Arbeitshilfe 3: Phishing-Mails und Social Engineering sicher erkennen

Phishing ist heute professionell, fehlerfrei und personalisiert. Klassische Warnzeichen wie Rechtschreibfehler, falsche Anrede oder schlechtes Deutsch reichen nicht mehr aus. Moderne Angriffe setzen auf psychologischen Druck und glaubwürdige Inhalte.

Entscheidend ist heute nicht mehr die Form, sondern der Inhalt.

Teil 1: Typische Warnsignale

- **Warnsignal 1:** Aufbau von Handlungsdruck
  Formulierungen: „Bitte sofort handeln", „Nur heute möglich", „Letzte Erinnerung", „Ihr Konto wird gesperrt, wenn Sie nicht reagieren"
  Taktik: Angreifer wollen, dass Sie keine Zeit zum Nachdenken haben.
- **Warnsignal 2:** Androhung von Konsequenzen
  Inhalte: Kontosperrung, Zugriffsverlust, Vertragskündigung, Sicherheitsvorfälle („Unbefugter Zugriff festgestellt")
  Taktik: Angst ist ein zentrales Werkzeug von Social Engineering.
- **Warnsignal 3:** Ausnutzen von Rollen und Hierarchien
  Formulierungen: „Ich bin aus der IT", „Geschäftsführung bittet um schnelle Rückmeldung", „HR/Personalabteilung/Compliance"
  Taktik: Autorität ersetzt Vertrauen.
- **Warnsignal 4:** Kontext passt „zu gut"
  Inhalte: Bezug auf Jobwechsel, Onboarding, Urlaubsvertretung oder aktuelle Projekte. Zeitlich perfekt platziert (z. B. direkt nach LinkedIn-Post)
  Taktik: KI macht kontextbezogene Angriffe extrem einfach.
- **Warnsignal 5:** Aufforderung zu Klicks oder Dateneingaben
  Formulierungen: „Passwort zurücksetzen", „Zugang bestätigen", „Dokument prüfen", „Sicherheitsüberprüfung durchführen"
  Taktik: Seriöse Stellen fordern sensible Daten selten per Link.

Teil 2: Konkrete Handlungsempfehlungen

- **Maßnahme 1:** Gesunden Menschenverstand einschalten
  Fragen Sie sich:
  - Ist das Anliegen realistisch?
  - Passt der Ton zur Organisation?
  - Würde diese Stelle wirklich so kommunizieren?
  - Warum gerade jetzt?

  Grundregel: Bauchgefühl ernst nehmen. Wenn etwas komisch wirkt, ist es meist auch komisch.
- **Maßnahme 2:** Tempo rausnehmen
  Nicht sofort handeln. Kurz pausieren. Mail bewusst noch mal lesen.
  Grundregel: Zeit ist der größte Feind von Phishing.
- **Maßnahme 3:** Rückversicherung über bekannte Wege
  Nicht auf „Antworten" klicken. Nicht auf Links klicken. Bekannte Kontaktwege nutzen: interne Telefonnummer, bekannte E-Mail-Adresse, offizielles Ticketsystem.
  Grundregel: Im Zweifel selbst den Kontakt herstellen.
- **Maßnahme 4:** Nachfragen ist ausdrücklich erwünscht
  „Lieber einmal zu viel gefragt" als falschen Link geklickt, Zugangsdaten preisgegeben oder Schaden verursacht.
  Grundregel: Sicherheitskultur lebt von Nachfragen, nicht von Schweigen.
- **Maßnahme 5:** Verdächtige Mails melden
  Interne Meldestelle nutzen. IT/Security/Datenschutz informieren. Mail nicht weiterleiten, sondern melden.

  Grundregel: Ein gemeldeter Vorfall schützt auch andere.