16.3 Phishing, Social Engineering und Identitätsangriffe

Viele Angriffe beginnen nicht mit einer technischen Schwachstelle, sondern mit Täuschung.

Angreifer versuchen, Menschen dazu zu bringen,

- Zugangsdaten einzugeben
- Links anzuklicken
- Anhänge zu öffnen
- MFA-Anfragen zu bestätigen
- Geld zu überweisen
- vertrauliche Informationen preiszugeben
- Schadsoftware auszuführen
- Sicherheitsregeln zu umgehen

Merksatz:

> Social Engineering greift Menschen und Prozesse an,
> nicht nur Technik.

Warum Phishing so gefährlich ist

Phishing ist gefährlich, weil es normale Arbeitsabläufe ausnutzt.

Beispiele:

- Rechnung prüfen
- Paketbenachrichtigung öffnen
- Passwort zurücksetzen
- Cloud-Datei ansehen
- Bewerbung herunterladen
- Supportanfrage beantworten
- dringende Chef-Anweisung befolgen

Angreifer nutzen dabei:

```
Zeitdruck
Vertrauen
Neugier
Angst
Hilfsbereitschaft
Autorität
Gewohnheit
```

Merksatz:

```
Phishing wirkt,
weil es menschliches Verhalten ausnutzt.
```

Phishing

Phishing ist der Versuch, Benutzer durch Täuschung zur Preisgabe vertraulicher Informationen zu bringen.

Ziele:

```
Passwörter
MFA-Codes
Zugangstokens
Bankdaten
Kundendaten
interne Informationen
Cloud-Zugänge
VPN-Zugänge
E-Mail-Konten
```

Typische Mittel:

```
gefälschte E-Mail
gefälschte Webseite
gefälschtes Loginformular
gefälschte Rechnung
gefälschte Sicherheitswarnung
gefälschter Cloud-Link
```

Merksatz:

```
Phishing täuscht Benutzer,
damit sie selbst etwas Gefährliches tun.
```

Typischer Phishing-Ablauf

Ein typischer Ablauf:

1. Benutzer erhält eine täuschend echte Nachricht.
2. Nachricht erzeugt Druck oder Interesse.
3. Benutzer klickt Link oder öffnet Anhang.
4. Gefälschte Webseite fragt Zugangsdaten ab.
5. Benutzer gibt Daten ein.
6. Angreifer nutzt die Zugangsdaten.
7. Konto wird übernommen oder Malware wird ausgeführt.

Merksatz:

```
Phishing ist oft der Einstieg in größere Angriffe.
```

Phishing per E-Mail

E-Mail-Phishing ist besonders verbreitet.

Typische Merkmale:

```
angebliche Rechnung
angebliche Lieferung
angebliche Kontosperrung
angebliche Passwortwarnung
angebliche Cloud-Dateifreigabe
angebliche Bewerbung
angebliche Sicherheitsmeldung
angeblicher Chefauftrag
```

Merksatz:

E-Mail ist ein häufiger Einstiegspunkt für Angriffe.

Phishing per SMS

Phishing per SMS wird oft genannt:

Smishing

Typische Beispiele:

Paket konnte nicht zugestellt werden.
Konto wurde gesperrt.
Zahlung erforderlich.
Sicherheitsprüfung notwendig.
Link zur Sendungsverfolgung.

Risiko:

Benutzer klicken am Smartphone oft schneller auf Links.

Merksatz:

Smishing ist Phishing über SMS.

Phishing per Telefon

Phishing per Telefon wird oft genannt:

Vishing

Dabei ruft ein Angreifer an und gibt sich zum Beispiel aus als:

IT-Support
Bankmitarbeiter
Chef
Dienstleister

Behörde

Sicherheitsabteilung

Ziel:

Zugangsdaten erhalten

MFA-Code erhalten

Fernwartung starten

Überweisung auslösen

interne Informationen bekommen

Merksatz:

Vishing ist Phishing per Telefon.

Phishing über Messenger

Angriffe können auch über Messenger laufen.

Beispiele:

angebliche Nachricht von Kollegen

gefälschter Supportkontakt

Link zu Cloud-Datei

dringende Zahlungsanweisung

angebliches Problem mit Benutzerkonto

QR-Code zu Loginseite

Merksatz:

Phishing ist nicht auf E-Mail beschränkt.

QR-Phishing

QR-Phishing wird auch Quishing genannt.

Dabei führt ein QR-Code auf eine gefälschte Webseite.

Risiko:

Link ist vor dem Scannen schwer erkennbar.
Smartphone zeigt Adresse oft nur verkürzt.
Benutzer erwarten bei QR-Codes schnelle Aktion.

Beispiele:

gefälschter Paketaufkleber
falsches WLAN-Portal
falsche Zahlungsseite
gefälschter Microsoft-Login
Plakat oder E-Mail mit QR-Code

Merksatz:

QR-Code nicht automatisch vertrauen.

Spear Phishing

Spear Phishing ist gezieltes Phishing gegen bestimmte Personen, Teams oder Organisationen.

Angreifer nutzen oft Informationen wie:

Name
Firma
Rolle
laufendes Projekt
bekannte Kollegen
verwendete Dienste
Signatur
Lieferanten
interne Begriffe

Dadurch wirkt die Nachricht glaubwürdiger.

Merksatz:

Spear Phishing ist gezielter und glaubwürdiger als Massenphishing.

Whaling

Whaling ist Phishing gegen besonders wichtige Personen.

Ziele:

```
Geschäftsführung
Finanzleitung
Personalabteilung
Administratoren
Projektleitung
Geschäftsbereichsleitung
```

Warum gefährlich?

```
Diese Personen haben oft besondere Rechte,
Informationen
oder Entscheidungsbefugnisse.
```

Merksatz:

```
Whaling richtet sich gegen besonders wertvolle Ziele.
```

CEO-Fraud

CEO-Fraud ist eine Betrugsform, bei der Angreifer sich als Geschäftsführung oder Vorgesetzte ausgeben.

Typisches Ziel:

```
schnelle Überweisung
Änderung von Bankdaten
Herausgabe vertraulicher Informationen
Einkauf von Gutscheinkarten
Umgehung normaler Freigabeprozesse
```

Typische Merkmale:

```
sehr dringend
vertraulich
keine Rückfrage erwünscht
ungewöhnliche Zahlungsdaten
außerhalb normaler Prozesse
```

Merksatz:

```
CEO-Fraud nutzt Autorität und Zeitdruck.
```

Business E-Mail Compromise

Business E-Mail Compromise wird oft abgekürzt:

```
BEC
```

Dabei wird ein geschäftliches E-Mail-Konto kompromittiert oder täuschend echt nachgeahmt.

Ziele:

```
Rechnungsbetrug
Änderung von Kontodaten
interne Täuschung
Phishing aus echtem Konto
Zugriff auf Geschäftskommunikation
```

Merksatz:

```
BEC nutzt geschäftliche E-Mail-Kommunikation für Betrug.
```

Fake Login

Ein Fake Login ist eine gefälschte Anmeldeseite.

Sie sieht oft aus wie:

Microsoft 365
Google
VPN-Portal
Cloud-Speicher
Bank
Paketdienst
Unternehmensportal

Ziel:

Zugangsdaten abgreifen

Merksatz:

Gefälschte Loginseiten sind ein Kernmittel von Phishing.

Credential Harvesting

Credential Harvesting bedeutet:

Zugangsdaten werden gesammelt.

Beispiele:

gefälschte Loginseite
Keylogger
Phishing-Mail
manipulierte Anwendung
Malware
unsichere Datenbank
abgegriffene Browserdaten

Merksatz:

Credential Harvesting sammelt Zugangsdaten für spätere Angriffe.

Session Hijacking

Session Hijacking bedeutet:

> Ein Angreifer übernimmt eine bestehende Sitzung.

Ziel:

> Zugriff erhalten,
> ohne das Passwort erneut eingeben zu müssen.

Mögliche Mittel:

> gestohlene Session-Cookies
> gestohlene Tokens
> Malware im Browser
> unsichere Verbindung
> XSS
> kompromittiertes Endgerät

Merksatz:

> Session Hijacking greift die laufende Anmeldung an.

MFA-Bypass

MFA macht Angriffe schwerer, aber nicht unmöglich.

Mögliche Angriffe:

> MFA-Push-Fatigue
> Phishing mit Echtzeit-Weiterleitung
> gestohlene Session-Tokens
> kompromittiertes Endgerät
> Social Engineering beim Support
> unsichere Ausnahmen
> SIM-Swapping bei SMS-MFA

Merksatz:

MFA ist wichtig,
aber keine alleinige Schutzmaßnahme.

MFA-Push-Fatigue

MFA-Push-Fatigue bedeutet:

Angreifer lösen viele MFA-Push-Anfragen aus.

Ziel:

Benutzer bestätigt aus Versehen,
aus Gewohnheit
oder genervt.

Schutz:

Number Matching
klare Anzeige von Ort und Anwendung
Schulung
Meldeweg für unerwartete MFA-Anfragen
Rate Limiting
verdächtige Anfragen blockieren

Merksatz:

Unerwartete MFA-Anfragen niemals bestätigen.

SIM-Swapping

SIM-Swapping bedeutet:

Angreifer übernehmen die Mobilfunknummer eines Opfers.

Ziel:

SMS-Codes empfangen
Passwortzurücksetzung durchführen
Konten übernehmen

Schutz:

SMS-MFA möglichst vermeiden
App-basierte MFA oder Hardwaretoken nutzen
Mobilfunkkonto schützen
ungewöhnliche Netzverluste beachten

Merksatz:

SMS als MFA-Faktor ist schwächer als sichere Authenticator- oder Hardwarelösungen.

Social Engineering

Social Engineering ist die Manipulation von Menschen, um Sicherheitsmaßnahmen zu umgehen.

Angreifer nutzen zum Beispiel:

Autorität
Dringlichkeit
Angst
Hilfsbereitschaft
Sympathie
Neugier
Gewohnheit
Vertraulichkeit

Merksatz:

Social Engineering nutzt Psychologie als Angriffsmittel.

Pretexting

Pretexting bedeutet:

Angreifer erfinden eine glaubwürdige Geschichte oder Rolle.

Beispiele:

angeblicher IT-Support
angeblicher neuer Mitarbeiter
angeblicher Dienstleister
angebliche Bank
angebliche Behörde
angeblicher Kunde

Ziel:

Vertrauen erzeugen
Informationen erhalten
Aktionen auslösen

Merksatz:

Pretexting arbeitet mit erfundener glaubwürdiger Rolle.

Baiting

Baiting bedeutet:

Angreifer legen einen Köder aus.

Beispiele:

USB-Stick mit Aufschrift „Gehälter“
kostenloser Download
angebliches Tool
Gutschein
Gewinnspiel
kostenlose Software

Ziel:

Benutzer soll etwas öffnen,
installieren
anschließen
oder Daten eingeben.

Merksatz:

Baiting nutzt Neugier oder Vorteilserwartung.

Tailgating

Tailgating bedeutet:

Eine unberechtigte Person folgt einer berechtigten Person in einen geschützten Bereich.

Beispiele:

Person folgt durch Sicherheitstür.
Person trägt angeblich schwere Kisten.
Person bittet freundlich,
die Tür aufzuhalten.

Merksatz:

Tailgating umgeht physische Zutrittskontrolle.

Shoulder Surfing

Shoulder Surfing bedeutet:

Angreifer beobachten Eingaben oder Bildschirme.

Beispiele:

Passwort beim Tippen ansehen
PIN am Automaten beobachten

Bildschirm im Zug mitlesen
MFA-Code ablesen

Schutz:

Sichtschutzfolie
Bildschirm sperren
Umgebung beachten
keine sensiblen Eingaben in unsicheren Umgebungen

Merksatz:

Shoulder Surfing nutzt Beobachtung.

Dumpster Diving

Dumpster Diving bedeutet:

Angreifer durchsuchen Müll oder entsorgte Unterlagen.

Ziele:

Passwörter
interne Dokumente
Netzwerkpläne
Rechnungen
Kundendaten
alte Datenträger
Notizzettel
Organigramme

Schutz:

Aktenvernichtung
sichere Datenträgervernichtung
Clean-Desk-Regel
Entsorgungsprozesse

Merksatz:

```
Auch entsorgte Informationen können sicherheitskritisch sein.
```

Identitätsangriffe

Identitätsangriffe richten sich gegen Benutzerkonten, Rollen und Anmeldungen.

Typische Angriffe:

```
Phishing
Brute Force
Credential Stuffing
Password Spraying
Session Hijacking
MFA-Missbrauch
Kontoübernahme
Rechteausweitung
```

Merksatz:

```
Wer Identität kontrolliert,
kontrolliert oft den Zugriff.
```

Account Takeover

Account Takeover bedeutet:

```
Ein Angreifer übernimmt ein Benutzerkonto.
```

Mögliche Folgen:

```
E-Mails lesen
interne Daten abrufen
Phishing aus echtem Konto senden
Dateien löschen
Rechte ausnutzen
weitere Konten angreifen
```

Regeln oder Weiterleitungen einrichten

Merksatz:

Kontoübernahme ist oft der Startpunkt für weitere Angriffe.

Brute Force

Brute Force bedeutet:

viele Passwörter werden systematisch ausprobiert.

Schutz:

MFA
Rate Limiting
starke Passwörter
Sperrmechanismen
Monitoring
keine Standardkonten
Passwortmanager

Merksatz:

Brute Force wird durch Begrenzung und MFA erschwert.

Credential Stuffing

Credential Stuffing bedeutet:

Angreifer nutzen geleakte Zugangsdaten aus anderen Diensten.

Beispiel:

Passwort aus altem Webshop-Leak
wird am Firmenportal ausprobiert.

Schutz:

```
keine Passwortwiederverwendung
MFA
Passwortmanager
Leak-Erkennung
riskante Loginversuche erkennen
```

Merksatz:

```
Credential Stuffing nutzt wiederverwendete Passwörter.
```

Password Spraying

Password Spraying bedeutet:

```
wenige häufige Passwörter werden gegen viele Konten getestet.
```

Beispiele:

```
Willkommen2026!
Sommer2026!
Passwort123!
```

Ziel:

```
Kontosperren vermeiden,
weil pro Konto nur wenige Versuche auftreten.
```

Merksatz:

```
Password Spraying verteilt wenige Passwörter auf viele Benutzer.
```

Passwort-Wiederverwendung

Passwort-Wiederverwendung bedeutet:

dasselbe Passwort wird bei mehreren Diensten genutzt.

Problem:

Wird ein Dienst kompromittiert,
können Angreifer das Passwort bei anderen Diensten ausprobieren.

Schutz:

Passwortmanager
eindeutige Passwörter
MFA
Schulung
Passwort-Leak-Prüfung

Merksatz:

Ein Passwort darf nicht mehrfach genutzt werden.

Starke Passwörter

Starke Passwörter sollten:

lang sein
nicht leicht erratbar sein
nicht wiederverwendet werden
nicht aus persönlichen Daten bestehen
nicht in Listen bekannter Passwörter vorkommen

Für viele Konten ist ein Passwortmanager sinnvoll.

Merksatz:

Länge und Einzigartigkeit sind wichtiger als komplizierte Merkhilfen.

Passwortmanager

Ein Passwortmanager hilft, für jeden Dienst ein eigenes starkes Passwort zu verwenden.

Vorteile:

```
eindeutige Passwörter
lange Passwörter
weniger Wiederverwendung
Erkennung falscher Webseiten möglich
sicherere Speicherung als Notizzettel
```

Merksatz:

```
Passwortmanager unterstützt starke und eindeutige Passwörter.
```

Account Lockout

Account Lockout bedeutet:

```
Ein Konto wird nach mehreren fehlgeschlagenen Anmeldeversuchen gesperrt.
```

Vorteil:

```
Schutz vor Brute Force
```

Risiko:

```
Angreifer können viele Konten absichtlich sperren.
```

Deshalb sinnvoll kombinieren mit:

```
Rate Limiting
Risikoanalyse
MFA
Monitoring
differenzierten Sperrregeln
```

Merksatz:

Kontosperren helfen,
müssen aber sinnvoll eingestellt sein.

Rate Limiting

Rate Limiting begrenzt, wie viele Anfragen oder Loginversuche in einer Zeit erlaubt sind.

Beispiele:

maximal 5 Loginversuche pro Minute
begrenzte API-Anfragen
Verzögerung nach Fehlversuchen

Merksatz:

Rate Limiting bremst automatisierte Angriffe.

Captcha

Captcha soll prüfen, ob ein Mensch oder ein automatisiertes Programm handelt.

Einsatz:

Loginformulare
Registrierungen
Passwortzurücksetzung
öffentliche Formulare

Grenze:

Captchas sind keine vollständige Sicherheitsmaßnahme.

Merksatz:

Captcha erschwert Automatisierung,
ersetzt aber keine sichere Authentifizierung.

Phishing-Erkennungsmerkmale

Mögliche Warnzeichen:

ungewöhnlicher Absender
unerwarteter Anhang
dringende Aufforderung
Drohung mit Sperrung
ungewöhnliche Zahlungsaufforderung
Rechtschreib- oder Formatfehler
verkürzte Links
Domain passt nicht
Login wird über Link gefordert
vertrauliche Daten werden verlangt
Absenderadresse und Anzeigename passen nicht zusammen

Merksatz:

Bei Druck,
ungewöhnlichem Link
oder Datenabfrage vorsichtig sein.

Links prüfen

Bei Links prüfen:

passt die Domain?
ist die Verbindung HTTPS?
ist die Adresse ungewöhnlich lang?
gibt es Tippfehler in der Domain?
wird eine bekannte Marke nachgeahmt?
führt der Link über Weiterleitungen?
ist es ein verkürzter Link?
passt der Link zum erwarteten Dienst?

Merksatz:

Nicht der sichtbare Text zählt,
sondern das echte Ziel des Links.

Anhänge prüfen

Gefährliche Anhänge können sein:

ausführbare Dateien
Makro-Dokumente
Archive mit Passwort
angebliche Rechnungen
Skripte
ISO-Dateien
LNK-Dateien
HTML-Dateien
manipulierte PDFs

Merksatz:

Unerwartete Anhänge immer kritisch prüfen.

Absender prüfen

Bei E-Mails ist der Anzeigename leicht fälschbar.

Zu prüfen:

echte Absenderadresse
Domain
Antwortadresse
Signatur
Schreibstil
Kontext
ungewöhnliche Anfrage
SPF,
DKIM
DMARC-Ergebnis je nach System

Merksatz:

```
Anzeigename allein beweist nichts.
```

SPF

SPF steht für:

```
Sender Policy Framework
```

SPF legt fest, welche Mailserver für eine Domain E-Mails senden dürfen.

Merksatz:

```
SPF prüft,
ob ein sendender Mailserver zur Domain passt.
```

DKIM

DKIM steht für:

```
DomainKeys Identified Mail
```

DKIM nutzt digitale Signaturen, um zu prüfen, ob eine E-Mail unterwegs verändert wurde und ob sie zur sendenden Domain passt.

Merksatz:

```
DKIM signiert E-Mails kryptografisch.
```

DMARC

DMARC steht für:

```
Domain-based Message Authentication,
Reporting and Conformance
```

DMARC baut auf SPF und DKIM auf.

Es legt fest, wie Empfänger mit E-Mails umgehen sollen, die SPF oder DKIM nicht bestehen.

Merksatz:

DMARC gibt Richtlinien für den Umgang mit verdächtigen E-Mails.

SPF, DKIM und DMARC einordnen

Technik	Zweck
SPF	prüft erlaubte sendende Mailserver
DKIM	prüft Signatur und Veränderung
DMARC	legt Richtlinie und Berichte fest

Wichtig:

Diese Techniken helfen gegen E-Mail-Spoofing,
verhindern aber nicht jede Phishing-Mail.

Merksatz:

SPF,
DKIM
und DMARC verbessern E-Mail-Authentizität.

Technische Schutzmaßnahmen gegen Phishing

Maßnahmen:

Spamfilter
Malwarefilter
Linkprüfung
Anhangprüfung
Sandboxing
SPF
DKIM
DMARC
MFA

Conditional Access
Passwortmanager
Webfilter
EDR
DNS-Filter
sichere Browserkonfiguration

Merksatz:

Phishing-Schutz braucht mehrere technische Schichten.

Organisatorische Schutzmaßnahmen gegen Phishing

Maßnahmen:

Schulungen
klare Meldewege
Phishing-Simulationen
Vier-Augen-Prinzip
Zahlungsprozesse absichern
Rückruf über bekannte Telefonnummer
Sicherheitsrichtlinien
Freigabeprozesse
Notfallplan bei Kontoübernahme

Merksatz:

Prozesse schützen dort,
wo Technik allein nicht reicht.

Verhalten bei verdächtiger Nachricht

Sinnvolles Vorgehen:

1. Nicht auf Links klicken.
2. Keine Anhänge öffnen.
3. Keine Zugangsdaten eingeben.

4. Absender und Domain prüfen.
5. Bei angeblichen internen Anfragen über bekannten Kanal nachfragen.
6. Nachricht melden.
7. Nicht weiterleiten,
   wenn dadurch Risiko entsteht.
8. IT oder Sicherheitsverantwortliche informieren.

Merksatz:

Bei Verdacht zuerst stoppen,
prüfen
und melden.

Wenn Zugangsdaten eingegeben wurden

Sofortmaßnahmen:

Passwort ändern
MFA-Sitzungen prüfen
aktive Sitzungen beenden
IT informieren
Konto-Logs prüfen
Weiterleitungsregeln prüfen
verdächtige Geräte prüfen
Tokens widerrufen
betroffene Dienste prüfen
weitere Benutzer warnen

Merksatz:

Nach Phishing zählt schnelle Reaktion.

Wenn ein Anhang geöffnet wurde

Sofortmaßnahmen:

Gerät vom Netzwerk trennen
IT informieren
Datei nicht weiter öffnen
Zeitpunkt dokumentieren
E-Mail sichern
EDR oder Antivirus prüfen
Logs sichern
betroffene Konten prüfen
keine weiteren Systeme nutzen,
bis Bewertung erfolgt

Merksatz:

Nach verdächtigem Anhang Gerät schnell isolieren.

Kontoübernahme erkennen

Anzeichen:

unbekannte Loginorte
neue Weiterleitungsregeln
gelesene E-Mails ohne Benutzeraktion
gesendete Phishing-Mails
Passwortänderung
MFA-Änderung
neue Geräte
ungewöhnliche Dateienzugriffe
Rollenänderungen
verdächtige API-Aktivität

Merksatz:

Kontoübernahme zeigt sich oft in Logs und ungewöhnlichen Kontoeinstellungen.

E-Mail-Weiterleitungsregel als Risiko

Nach Kontoübernahme legen Angreifer oft Weiterleitungsregeln an.

Zweck:

```
E-Mails mitlesen
Rechnungen abfangen
Antworten verstecken
weitere Angriffe vorbereiten
```

Prüfen:

```
unbekannte Weiterleitungen
versteckte Regeln
Regeln zum Löschen
Regeln zum Verschieben
externe Empfänger
```

Merksatz:

```
Nach Kontoübernahme immer Weiterleitungsregeln prüfen.
```

Schutz durch Conditional Access

Conditional Access kann Logins abhängig machen von:

```
Standort
Gerät
MFA
Risiko
Benutzergruppe
Anwendung
Netzwerk
Gerätezustand
```

Beispiele:

```
Adminzugriff nur mit MFA

Zugriff aus unbekanntem Land blockieren
```

Zugriff nur von verwalteten Geräten

Merksatz:

Conditional Access erschwert missbräuchliche Logins.

Schutz durch Schulung

Benutzer sollten wissen:

wie Phishing aussieht
wie man Links prüft
wie man Anhänge bewertet
wie man verdächtige Nachrichten meldet
warum MFA-Anfragen nicht blind bestätigt werden
warum Passwörter eindeutig sein müssen
warum Zahlungsprozesse eingehalten werden

Merksatz:

Schulung macht Benutzer zu aktiven Schutzfaktoren.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was ist Phishing?
- Was ist Spear Phishing?
- Was ist Whaling?
- Was ist Social Engineering?
- Was ist CEO-Fraud?
- Was ist Business E-Mail Compromise?
- Was ist Smishing?
- Was ist Vishing?
- Was ist Credential Harvesting?
- Was ist Session Hijacking?
- Was ist MFA-Push-Fatigue?

- Was ist SIM-Swapping?
- Was ist Pretexting?
- Was ist Tailgating?
- Was ist Shoulder Surfing?
- Was ist Credential Stuffing?
- Was ist Password Spraying?
- Welche Merkmale können auf Phishing hinweisen?
- Was machen SPF, DKIM und DMARC?
- Wie reagiert man auf eine verdächtige Phishing-Mail?
- Warum sind Passwortmanager sinnvoll?

Typische Prüfungsfallen

Phishing ist nicht nur E-Mail.

Social Engineering ist nicht rein technisch.

Spear Phishing ist gezielt.

Whaling betrifft besonders wichtige Personen.

Smishing läuft über SMS.

Vishing läuft über Telefon.

CEO-Fraud nutzt Autorität.

BEC nutzt geschäftliche E-Mail-Kommunikation.

Anzeigename einer E-Mail beweist nichts.

HTTPS allein beweist nicht,
dass die Seite echt ist.

MFA ist wichtig,
aber nicht unfehlbar.

Unerwartete MFA-Anfragen nicht bestätigen.

Credential Stuffing nutzt geleakte Passwörter.

Password Spraying probiert wenige Passwörter bei vielen Konten.

Passwort-Wiederverwendung ist gefährlich.

SPF,
DKIM
und DMARC helfen gegen Spoofing,
verhindern aber nicht jedes Phishing.

Verdächtige Nachrichten melden,
nicht ignorieren.

Nach Kontoübernahme Weiterleitungsregeln prüfen.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Phishing	Täuschung zur Preisgabe vertraulicher Daten
Smishing	Phishing per SMS
Vishing	Phishing per Telefon
Quishing	Phishing über QR-Code
Spear Phishing	gezieltes Phishing
Whaling	Phishing gegen wichtige Personen
CEO-Fraud	Betrug durch angebliche Chef-Anweisung
BEC	Business E-Mail Compromise
Fake Login	gefälschte Anmeldeseite
Credential Harvesting	Sammeln von Zugangsdaten
Session Hijacking	Übernahme einer laufenden Sitzung
MFA-Bypass	Umgehung oder Missbrauch von MFA
MFA-Push-Fatigue	viele MFA-Anfragen zur Ermüdung
SIM-Swapping	Übernahme einer Mobilfunknummer
Social Engineering	Manipulation von Menschen
Pretexting	erfundene glaubwürdige Geschichte

Begriff	Kurze Erklärung
Baiting	Köder zur Täuschung
Tailgating	unberechtigtes Folgen durch Zutritt
Shoulder Surfing	Beobachten von Eingaben
Dumpster Diving	Informationssuche im Müll
Account Takeover	Kontoübernahme
Brute Force	systematisches Ausprobieren
Credential Stuffing	Nutzung geleakter Zugangsdaten
Password Spraying	wenige Passwörter gegen viele Konten
Passwortmanager	Verwaltung starker eindeutiger Passwörter
Account Lockout	Kontosperre nach Fehlversuchen
Rate Limiting	Begrenzung von Anfragen
Captcha	Mensch-Maschine-Prüfung
SPF	Prüfung erlaubter Mailserver
DKIM	kryptografische E-Mail-Signatur
DMARC	Richtlinie für SPF/DKIM-Ergebnisse
Conditional Access	Zugriff abhängig von Bedingungen

IHK-sichere Kurzformulierung

Phishing ist eine Form des Social Engineerings, bei der Angreifer Benutzer durch Täuschung dazu bringen, vertrauliche Informationen preiszugeben, Links anzuklicken, Anhänge zu öffnen oder gefährliche Aktionen auszuführen. Spear Phishing ist gezieltes Phishing, Whaling richtet sich gegen besonders wichtige Personen, Smishing erfolgt per SMS und Vishing per Telefon. Identitätsangriffe wie Credential Stuffing, Password Spraying, Brute Force, Session Hijacking und Kontoübernahmen zielen auf Benutzerkonten und Zugänge. Schutzmaßnahmen sind MFA, starke eindeutige Passwörter, Passwortmanager, Spam- und Malwarefilter, SPF, DKIM, DMARC, Conditional Access, Schulungen, klare Meldewege, Vier-Augen-Prinzip und schnelle Reaktion bei verdächtigen Vorfällen.

Merksätze

Phishing täuscht Benutzer.

Social Engineering manipuliert Menschen.

Phishing ist nicht nur E-Mail.

Smishing = SMS-Phishing.

Vishing = Telefon-Phishing.

Quishing = QR-Code-Phishing.

Spear Phishing ist gezielt.

Whaling trifft wichtige Personen.

CEO-Fraud nutzt Autorität.

BEC nutzt geschäftliche E-Mails.

Fake Login stiehlt Zugangsdaten.

Credential Harvesting sammelt Zugangsdaten.

Session Hijacking übernimmt Sitzungen.

MFA ist wichtig,
aber nicht unfehlbar.

Unerwartete MFA-Anfragen niemals bestätigen.

SIM-Swapping gefährdet SMS-MFA.

Pretexting nutzt erfundene Rollen.

Baiting nutzt Köder.

Tailgating umgeht Zutrittskontrolle.

Shoulder Surfing nutzt Beobachtung.

Dumpster Diving nutzt weggeworfene Informationen.

Identitätsangriffe zielen auf Konten.

Account Takeover ist Kontoübernahme.

Brute Force probiert systematisch.

Credential Stuffing nutzt geleakte Zugangsdaten.

Password Spraying verteilt wenige Passwörter auf viele Konten.

Passwörter nicht wiederverwenden.

Passwortmanager nutzen.

Rate Limiting bremst Angriffe.

Captcha ersetzt keine sichere Anmeldung.

Anzeigename beweist nichts.

Links immer auf echte Domain prüfen.

Anhänge kritisch prüfen.

SPF prüft erlaubte Mailserver.

DKIM signiert E-Mails.

DMARC legt Richtlinien fest.

Technik und Schulung gemeinsam schützen.

Verdächtige Nachrichten melden.

Nach Phishing schnell reagieren.

Nach Kontoübernahme Weiterleitungsregeln prüfen.