Name: _____ Datum: _____ Punkte: _____

Phishing-Angriffe und Social Engineering

Spear-Phishing, Whaling-Betrug, die Protokolle SPF/DKIM/DMARC, Absender-Spoofing und Sicherheitsschulungen für Mitarbeiter.

LERNÜBERSICHT PHISHING-ANGRIFFE

GESICHERT
DATENVERSCHLÜSSELUNG
256-Bit-AES-Standard

KONFORM
GLOBALE STANDARDS
Rahmenwerke DSGVO (GDPR) und CCPA

ZERO-TRUST
ZUGRIFFSRICHTLINIE
Mehr-Faktor-Authentifizierung

Willkommen! Dieses Aktivitätspaket führt Sie durch Phishing-Angriffe und Social Engineering. Sie lernen Spear-Phishing, Whaling, Domain-Spoofing, die Protokolle SPF/DKIM/DMARC, Linksicherheit und Sensibilisierungsschulungen für Mitarbeitende kennen.

KONTROLLPUNKTE DES ARBEITSBLATTS

- [ ] **Teil 1-4: Cybersicherheit und Bedrohungsabwehr beherrschen.**
- [ ] **Teil 5-7: Kreuzworträtsel und Suchsel lösen.**
- [ ] **Teil 8-9: Fallstudien und Chiffre-Aufgabe lösen.**
- [ ] **Teil 10: Seiten mit grundlegenden und fortgeschrittenen häufigen Fragen durchgehen.**
- [ ] **Teil 11: 10 interessante Fakten aus der Praxis entdecken.**
- [ ] **Bonus: Herausforderung Schnell denken.**

Cybersicherheits-Leitfaden von VPN.com öffnen

URL: https://www.vpn.com/de/cybersicherheit/phishing-angriffe/

Ihr Lernfahrplan: Abwehr von Phishing

- Gängige Phishing-, Vishing- und Support-Pop-up-Betrugsmaschen erkennen.
- Verfahren zur Bestätigung von Transaktionen über einen separaten Kanal (Out-of-Band) einführen.
- Konfigurieren Sie SPF-, DKIM- und DMARC-Regeln, um gefälschte Domains zu blockieren.

ANLEITUNG ZUM LEITFADEN PHISHING-ANGRIFFE

Beantworten Sie die Auswahlaufgaben und Richtig/Falsch-Fragen, vervollständigen Sie die Lückensätze mithilfe der Wortliste, ordnen Sie die Definitionen zu und lösen Sie das Kreuzworträtsel und das Suchsel. Wenden Sie Ihr Wissen in folgenden Bereichen an: E-Mail-Authentifizierung. Zum Schluss folgt die Bonusaufgabe Schnell denken.

PHISHING-ANGRIFFE UND SOCIAL ENGINEERING (EINFÜHRUNG)

Phishing-Angriffe nutzen gezielte Nachrichten, Whaling-Betrug und Domain-Spoofing, um Anmeldedaten von Nutzern abzugreifen. Zum Schutz von Unternehmenssystemen müssen SPF-, DKIM- und DMARC-Regeln am Gateway eingesetzt werden, ergänzt durch Freigabeschritte über einen separaten Kanal.

LESEN SIE JEDEN KONTROLLPUNKT SORGFÄLTIG UND WÄHLEN ODER SCHREIBEN SIE DIE RICHTIGE ANTWORT.

Kontrollpunkt 1: Auswahlaufgaben

1 **1. Was ist Spear-Phishing?**

- A. Eine gezielte Phishing-E-Mail, die auf eine bestimmte Person oder Organisation zugeschnitten ist
- B. Eine breit gestreute Massen-E-Mail an Millionen zufälliger Adressen
- C. Ein Netzwerkangriff, der Webserver mit Datenverkehr überflutet
- D. Eine Technik zum Auslesen von Datenbanken, die auf Benutzerdatensätze abzielt

2 **2. Mit welchem Protokoll kann eine Domain ihre autorisierten Absender-IP-Adressen im DNS veröffentlichen, um Spoofing zu bekämpfen?**

- A. SPF
- B. DKIM
- C. DMARC
- D. HTTPS

3 **3. Was ist ein Whaling-Angriff?**

- A. Eine Phishing-Kampagne, die gezielt auf hochrangige Führungskräfte von Unternehmen abzielt
- B. Ein SQL-Injection-Angriff auf Datenbanksicherungen
- C. Ein physischer Diebstahl von Routern des lokalen Netzwerks
- D. Ein automatisierter Brute-Force-Scan mittels Credential Stuffing

4 **4. Was macht DKIM?**

- A. Fügt E-Mails eine kryptografische Signatur hinzu, um die Echtheit des Absenders zu bestätigen
- B. Blockiert eingehenden Netzwerkpaketverkehr an der Firewall
- C. Verschlüsselt Datenbank-Speichervolumes im Ruhezustand
- D. Durchsucht E-Mail-Anhänge nach signaturbasierter Malware

5 **5. Welche Rolle spielt DMARC?**

- A. Vorgabe für empfangende Mailserver, wie mit fehlgeschlagenen SPF/DKIM-Prüfungen umzugehen ist
- B. Entschlüsseln von Systempasswörtern mithilfe vorberechneter Rainbow Tables
- C. Komprimieren von E-Mail-Anhängen vor der Zustellung
- D. Konfigurieren von Zugriffsrechten für das Netzwerk-Routing

Kontrollpunkt 2: Richtig oder falsch

6 Frage 6

6. Spear-Phishing beruht auf allgemeinen Massen-E-Mails, die an Millionen zufälliger Adressen gesendet werden.

- ○ Richtig
- ○ Falsch

7 Frage 7

7. DMARC-Richtlinien können Mailserver anweisen, nicht autorisierte gefälschte Nachrichten abzulehnen.

- ○ Richtig
- ○ Falsch

8 Frage 8

8. Die SPF-Prüfung erfolgt durch Validierung der kryptografischen Signatur des E-Mail-Inhalts.

- ○ Richtig
- ○ Falsch

9 Frage 9

9. Whaling-Angriffe zielen auf untergeordnete Unternehmensadministratoren ab, um an Datenbankdateien zu gelangen.

- ○ Richtig
- ○ Falsch

10 Frage 10

10. Die Überprüfung von Zahlungsanforderungen über einen separaten Kanal hilft, Überweisungsbetrug zu verhindern.

- ○ Richtig
- ○ Falsch

Kontrollpunkt 3: Schlüsselbegriffe einsetzen

Lesen Sie jeden der folgenden Sätze und füllen Sie die Lücke mit dem richtigen Begriff aus der Wortliste.

1. Wer einen bestimmten Mitarbeiter mit personalisierten Informationen ins Visier nimmt, betreibt Phishing vom Typ _____ .

2. Das Fälschen eines E-Mail-Headers, damit Nachrichten seriös wirken, nennt man _____ des Absenders.

3. Die DNS-Liste der autorisierten Mailserver-IPs heißt _____ .

4. Der E-Mail-Signaturstandard zur Verifizierung des Absenders ist _____ .

5. Richtlinien zur Ablehnung von Nachrichten mit fehlgeschlagener SPF/DKIM-Prüfung legt man mit _____ fest.

6. Eine Phishing-Kampagne gegen Führungskräfte der C-Ebene nennt man _____ .

WORTSCHATZ-WORTBANK

DKIM DMARC PHISHING SPEAR SPF-EINTRAG SPOOFING VISHING WHALING

Schreiben Sie Ihre Antworten hier:

1.
2.
3.
4.
5.
6.

Kontrollpunkt 4: Zuordnung von Sicherheits-Begriffen

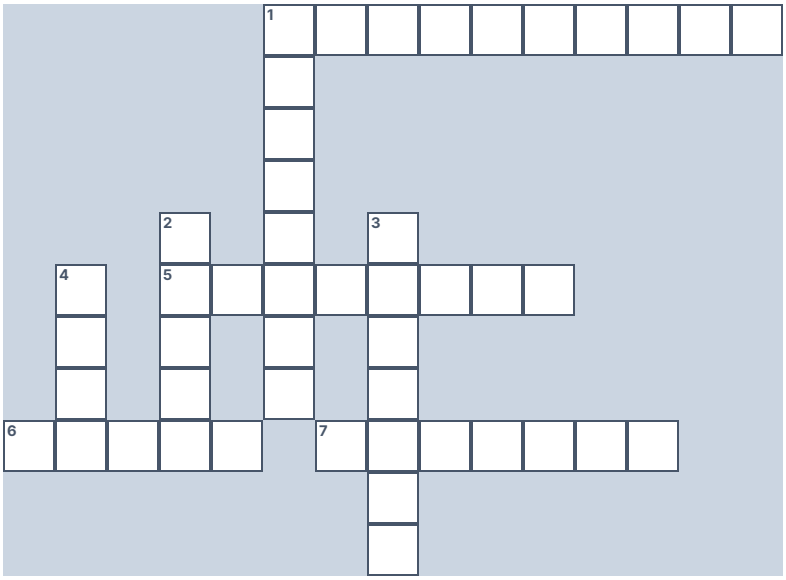
DEFINITIONEN ZUORDNEN

Ordnen Sie jeden Fachbegriff links der richtigen Definition rechts zu, indem Sie den passenden Buchstaben (A–H) in das ausfüllbare Eingabefeld schreiben.

☐	1. SPEAR	A	Sprachbasierte Betrugsanrufe.
☐	2. SPOOFING	B	Zielt auf Führungskräfte der obersten Ebene ab.
☐	3. SPF	C	Anweisungen zur Richtlinie für Ablehnung.
☐	4. DKIM	D	Im DNS hinterlegte autorisierte Absender-IPs.
☐	5. DMARC	E	Social-Engineering-E-Mail.
☐	6. WHALING	F	Personalisierte, gezielte E-Mail.
☐	7. PHISHING	G	Fälschen der Absender-E-Mail-Adresse.
☐	8. VISHING	H	Kryptografische Signatur in E-Mails.

Kontrollpunkt 5: Kreuzworträtsel

Lösen Sie das Kreuzworträtsel, indem Sie Buchstaben in die aktiven weißen Felder eingeben. Die Zahlen entsprechen den Hinweisen unten.



WAAGERECHT

1. DNS-Liste autorisierter Absender-IPs. (10)

5. Social Engineering per E-Mail. (8)

6. Richtlinie mit Anweisungen zur Ablehnung. (5)

7. Betrügerische Sprachanrufe. (7)

SENKRECHT

1. Fälschen der Absenderadresse einer E-Mail. (8)

2. Personalisierte, gezielte E-Mail. (5)

3. Angriff auf Führungskräfte der C-Ebene. (7)

4. Kryptografische Signatur in E-Mails. (4)

Kontrollpunkt 5, Alternative: Barrierefreie Kreuzworträtsel-Hinweise

Nutzer von Screenreadern und Tastatur können die Kreuzworträtsel-Antworten direkt in die Textfelder unten eingeben.

WAAGERECHT

1 waagerecht: DNS-Liste autorisierter Absender-IPs. (10 Buchstaben):

5 waagerecht: Social Engineering per E-Mail. (8 Buchstaben):

6 waagerecht: Richtlinie mit Anweisungen zur Ablehnung. (5 Buchstaben):

7 waagerecht: Betrügerische Sprachanrufe. (7 Buchstaben):

SENKRECHT

1 senkrecht: Fälschen der Absenderadresse einer E-Mail. (8 Buchstaben):

2 senkrecht: Personalisierte, gezielte E-Mail. (5 Buchstaben):

3 senkrecht: Angriff auf Führungskräfte der C-Ebene. (7 Buchstaben):

4 senkrecht: Kryptografische Signatur in E-Mails. (4 Buchstaben):

Kontrollpunkt 6: Suchsel

Finden Sie die 8 wichtigen Fachbegriffe, die im Gitter unten versteckt sind. Die Wörter können waagerecht, senkrecht oder diagonal verlaufen.

U S T E L J B A B C P X L K Y
K X T K D Q M J W D I N N K Q
P G M M Q R S T T H G C S Q O
H S G N I H S I V B A W D S Z
G V C Z W S F K H Z D L N D Q
N M X P C P U S B R A Z I N D
I I K A D F O D P F A H I N D
H K R Q M E E I R O Z E S F G
S D Q V F I A A Q O O N P P T
I X Q K R N D U S D N F Y S B
H F S X W T M J A R Z Y I Y L
P G I M R R A J M L T O H N Q
Q H Z A O A R V G U B Y R Y G
B H L Z G G C J O P N W C M Z
Y G Y O W U K V P B N V T M G

WORTSCHATZ-WORTLISTE

SPEAR SPOOFING SPFEINTRAG DKIM DMARC WHALING PHISHING VISHING

Kontrollpunkt 6, Alternative: Barrierefreie Begriffszuordnung

Ordnen Sie jeden der 8 Fachbegriffe aus dem Suchrätsel der richtigen Definition zu, indem Sie den Buchstaben (A–H) in die Lücke schreiben.

FACHBEGRIFFE

- **A. SPEAR**
- **B. SPOOFING**
- **C. SPFEINTRAG**
- **D. DKIM**
- **E. DMARC**
- **F. WHALING**
- **G. PHISHING**
- **H. VISHING**

DEFINITIONEN UND ZUORDNUNGSFELDER

1. Fälschen der Absenderadresse einer E-Mail.
2. Personalisierte, gezielte E-Mail.
3. Betrügerische Sprachanrufe.
4. DNS-Liste autorisierter Absender-IPs.
5. Social Engineering per E-Mail.
6. Richtlinie mit Anweisungen zur Ablehnung.
7. Kryptografische Signatur in E-Mails.
8. Angriff auf Führungskräfte der C-Ebene.

Kontrollpunkt 7: Buchstabensalat

Bringen Sie die Buchstaben unten in die richtige Reihenfolge, um zentrale Begriffe der Cybersicherheit aufzudecken. Schreiben Sie Ihre Antworten in die vorgesehenen Eingabefelder.

1. **AESRP** _____
2. **AESPIGTRNF** _____
3. **ADCRM** _____
4. **SNGIHPHI** _____
5. **FIPGOSNO** _____
6. **IMDK** _____
7. **WNIGHLA** _____
8. **IHGVNIS** _____

Bonusaufgabe: Schnell denken

3 ANTWORTEN PRO KATEGORIE. WER DIE LISTE ZUERST VOLLSTÄNDIG AUSFÜLLT, GEWINNT.

1	Geräte, die gehackt werden können			
2	Anzeichen einer Phishing-E-Mail			
3	Anzeichen, dass ein Computer infiziert ist			
4	Wörter, die falsche Dringlichkeit erzeugen			
5	Möglichkeiten, einen Absender zu überprüfen			
6	Personen, die Sie um IT-Hilfe bitten können			
7	Dinge, von denen Sie ein Backup machen			
8	Fische oder Meerestiere, die Sie kennen			
9	Unternehmen, als die sich Betrüger ausgeben			
10	Sichere Gewohnheiten, mit denen Sie heute beginnen können			
11	Dinge, die nach dem Klick auf einen gefälschten Link zu tun sind			
12	Dinge, die nach einem Datenleck zu tun sind			
13	Kanäle, über die Phishing stattfindet			
14	Dinge, die Sie niemals per E-Mail senden			
15	Möglichkeiten, Ihre Konten zu schützen			

Kontrollpunkt 8: Fallstudien zur Cybersicherheit

Wenden Sie die erlernten Konzepte an, um die folgenden praxisnahen Szenarien zu lösen.

FALLSTUDIE 1: BEHEBUNG EINES WHALING-ANGRIFFS AUF DIE FÜHRUNGSEBENE



Szenario: Ein Finanzvorstand (CFO) erhält eine stark personalisierte E-Mail, die angeblich vom CEO stammt und eine schnelle Überweisung von $50,000 zum Abschluss eines vertraulichen Domainkaufs verlangt.

Diskussionsfrage: Analysieren Sie die Risiken des Marken-Spoofings und beschreiben Sie SPF/DKIM/DMARC sowie Authentifizierungskontrollen.

FALLSTUDIE 2: EINFÜHRUNG VON SPF/DKIM/DMARC-GATEWAY-RICHTLINIEN



Szenario: Ein Unternehmen besteht Sicherheitsaudits nicht, weil ausgehende Marketing-E-Mails häufig als Spam markiert werden und Hacker die Markendomain des Unternehmens aktiv fälschen.

Diskussionsfrage: Legen Sie technische und organisatorische Kontrollen fest, um die Echtheit von E-Mails zu überprüfen.

Kontrollpunkt 9: Entschlüsselung der Chiffre

Eine Fachkraft für Cybersicherheit schützt Netzwerkressourcen vor Bedrohungsakteuren im Internet. Entschlüsseln Sie mithilfe des Buchstaben-Zahlen-Schlüssels unten die Nachricht, indem Sie die passenden Buchstaben in die Lücken schreiben.

SCHLÜSSEL FÜR DIE BUCHSTABEN-ZAHLEN-VERSCHLÜSSELUNG

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

5	18	11	5	14	14	5	14		19	9	5		19	15	3	9	1	12
5	14	7	9	14	5	5	18	9	14	7		13	9	20		5	13	1	9	12
							1	21	4	9	20	19								

Entschlüsselte Nachricht:

TIPP: JEDE ZAHL STEHT FÜR DIE POSITION DIESES BUCHSTABENS IM ALPHABET (Z. B. 1 = A, 2 = B, 26 = Z).

Kontrollpunkt 10: Grundlegende häufige Fragen zur Cybersicherheit (Teil A)

Sehen Sie sich häufige Fragen und Antworten zur Abwehr von Online-Bedrohungen an.

Q1: Was ist Phishing?

Phishing ist ein Social-Engineering-Angriff, bei dem Kriminelle betrügerische Nachrichten senden, um Nutzer zur Preisgabe sensibler Daten zu verleiten.

Q2: Was ist der Unterschied zwischen Phishing und Spear-Phishing?

Phishing richtet sich mit allgemeinen Inhalten an breite Gruppen, während Spear-Phishing mit maßgeschneiderten Details auf bestimmte Opfer zielt.

Q3: Was ist Whaling?

Whaling ist ein stark zielgerichteter Phishing-Angriff auf hochrangige Führungskräfte mit Verwaltungsbefugnissen.

Q4: Was ist E-Mail-Spoofing?

E-Mail-Spoofing ist das Erstellen von E-Mails mit gefälschter Absenderadresse, um den Empfänger dazu zu bringen, der Quelle zu vertrauen.

Q5: Wie verhindert SPF Spoofing?

Es veröffentlicht im DNS eine Liste autorisierter sendender IP-Adressen, sodass empfangende Server die Herkunft der E-Mail überprüfen können. [1]

Kontrollpunkt 10: Grundlegende häufige Fragen zur Cybersicherheit (Teil B)

Sehen Sie sich häufige Fragen und Antworten zur Abwehr von Online-Bedrohungen an.

Q6: Was ist DKIM?

DomainKeys Identified Mail fügt den E-Mail-Headern eine kryptografische Signatur hinzu, die belegt, dass eine Domain die Verantwortung übernommen hat und die Nachricht nicht verändert wurde.

Q7: Wofür steht DMARC?

Domain-based Message Authentication, Reporting, and Conformance (domainbasierte Nachrichtenauthentifizierung, Berichterstattung und Konformität). [2]

Q8: Was ist eine DMARC-Richtlinie?

Eine Richtlinie, die Mailservern vorgibt, wie sie mit Nachrichten umgehen sollen, die SPF/DKIM nicht bestehen (none, quarantine oder reject). [2]

Q9: Was ist Vishing?

Telefon-Phishing, bei dem Angreifer über betrügerische Anrufe administrative oder finanzielle Daten erbeuten.

Q10: Wie helfen Link-Scanner?

Sie prüfen eingehende E-Mail-Links und schreiben sie um, um die Sicherheit der Zielwebseiten zum Zeitpunkt des Klicks zu überprüfen.

Kontrollpunkt 10: Fortgeschrittene häufige Fragen zur Sicherheit (Teil C)

Erkunden Sie fortgeschrittene technische Aspekte von Sicherheits-Frameworks, Malware-Analyse und Daten-Compliance.

Q1: Wie funktioniert ein Homographenangriff?

Angreifer registrieren Domainnamen mit ähnlich aussehenden Nicht-ASCII-Unicode-Zeichen, um eine legitime Domain optisch nachzuahmen.

Q2: Was ist eine Punycode-Darstellung?

Eine Kodierung, die Unicode-Domainnamen in ASCII-kompatible Zeichenfolgen mit dem Präfix 'xn--' umwandelt, damit DNS sie verarbeiten kann.

Q3: Warum ist 'p=reject' die sicherste DMARC-Einstellung?

Es fordert empfangende Server auf, E-Mails, die DMARC (ausgerichtetes SPF/DKIM) nicht bestehen, schon während der SMTP-Sitzung abzulehnen, und blockiert so direktes Spoofing. [2]

Q4: Wie umgehen Angreifer SPF-Regeln?

Durch Ausnutzen ähnlich aussehender Domains (Typosquatting) oder Verwenden kompromittierter Konten bei legitimen E-Mail-Diensten von Drittanbietern.

Q5: Was ist Business Email Compromise (BEC)?

Ein Betrug gegen Unternehmen, bei dem Angreifer geschäftliche E-Mail-Konten kapern oder sich als deren Inhaber ausgeben, um betrügerische Zahlungen zu veranlassen.

Kontrollpunkt 10: Fortgeschrittene häufige Fragen zur Sicherheit (Teil D)

Erkunden Sie fortgeschrittene technische Aspekte von Sicherheits-Frameworks, Malware-Analyse und Daten-Compliance.

Q6: Wie stoppt die Multi-Faktor-Authentifizierung Phishing?

Es erfordert zusätzliche Token (etwa Hardwareschlüssel), die sich nicht allein über nachgeahmte Landingpages stehlen lassen.

Q7: Was ist eine Landingpage zum Abgreifen von Zugangsdaten?

Ein nachgeahmtes Anmeldeportal, das eingegebene Benutzernamen, Passwörter und MFA-Codes in Echtzeit abgreifen soll.

Q8: Was ist Subdomain-Hijacking?

Ein Angreifer übernimmt einen ungenutzten DNS-Subdomain-Verweis, um unter einer vertrauenswürdigen übergeordneten Domain schädliche Phishing-Seiten zu hosten.

Q9: Wie funktioniert die Prüfung der DKIM-Ausrichtung (Alignment)?

Es prüft, ob die Domain im Header „From“ mit der Domain übereinstimmt, die die Nachricht im DKIM-Header kryptografisch signiert hat.

Q10: Welche Rolle spielt ein E-Mail-Gateway?

Filtern eingehender E-Mails, Prüfen von Links, Ausführen von Anhängen in einer Sandbox und Überprüfen der Einhaltung von SPF/DKIM/DMARC.

Teil 11: 10 Fakten und Einblicke zur Cybersicherheit aus der Praxis

Lernen Sie reale Fakten zu Sicherheitsvorfällen, Abwehrmechanismen und Compliance-Standards kennen.

1. SICHERHEITS-EINBLICK

Phishing und Spoofing waren 2025 die beim IC3 des FBI am häufigsten gemeldete Deliktart, mit 191,561 Beschwerden. [4]

2. SICHERHEITS-EINBLICK

Business Email Compromise (BEC) verursachte 2025 Verluste von über $3 Milliarden, die dem IC3 des FBI gemeldet wurden. [4]

3. SICHERHEITS-EINBLICK

Homograph-Angriffe nutzen ähnlich aussehende kyrillische Buchstaben, um Exact-Match-Markendomains im Browser optisch zu kopieren.

4. SICHERHEITS-EINBLICK

Mit „p=reject“ fordert eine Domain Empfänger auf, nicht bestandene E-Mails bereits bei der Zustellung abzulehnen, statt sie als Spam abzulegen. [2]

5. SICHERHEITS-EINBLICK

Whaling-Angriffe auf CEOs fordern häufig dringende Zahlungen für vertrauliche Fusionen oder Domainkäufe.

6. SICHERHEITS-EINBLICK

Portale zum Abgreifen von Zugangsdaten kopieren echte Anmeldeseiten, sodass Opfer ihre Passwörter direkt in das Formular des Angreifers eingeben.

7. SICHERHEITS-EINBLICK

Die gemeinsame Phishing-Empfehlung der CISA rät zu Schulungen der Benutzer zusätzlich zu DMARC, SPF, DKIM und phishingresistenter MFA. [3]

8. SICHERHEITS-EINBLICK

Die SPF-Auswertung ist auf 10 Begriffe mit DNS-Abfragen begrenzt; wird das Limit überschritten, lautet das Ergebnis 'permerror'. [1]

9. SICHERHEITS-EINBLICK

FIDO2-Hardware-Sicherheitsschlüssel bieten kryptografisch gestützten Schutz vor dem Abgreifen von Zugangsdaten aus der Ferne.

10. SICHERHEITS-EINBLICK

Phishing ist einer der häufigsten Wege, auf denen Angreifer zuerst in eine Organisation eindringen, weshalb regelmäßige Sensibilisierungsschulungen eine wirksame Abwehr sind.

Technische Referenzen und Quellen

Der Lernleitfaden und die interaktiven Rätsel wurden aus globalen Standards von NIST und OWASP sowie aus Datenschutz-Compliance-Standards zusammengestellt.

WISSENSCHAFTLICHE UND FACHLICHE QUELLEN

[1] IETF. (2014). RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1.

https://www.rfc-editor.org/rfc/rfc7208.html

[2] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).

https://www.rfc-editor.org/rfc/rfc7489.html

[3] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[4] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

Lösungsschlüssel: Kontrollpunkt 1 – Auswahlaufgaben

1 Frage 1

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Was ist Spear-Phishing? → Eine gezielte Phishing-E-Mail, die auf eine bestimmte Person oder Organisation zugeschnitten ist

2 Frage 2

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

SPF veröffentlicht die autorisierten Absender-Hosts einer Domain im DNS, damit Empfänger den Envelope-Absender prüfen können.

3 Frage 3

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Was ist ein Whaling-Angriff? → Eine Phishing-Kampagne, die gezielt auf hochrangige Führungskräfte von Unternehmen abzielt

4 Frage 4

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Was macht DKIM? → Fügt E-Mails eine kryptografische Signatur hinzu, um die Echtheit des Absenders zu bestätigen

5 Frage 5

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Welche Rolle spielt DMARC? → Vorgabe für empfangende Mailserver, wie mit fehlgeschlagenen SPF/DKIM-Prüfungen umzugehen ist

Lösungsschlüssel: Kontrollpunkt 2 – Richtig oder Falsch

6 Frage 6

Richtige Antwort: Falsch

HINWEIS FÜR LEHRKRÄFTE

Falsch: Spear-Phishing ist auf bestimmte Personen zugeschnitten, anders als allgemeines Massen-Phishing.

7 Frage 7

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

DMARC-Richtlinien können Mailserver anweisen, nicht autorisierte gefälschte Nachrichten abzulehnen.

8 Frage 8

Richtige Antwort: Falsch

HINWEIS FÜR LEHRKRÄFTE

Falsch: SPF prüft die sendende IP anhand des DNS; DKIM ist das Verfahren, das eine kryptografische Signatur überprüft.

9 Frage 9

Richtige Antwort: Falsch

HINWEIS FÜR LEHRKRÄFTE

Falsch: Whaling zielt auf hochrangige Führungskräfte ab, die Zahlungen freigeben und auf sensible Daten zugreifen können.

10 Frage 10

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

Richtig: Die Bestätigung von Zahlungsanforderungen über einen separaten, bekannten Kanal hilft, Überweisungsbetrug zu verhindern.

Vokabelschlüssel und Bewertungsraster

Bewertungsraster für Lehrkräfte: Vergeben Sie 1 Punkt für jede richtige Zuordnung (insgesamt 8 Punkte) und jeden Kontextbegriff (insgesamt 6 Punkte).

KONTROLLPUNKT 4: LÖSUNG BEGRIFFSZUORDNUNG

F 1. SPEAR	G 2. SPOOFING	D 3. SPF	H 4. DKIM
C 5. DMARC	B 6. WHALING	E 7. PHISHING	A 8. VISHING

KONTROLLPUNKT 3: LÖSUNG SCHLÜSSELBEGRIFFE

1 SPEAR	2 SPOOFING	3 SPF-EINTRAG	4 DKIM
5 DMARC	6 WHALING		

KONTROLLPUNKT 6, ALTERNATIVE: LÖSUNG WORTZUORDNUNG

1 B – SPOOFING	2 A – SPEAR	3 H – VISHING	4 C – SPFEINTRAG
5 G – PHISHING	6 E – DMARC	7 D – DKIM	8 F – WHALING

DISKUSSIONSHINWEISE FÜR LEHRKRÄFTE

Schlüsselbegriffe:
Prüfen Sie, ob die Lernenden SPEAR, SPOOFING und SPF in eigenen Worten erklären und jeweils ein Beispiel nennen können.

Fallstudien:
Bitten Sie die Lernenden, ihre Empfehlungen mit Fakten aus dem Arbeitsblatt statt mit Vermutungen zu begründen.

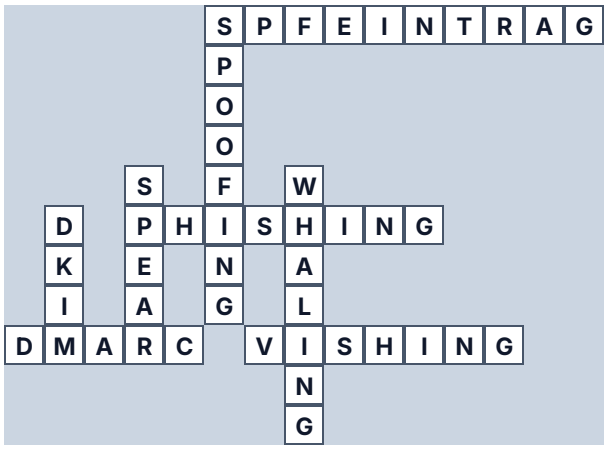
Quellenbewertung:
Lassen Sie die Lernenden mindestens eine Aussage anhand der Quellen des Arbeitsblatts prüfen und besprechen Sie, warum sich Zahlen, Preise und Regeln mit der Zeit ändern können.

Rätsellösungen und Hinweise für Lehrkräfte

LÖSUNG DES SUCHSELS

U	S	T	E	L	J	B	A	B	C	P	X	L	K	Y
K	X	T	K	D	Q	M	J	W	D	I	N	N	K	Q
P	G	M	M	Q	R	S	T	T	H	G	C	S	Q	O
H	S	G	N	I	H	S	I	V	B	A	W	D	S	Z
G	V	C	Z	W	S	F	K	H	Z	D	L	N	D	Q
N	M	X	P	C	P	U	S	B	R	A	Z	I	N	D
I	I	K	A	D	F	O	D	P	F	A	H	I	N	D
H	K	R	Q	M	E	E	I	R	O	Z	E	S	F	G
S	D	Q	V	F	I	A	A	Q	O	O	N	P	P	T
I	X	Q	K	R	N	D	U	S	D	N	F	Y	S	B
H	F	S	X	W	T	M	J	A	R	Z	Y	I	Y	L
P	G	I	M	R	R	A	J	M	L	T	O	H	N	Q
Q	H	Z	A	O	A	R	V	G	U	B	Y	R	Y	G
B	H	L	Z	G	G	C	J	O	P	N	W	C	M	Z
Y	G	Y	O	W	U	K	V	P	B	N	V	T	M	G

KREUZWORTRÄTSEL-LÖSUNG



LEITFADEN FÜR LEHRKRÄFTE ZU DEN KREUZWORTRÄTSEL-LÖSUNGEN

WAAGERECHT

1 waagerecht: SPFEINTRAG DNS-Liste autorisierter Absender-IPs. (10 Buchstaben)

5 waagerecht: PHISHING Social Engineering per E-Mail. (8 Buchstaben)

6 waagerecht: DMARC Richtlinie mit Anweisungen zur Ablehnung. (5 Buchstaben)

7 waagerecht: VISHING Betrügerische Sprachanrufe. (7 Buchstaben)

SENKRECHT

1 senkrecht: SPOOFING Fälschen der Absenderadresse einer E-Mail. (8 Buchstaben)

2 senkrecht: SPEAR Personalisierte, gezielte E-Mail. (5 Buchstaben)

3 senkrecht: WHALING Angriff auf Führungskräfte der C-Ebene. (7 Buchstaben)

4 senkrecht: DKIM Kryptografische Signatur in E-Mails. (4 Buchstaben)

Lösungsschlüssel für Buchstabensalat und Chiffre

Lösungsschlüssel für die Wort-Entwirr-Aufgabe und die Geheime Chiffre-Aufgabe.

LÖSUNGSSCHLÜSSEL BUCHSTABENSALAT

1. AESRP — SPEAR
2. AESPIGTRNF — SPFEINTRAG
3. ADCRM — DMARC
4. SNGIHPHI — PHISHING
5. FIPGOSNO — SPOOFING
6. IMDK — DKIM
7. WNIGHLA — WHALING
8. IHGVNIS — VISHING

LÖSUNGSSCHLÜSSEL ZUR GEHEIMEN CHIFFRE-AUFGABE

"ERKENNEN SIE SOCIAL ENGINEERING MIT EMAIL AUDITS"

Lösungsschlüssel zu den Fallstudien

A Fallstudie 1: Behebung eines Whaling-Angriffs auf die Führungsebene

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Eine Finanzvorständin erhält eine stark personalisierte E-Mail, die angeblich vom CEO stammt und eine schnelle Überweisung von $50,000 verlangt, um einen vertraulichen Domainkauf abzuschließen.
- Empfohlene Strategie und Lösung: Konfigurieren Sie DMARC mit der Richtlinie 'p=reject', um gefälschte Absenderdomains zu blockieren. Fügen Sie am Gateway Warnbanner für externe Absender hinzu und verlangen Sie für alle Finanztransaktionen eine mündliche Bestätigung über einen separaten Kanal (Out-of-Band).

B Fallstudie 2: Einführung von SPF/DKIM/DMARC-Gateway-Richtlinien

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Ein Unternehmen fällt bei Sicherheitsaudits durch, weil ausgehende Marketing-E-Mails häufig als Spam markiert werden und Hacker die Marken-Domain des Unternehmens aktiv fälschen (Spoofing).
- Empfohlene Strategie und Lösung: Veröffentlichen Sie einen TXT-Eintrag für SPF mit den autorisierten Absender-IPs. Konfigurieren Sie DKIM-Signaturschlüssel auf den ausgehenden Mailservern und werten Sie eingehende DMARC-XML-Berichte aus, um Missbrauch zu erkennen.