch im Bereich des präventiven Wirtschaftsschutzes arbeitet dieser eng zusammen. Auf diese Weise entsteht ein starkes Netzwerk bis zu Ihnen vor Ort. Eine Übersicht über die Ansprechbarkeiten in den Landesbehörden finden Sie unter **www.verfassungsschutz.de**.*

initiative wirtschaftsschutz
Gemeinsam. Werte. Schützen.

*Die Initiative Wirtschaftsschutz ist ein Zusammenschluss von BfV, BKA, BND und BSI. Auf der Informationsplattform **www.wirtschaftsschutz.info** stellen sie zusammen mit verschiedenen Partnerverbänden ihre Expertise im Bereich Wirtschaftsschutz zur Verfügung. Dazu gehört das Thema Cyberkriminalität genauso wie Wirtschafts- und Wissenschaftsspionage oder das Thema IT-Sicherheit.*

Ihr direkter Kontakt zum Wirtschaftsschutz

Bundesamt für Verfassungsschutz
Bereich Prävention (Wirtschafts- und Wissenschaftsschutz)

+49 (0)30 18 792 33 22
wirtschaftsschutz@bfv.bund.de