knowbe4

2026 Monat der Cybersicherheit

Strategiedossier für das Ressourcen-Kit

WOCHE 1
WOCHE 2
WOCHE 3
WOCHE 4

AUFTRAGSBESCHREIBUNG:

Monat der Cybersicherheit 2026

Ihr Auftrag, sofern Sie diesen annehmen, lautet: Vermitteln Sie Ihrem Team die benötigten Kompetenzen zum Schutz vor global agierenden Cyberkriminellen.

In diesem Jahr stehen Ihnen zahlreiche Tools, Ressourcen sowie die Mitglieder eines Elite-Teams der „Abteilung für Personalrisiken (APR)“ zur Verfügung. Als Mitglied der APR helfen Sie den Nutzerinnen und Nutzern bei einem Einsatz mit vier einwöchigen Aufträgen, bei denen jeweils eine andere Cyberbedrohung im Mittelpunkt steht.

Die Verwandlung Ihrer Belegschaft in eine an vorderster Front kämpfende Abwehrkette ist jetzt deutlich einfacher. Dafür haben wir für Sie einige kostenlose Ressourcen zusammengestellt.

In diesem Kampagnenpaket für den Monat der Cybersicherheit werden Ihre Mitarbeitenden als „Geheimagentinnen und Geheimagenten“ angeworben, die gegen Cyberkriminalität vorgehen. Neben kostenlosen Trainingsmodulen sowie dazugehörigen Postern und Dokumenten erhalten Sie vier Charakterkarten für Teammitglieder, auf denen die für die heutige Bedrohungslage benötigten Kompetenzen verkörpert werden. Die vier vorgefertigten Tabletop-Übungen können persönlich oder virtuell durchgespielt werden. Sie helfen Ihrem Team beim Aufbau von Resilienz gegenüber zukünftigen Bedrohungen.

Ihre Ressourcen

Im Kit enthalten:

Nur für Sie bestimmt

FOR YOUR EYES ONLY

- **Webinar:** So funktioniert die sichere Nutzung von KI-Tools (in englischer Sprache)
- **Whitepaper:** Schutz der hybriden Belegschaft aus Menschen und KI-Agenten in einem neuen Zeitalter
- **Vier themenbasierte Tabletop-Übungen** inkl. Dokumenten

  Online-Wochenplaner (auf Englisch), in dem alle unten aufgeführten Ressourcen für Ihre Nutzerinnen und Nutzer thematisch organisiert sind:

WOCHENPLANER

Für Ihre Agentinnen und Agenten bestimmt

Der Zugriff auf alle Kurse und Inhalte ist über die bereitgestellten Links bis zum **31. Oktober 2026** möglich.

- **sechs kostenlose interaktive Trainingsmodule oder Videomodule**
  – Smishing-Rausch (in 35 Sprachen verfügbar)
  – Ein Social-Engineering-Angriff mit Deepfake (in 35 Sprachen verfügbar)
  – Schutz von geistigem Eigentum (in 12 Sprachen verfügbar)
  – Starke Passwörter, sichere Konten (in 35 Sprachen verfügbar)
  – Audiocast „Hacking-sichere Gewohnheiten“ (in 12 Sprachen verfügbar)
  – Spiel „Das Streben nach Datenschutz“ (in 13 Sprachen verfügbar)
- **vier Charakterkarten/-poster zu den Teammitgliedern der Abteilung für Personalrisiken (APR)**

  vier Poster und Digital-Signage-Elemente zur Verinnerlichung wichtiger Konzepte

Basiswissen über die Abteilung für Personalrisiken

Agentinnen und Agenten der APR kämpfen ununterbrochen gegen Akteurinnen und Akteure mit schlechten Absichten. Daher haben wir die Rekrutierung neuer Agentinnen und Agenten so einfach wie möglich gemacht. Die bereitgestellten Inhalte lassen sich den vier Themen zuordnen, die in den vier Oktoberwochen jeweils den Schwerpunkt bilden. Sie können in jeder Woche eine oder mehrere Ressourcen aus den folgenden Trainingsformaten auswählen:

- **Videomodul oder interaktives Trainingsmodul**
- **Poster/Dokument mit Informationen**
- **Charakterkarte für APR-Teammitglieder**
- **Dokument für Tabletop-Übung**

Später gehen wir noch ausführlich auf die einzelnen Themen jeder Woche ein. Hier ist die Kurzfassung:

- **Woche 1:** Phishing und Social Engineering
- **Woche 2:** Deepfakes und sichere Nutzung von KI-Tools
- **Woche 3:** Datensicherheit und Passwörter
- **Woche 4:** Melden von Vorfällen

Eine Übersicht finden Sie in unserem Online-Wochenplaner:

WOCHENPLANER

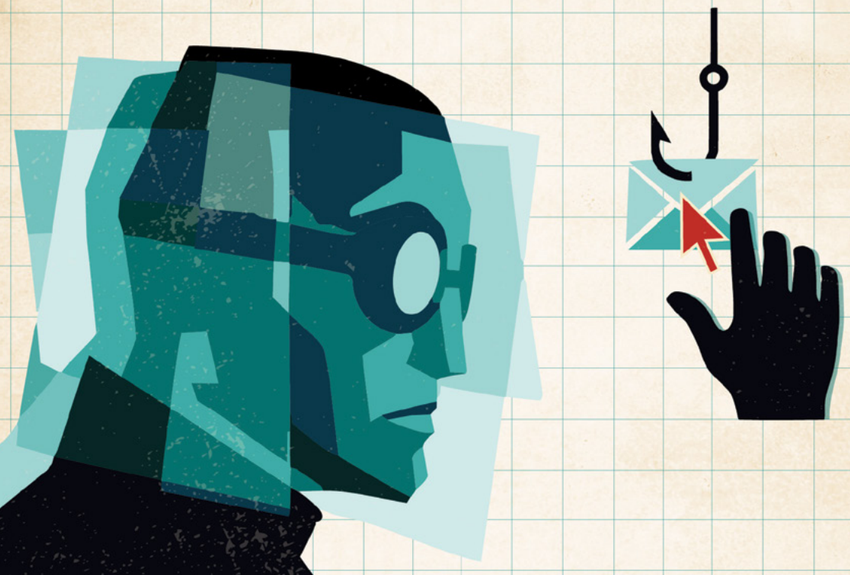
Über den Wochenplaner erhalten Sie Zugriff auf alle für Sie bereitgestellten APR-Ressourcen.

Profile der APR-Teammitglieder

Die Aufträge stehen fest. Jetzt erfahren Sie mehr über die einzelnen Teammitglieder. Informieren Sie die Nutzerinnen und Nutzer mithilfe dieser Profile über die vier Kompetenzbereiche, die sie zum Durchführen der Aufträge im Monat der Cybersicherheit beherrschen müssen. Den Rest müssen Ihre Nutzerinnen und Nutzer selbst erledigen.

PHISHING/SOCIAL ENGINEERING

GEIST



MOTTO:
VERTRAUEN,
ABER VERIFIZIEREN ...
UND DANN
ERNEUT VERIFIZIEREN

ROLLE: SPIONAGEABWEHREINHEIT

SPEZIALGEBIET: ERKENNEN VON PRETEXTING UND AUSGEFEILTEN SOCIAL-ENGINEERING-ANGRIFFEN

RATSCHLAG: WENN EINE E-MAIL EIN FALSCHES GEFÜHL DER DRINGLICHKEIT ERZEUGT, HANDELT ES SICH WAHRSCHEINLICH UM EINE FALLE.

SEITE

KI-BEDROHUNGEN/SICHERHEIT

GADGET

MOTTO:
BEREITEN SIE SICH
GUT VOR
UND BLEIBEN SIE
WACHSAM

ROLLE: TECHNOLOGIEEINHEIT

SPEZIALGEBIET: SICHERE NUTZUNG VON KI-TOOLS UND ERKENNUNG VON DEEPFAKES

RATSCHLAG: VEREINBAREN SIE MIT FAMILIEN- ODER TEAMMITGLIEDERN EIN CODEWORT, UM BEI EINEM „DRINGENDEN“ ANRUF DEREN IDENTITÄT ZU VERIFIZIEREN.

SEITE

DATENSICHERHEIT UND PASSWÖRTER

SCHLOSS UND RIEGEL

MOTTO:

[GESCHWÄRZT]

ROLLE: KRYPTOGRAPHIEEINHEIT

SPEZIALGEBIET: PASSKEYS, MFA UND VERSCHLÜSSELUNG

RATSCHLAG: VERWENDEN SIE ALS PASSWORT KEIN WORT, SONDERN EINE NUR IHNEN BEKANNTE GESCHICHTE.

MELDEN VON VORFÄLLEN

SPÄHERIN

MOTTO:

WENN ES QUAKT WIE EINE
DATENSCHUTZVERLETZUNG
UND WATSCHELT WIE EINE
DATENSCHUTZVERLETZUNG,
SOLLTEN SIE ES BESSER MELDEN

ROLLE: AUßENEINSATZ

SPEZIALGEBIET: MELDEN VON VORFÄLLEN UND PHYSISCHE SICHERHEIT

RATSCHLAG: WENN ES UM SICHERHEIT GEHT, IST MELDEN DIE RICHTIGE ENTSCHEIDUNG.

Alle an einem Tisch

Vier umfassende Übungspläne helfen Ihrem Team beim Durchspielen der Tabletop-Übungen, in denen Sicherheitskrisen simuliert werden.

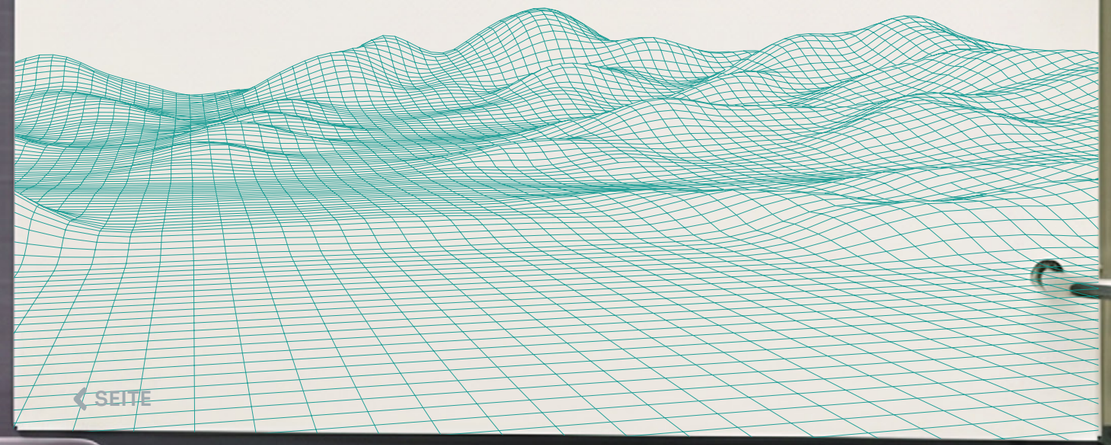
Die Übung richtet sich an alle Nutzerinnen und Nutzer, unabhängig von deren technischen Vorkenntnissen. Schwerpunkte sind die Identifizierung von Rollen, die Entscheidungsfindung und die Teamkoordination. Bei den Tabletop-Übungen müssen die in einer Checkliste enthaltenen Reaktionsmaßnahmen richtig angeordnet werden. Darüber hinaus werden realistische Szenarien mit Komplikationen simuliert. Ihre Mitarbeitenden erlernen in praktischen Übungen und strukturierten Nachbesprechungen bewährte Verfahren zum Reagieren auf Vorfälle, die funktionsübergreifende Kommunikation sowie die Anpassung von Strategien bei Sicherheitsvorfällen.

Einige sofort umsetzbare Vorschläge für diese Ressourcen:

1. Kampagne für Abteilungsleitungen:
Leiten Sie diese Ressourcen mit *strategischen Anweisungen* an die Abteilungsleitungen weiter. Schlagen Sie vor, dass die Abteilungsleitungen ein für die jeweilige Abteilung relevantes Thema auswählen, das während eines bereits feststehenden wöchentlichen Meetings in einer 30-minütigen „*Rapid Response*“-Version durchgespielt wird.

2. Hacking-Angriff für Remote-Arbeitskräfte:
Verwenden Sie die Abschnitte auf der *Szenarienkarte* der Tabletop-Übung während einer regulären Videokonferenz mit dem gesamten Team im Oktober als Fragen für ein Überraschungsquiz. Besprechen Sie die Ergebnisse in der Konferenz der darauffolgenden Woche.

3. Die Sofortnachricht *Ihr eigenes Abenteuer*:
Senden Sie an einem Tag in der Woche eine *Szenarienkarte* an den Informationssicherheitskanal bzw. Security-Awareness-Kanal Ihrer internen Messaging-App. Die Agentin bzw. der Agent, die bzw. der den Vorfall im Thread zuerst meldet und erklären kann, wo das Problem liegt und welche Maßnahmen ergriffen werden können, könnte einen thematisch passenden Preis oder ein anderes Incentive von Ihrer Organisation erhalten.



Rat von den APR-Intelligenzbestien: Kampagnenstrategien

Unser WRD-Team aus Wissenschaftlerinnen, Wissenschaftlern und Forschenden agiert vielleicht im Hintergrund, kennt sich jedoch bestens aus. Die Köpfe hinter all diesen Ressourcen wissen, dass die folgenden Strategien bei Organisationen jeder Größe funktionieren:

Wie die Führungsriege denken, wie Agentinnen und Agenten im Einsatz handeln
Das Ziel ist die Änderung riskanter Verhaltensweisen – nicht nur die Vermittlung von Informationen. Denken Sie daran, wie mächtige Geheimdienste glaubwürdige Tarnszenarien untermauern – sie sorgen dafür, dass sich jeder Aspekt anhand mehrerer Quellen bestätigen lässt. Daher erhalten Sie von uns genügend Ressourcen für einen Ansatz, bei dem mehrere Kanäle „Surround Sound“ liefern. Stellen Sie im Laufe einer Woche verschiedene Medienformate (Videos, Spiele und Dokumente) bereit, um die Sicherheitsreflexe Ihrer Mitarbeitenden durch regelmäßige Reize zu trainieren. So verwandeln Sie passive Mitarbeitende in eine starke letzte Verteidigungslinie.

Ressourcen aus allen Bereichen einbinden
Keine Geheimdienstoperation gelingt in vollständiger Isolation. Zum Aufbau einer resilienten Sicherheitskultur benötigen Sie die Unterstützung verschiedener Verbündeter, nicht nur der IT-Abteilung. Aktivieren Sie im Oktober die „schlummernden Kräfte“ in der Personal-, Rechts- und Marketingabteilung. Erklären Sie ihnen, dass auch sie eine wichtige Rolle in der APR spielen. Wenn die Botschaft von vertrauenswürdigen Peers aus der eigenen Abteilung (und nicht „dem IT-Team“) kommt, können Sie diese Kräfte viel wahrscheinlicher einbinden.

Auftragsspezifische Informationen einordnen
Überfordern Sie Ihre Agentinnen und Agenten nicht mit zu vielen auftragsspezifischen Informationen. Wenn Sie zu viele Informationen auf einmal bereitstellen, führt das eventuell dazu, dass sich ihre Mitarbeitenden einfach blind durch die Anweisungen klicken. Ermitteln Sie stattdessen die zwei oder drei wichtigsten Schwachstellen in Ihrer Organisation und konzentrieren Sie sich darauf. Mit unseren Themen für die einzelnen Wochen (Phishing, sichere Nutzung von KI-Tools, Passwörter und Melden von Vorfällen) werden Ihre Mitarbeitenden zu kompetenten Agentinnen und Agenten ausgebildet. Konzentrieren Sie sich auf den jeweiligen Auftrag, erreichen Sie das Ziel und archivieren Sie die Informationen für künftige Operationen.

Die Ressourcen in diesem Kit können selbstverständlich kein umfassendes Security-Awareness-Trainingsprogramm ersetzen. Sie lassen sich jedoch einfach bereitstellen und sprechen Ihre Mitarbeitenden besonders wirkungsvoll an.

Die einzelnen Aufträge im Detail

Auf den folgenden Seiten finden Sie den Content für jede Woche mit empfohlenen Inhalten sowie dazugehörige E-Mail-Vorlagen.

Jetzt sollten Sie bereits einige Ideen oder Strategien im Kopf haben, wie Sie den Monat bestreiten möchten. Ganz egal, wie Sie Ihre Kampagne aufziehen: Wir empfehlen, am 1. Oktober oder in der letzten Septemberwoche eine E-Mail mit grundlegenden Kampagneninformationen zu versenden.

Im Folgenden finden Sie eine Beispiel-E-Mail:

Vorgeschlagene Betreffzeile:
[START DES AUFTRAGS] **Einarbeitung bei der Abteilung für Personalrisiken**

MONAT DER CYBERSICHERHEIT 2026 | START DES AUFTRAGS

knowbe4

Abteilung für Personalrisiken: Einführung

An alle Agentinnen und Agenten,

in der risikoreichen Welt der Spionage gehören Sie zu den Hauptangriffszielen UND zu unserer stärksten Verteidigungslinie.

Nur die besten Kräfte können sich der Welle an KI-Deepfakes, ausgefeilten Social-Engineering-Angriffen und dem digitalen Schattenkrieg in unserem Netzwerk widersetzen.

Der Auftrag ist gefährlich. Handeln Sie nicht in vollständiger Isolation. Wir haben eine Reihe von Sitzungen bewilligt, um Sie auf Ihren Auftrag vorzubereiten.

DER AUFTRAG:
In diesem Oktober werden im Rahmen des Monats der Cybersicherheit alle Mitglieder unseres Teams in die Abteilung für Personalrisiken (APR) eingeführt. Während dieses Monats werden Sie jede Woche von einem Teammitglied unterrichtet, das jeweils eine kritische Säule der Sicherheitskultur darstellt.

Bereiten Sie sich auf einen vierwöchigen Einsatz vor. Sie erhalten jede Woche einen neuen Auftrag.

Das erwartet Sie in diesem Monat: **[Hier geplante Aktivitäten oder Themen einfügen. Nutzen Sie die Ideen aus diesem Leitfaden als Inspiration!]**

Wenden Sie sich bei Fragen an **[Kontaktperson, E-Mail-Adresse o. ä. einfügen]**.

Die ersten Anweisungen erhalten Sie am Montag. Wir wünschen Ihnen viel Erfolg.

WOCHE 1

Phishing und Social Engineering

Die besten Spitzel verschaffen sich nicht durch Einbruch Zugang, sondern durch ihre Redegewandtheit. In dieser Woche konzentrieren wir uns auf die subtilen Warnsignale für Social Engineering, die eventuell von technischen Filtern übersehen werden, und wie man diese erkennt.

Im Folgenden finden Sie die Ressourcen für diese Woche im Überblick:

Trainingsmodul „Smishing-Rausch“

In diesem siebenminütigen Modul werden die Gefahren von Smishing – Phishing mithilfe von Textnachrichten – vorgestellt. Die Nutzerinnen und Nutzer erfahren, wie sie es vermeiden, das nächste Opfer dieser Art von Cyberangriff zu werden.

Ihre Mitarbeitenden erfahren:

- **wie Cyberkriminelle Social Engineering in Textnachrichten einsetzen**
- **wie Smishing in der Regel aussieht**

ZUR RESSOURCE

Ressource für Tabletop-Übung - Phishing- und Whaling-Angriffe aufdecken

In dieser Tabletop-Übung lernen die Mitarbeitenden, ausgefeilte Phishing- und Whaling-Angriffe zu erkennen und darauf zu reagieren. Die Teilnehmenden analysieren einen CEO-Betrug und müssen zwischen KI-generierten Indikatoren, die falsches Vertrauen vermitteln, und tatsächlichen Warnsignalen im Verhalten unterscheiden. Entwickelt für Mitarbeitende aller Ebenen, um kritisches Denken und die Anwendung der offiziellen Verfahren Ihrer Organisation zu üben.

Zwei Ressourcen zum Herunterladen

- **Nicht anbeißen: Jeden Phishing-Versuch melden:** Poster mit einer Erinnerung an gängige Warnsignale für Phishing-E-Mails und was bei einem Phishing-Verdacht zu tun ist
- **Ihre Rolle bei der Internetsicherheit:** Infografik mit einer Erinnerung an die gängigsten Taktiken in der Cyberkriminalität sowie Abwehrmaßnahmen

RESSOURCEN FÜR WOCHE 1

Weitergabe von Content

Im Folgenden finden Sie ein Beispiel für eine E-Mail von Teammitglied „Geist“, die Sie bei der Weitergabe des Trainingsmoduls für diese Woche verwenden können:

Vorgeschlagene Betreffzeile:
[AUFTRAG FÜR WOCHE 1] **Abwehr der „Smishing“-Bedrohung**

knowbe4

Abwehr der „Smishing“-Bedrohung

MONAT DER CYBERSICHERHEIT 2026 | AUFTRAG FÜR WOCHE 1

An alle Agentinnen und Agenten,

hier ist Teammitglied **Geist**.

Unsere Mobilgeräte sind nun das Hauptziel externer Angriffe. Feindliche Kräfte lauern nicht mehr nur im Posteingang, sondern auch in Ihrer Tasche.

DER AUFTRAG:
Absolvieren Sie „Smishing-Rausch“. In diesem Trainingsmodul werden die Gefahren von Smishing – Phishing mithilfe von Textnachrichten – vorgestellt. Sie erfahren, wie Sie vermeiden, das nächste Opfer dieser Art von Cyberangriff zu werden.

Sie erfahren:

- **wie Cyberkriminelle Social Engineering in Textnachrichten einsetzen**
- **wie Smishing in der Regel aussieht**

Hier finden Sie die Ressource: (https://training.knowbe4.com/modstore/view/af44ce18-ea58-47c9-a352-fb1f277ec903)

Senden Sie bei Fragen ein Kommuniqué an **[Kontaktperson, E-Mail-Adresse o. ä. einfügen]**.

Bleiben Sie sicher. Im Verlauf des Monats erhalten Sie weitere Anweisungen.

Ende der Anweisungen.

SEITE

WOCHE 2

KI und Deepfakes

Im Fokus steht die zwielichtige Schattenseite von KI: Erläutern Sie Ihren Nutzerinnen und Nutzern, wie Akteurinnen und Akteure mit schlechten Absichten mithilfe von KI-Tools perfekte Klone und Skripte generieren. Ihre Agentinnen und Agenten müssen sich auf ihre wertvollste Ressource verlassen – kritisches Denken –, um Echt von Fake zu unterscheiden.

Im Folgenden finden Sie die Ressourcen für diese Woche im Überblick:

Videomodul „Ein Social-Engineering-Angriff mit Deepfake“

In diesem sechsminütigen Videomodul demonstrieren Mitwirkende der beliebten Security-Awareness-Serie „The Inside Man“, wie sich Cyberkriminelle mithilfe von KI-Voice-Cloning und Video-Deepfake-Technologie als Personen ausgeben können, die Sie kennen.

Ihre Mitarbeitenden erfahren:

- **wie Cyberkriminelle mithilfe von Deepfakes und Social Engineering über einfache Anfragen die Abwehrmechanismen einer Organisation aushebeln können**
- **auf welche Warnsignale sie achten müssen, um sich selbst und Ihre Organisation vor ausgefeilten Deepfake-Angriffen zu schützen**

ZUR RESSOURCE

Trainingsmodul „Schutz von geistigem Eigentum“

In diesem zehnminütigen Trainingsmodul aus der Compliance Plus-Bibliothek von KnowBe4 wird die Bedeutung von geistigem Eigentum erläutert.

Ihre Mitarbeitenden erfahren:

- **worum es sich bei geistigem Eigentum handelt und warum geistiges Eigentum so wertvoll ist**
- **wie geistiges Eigentum vor Diebstahl, Verletzung und versehentlicher Offenlegung geschützt werden kann – dabei wird auch der Bereich künstliche Intelligenz behandelt**

ZUR RESSOURCE

Ressource für Tabletop-Übung - die KI-Prompt-Challenge

In dieser Tabletop-Übung lernen die Mitarbeitenden, welche Risiken von unsicheren Prompts am Arbeitsplatz ausgehen. Die Teilnehmenden analysieren KI-Prompts und müssen entscheiden, welche sicher sind und welche sensible Daten gefährden. Entwickelt für Mitarbeitende aller Ebenen, um kritisches Denken und die Einhaltung der Richtlinien ihrer Organisation zu üben.

SEITE

Zwei Ressourcen/Digital-Signage-Elemente zum Herunterladen

- **Echt oder falsch? Deepfakes erkennen:** Poster mit einer Erinnerung, beim Erkennen von Deepfakes auf den Kontext zu achten und kritisches Denken anzuwenden
- **Phishing wird immer raffinierter: Wie KI Online-Betrug verändert:** Infografik mit einer Erläuterung, warum es durch den Einsatz von KI schwieriger wird, Phishing-Versuche zu erkennen

RESSOURCEN FÜR WOCHE 2

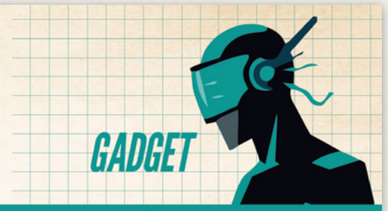
Weitergabe von Content

Im Folgenden finden Sie ein Beispiel für eine E-Mail von Teammitglied „Gadget“, die Sie beim Weitergeben der vorgeschlagenen Ressource für diese Woche verwenden können: Videomodul „Ein Social-Engineering-Angriff mit Deepfake“.

Vorgeschlagene Betreffzeile:
[AUFTRAG FÜR WOCHE 2] **Durchblick bei Deepfakes**

knowbe4

Durchblick bei Deepfakes



MONAT DER CYBERSICHERHEIT 2026 | AUFTRAG FÜR WOCHE 2

An alle Agentinnen und Agenten,

hier ist Teammitglied **Gadget** .

Es ärgert mich maßlos, wenn fortschrittliche KI-Technologie für böswillige Zwecke missbraucht wird. Akteurinnen und Akteure mit schlechten Absichten ahmen mithilfe von KI-Voice-Cloning und Deepfake-Videos Führungskräfte und Teammitglieder nach. Alle, die „geklont“ werden können, um sich dadurch Zugriff auf die gewünschten Netzwerke und Daten zu verschaffen, sind ein „legitimes“ Ziel.

DER AUFTRAG:

Absolvieren Sie „*Ein Social-Engineering-Angriff mit Deepfake*“. In diesem Videomodul demonstrieren Mitwirkende aus „The Inside Man“, wie sich Cyberkriminelle mithilfe von KI-Voice-Cloning und Deepfake-Videos als Personen ausgeben können, die Sie kennen.

Sie erfahren:

- **wie Cyberkriminelle mithilfe von Deepfakes und Social Engineering über einfache Anfragen die Abwehrmechanismen einer Organisation aushebeln können**
- **auf welche Warnsignale sie achten müssen, um sich selbst und Ihre Organisation vor ausgefeilten Deepfake-Angriffen zu schützen**

Hier finden Sie die Ressource: (https://training.knowbe4.com/modstore/view/0451be1f-0531-4724-a664-21f109be6308)

Wenden Sie sich bei Fragen an **[Kontaktperson, E-Mail-Adresse o. ä. einfügen]**.

Bereiten Sie sich gut vor und bleiben Sie wachsam. Im Verlauf des Monats erhalten Sie weitere Anweisungen.

Ende der Anweisungen.

SEITE

WOCHE 3

Datensicherheit und Passwörter

Sensible Daten sind die Währung der modernen Welt. Akteurinnen und Akteure mit schlechten Absichten setzen alles daran, an diese Daten zu gelangen. Ihre Agentinnen und Agenten müssen den Wert dieses zu schützenden Guts und die drohenden Gefahren bei einem Verlust kennen. In dieser Woche liegt der Fokus auf Passwort-Managern und MFA und wie sichergestellt werden kann, dass bei der Enttarnung von Agentinnen und Agenten die Daten der Organisation verschlüsselt bleiben.

Im Folgenden finden Sie die Ressourcen für diese Woche im Überblick:

Für Mobilgeräte optimiertes Modul „Starke Passwörter, sichere Konten“

In diesem fünfminütigen für Mobilgeräte optimierten Modul wird die Bedeutung von sicheren Passwörtern und Passphrasen für berufliche und private Geräte hervorgehoben.

Ihre Mitarbeitenden erfahren:

- **wie sie starke, sichere Passwörter erstellen und Passphrasen effektiv nutzen**
- **wie sie häufige Fehler vermeiden, die Konten angreifbar machen**
- **mehr über Best Practices für sichere Passwörter und Passphrasen**

ZUR RESSOURCE

Ressource für Tabletop-Übung - Passwörter-Raten

In dieser Tabletop-Übung nehmen Mitarbeitende die Rolle einer Hackerin oder eines Hackers ein und erfahren, wie schwache Passwörter geknackt werden. Die Teilnehmenden sehen sich Social-Media-Beiträge an und versuchen, die Passwörter der zugehörigen Personen allein aus den Informationen zu erraten, die diese online teilen. Diese Übung demonstriert, wie das übermäßige Teilen von Informationen im Internet („Oversharing“) und schwache Passwort-Praktiken dazu führen, dass Akteurinnen und Akteure mit schlechten Absichten Konten einfacher knacken können.

SEITE

WOCHE 3
WOCHE 4

Zwei Ressourcen/Digital-Signage-Elemente zum Herunterladen

- **Starke Passwörter schützen Ihren Seelenfrieden:** Poster zur Bedeutung starker Passwörter
- **Sensible Daten: Geheim halten und schützen:** Infografik über die Grundlagen zum Schutz sensibler Daten inklusive Erläuterung

RESSOURCEN FÜR WOCHE 3

Weitergabe von Content

Im Folgenden finden Sie ein Beispiel für eine E-Mail *von* Teammitglied „Schloss und Riegel“, die Sie bei der Weitergabe des Trainingsmoduls für diese Woche verwenden können:

Vorgeschlagene Betreffzeile:
[AUFTRAG FÜR WOCHE 3] **Sicherung des Tresors**

knowbe4

Sicherung des Tresors

SCHLOSS UND RIEGEL

MONAT DER CYBERSICHERHEIT 2026 | AUFTRAG FÜR WOCHE 3

An alle Agentinnen und Agenten,

hier ist Teammitglied **Schloss und Riegel**, ich melde mich aus … nun ja, diese Info liegt hinter Schloss und Riegel.

Ein Geheimnis ist nur so sicher wie sein Schloss. Deswegen geht es wieder einmal um die Grundlagen: das Erstellen sicherer Passwörter. Sie finden, das klingt nach einer Aufgabe für Azubis? Nichtsdestotrotz ist diese Aufgabe enorm wichtig. Ein Tresor bringt rein gar nichts, wenn er offen gelassen wird.

DER AUFTRAG:

Absolvieren Sie das für Mobilgeräte optimierte Trainingsmodul „Starke Passwörter, sichere Konten“. Erfahren Sie, warum Passphrasen besser als Passwörter sind und wie Sie gängige Fehler vermeiden, damit wir nicht ohne Schutz sind.

Sie erfahren:

- **wie Sie starke, sichere Passwörter erstellen und Passphrasen effektiv nutzen**
- **wie Sie häufige Fehler vermeiden, die Konten angreifbar machen**
- **mehr über Best Practices für sichere Passwörter und Passphrasen**

Hier finden Sie die Ressource: (https://training.knowbe4.com/modstore/view/c0ee0966-ff3a-4fc2-93bb-2a632811140b)

Senden Sie bei Fragen ein verschlüsseltes Kommuniqué an **[Kontaktperson, E-Mail-Adresse o. ä. einfügen]**.

Nicht vergessen: „Haltet sie geheim. Bewahrt sie sicher auf.“

S+R

WOCHE 4

Melden von Vorfällen

Bei den kritischen Geheimoperationen der Abteilung für Personalrisiken müssen stets die Ohren offen gehalten werden. Die Agentinnen und Agenten können die Aufträge nicht allein bewältigen. Sie müssen wissen, dass es wichtig ist, bei Ungereimtheiten das Team einzuschalten. In dieser Woche erfahren die Agentinnen und Agenten, bei welchen verdächtigen Warnsignalen Verstärkung angefordert werden muss.

Im Folgenden finden Sie die Ressourcen für diese Woche im Überblick:

Audiocast „Hacking-sichere Gewohnheiten: Reporting“

In diesem zweiteiligen Audiocast (aufgeteilt in ein fünf- und ein zehnminütiges Modul) wird erläutert, wie wichtig es ist, Sicherheitsbedrohungen zu melden.

Ihre Mitarbeitenden erfahren:

- **was sie vom Melden einer Bedrohung abhalten kann**
- **warum das Melden von Bedrohungen im Kampf gegen Cyberkriminalität wichtig ist**
- **mit welchem Entscheidungsfindungsprozess sie Situationen analysieren und sichere Entscheidungen treffen können**

ZU TEIL 1

ZU TEIL 2

Spiel „Das Streben nach Datenschutz“

In diesem 15-minütigen interaktiven Spiel verbessern die Nutzerinnen und Nutzer in einem spannenden Abenteuer, mit dem sie ihr Compliance-Wissen ausbauen, ihre Kenntnisse in Bezug auf internationale Datenschutzgesetze.

Ihre Mitarbeitenden erfahren:

- **wie wichtig Datenschutzvorschriften sind**
- **mehr über regionale und internationale Ansätze in Bezug auf Datenschutz**

ZUR RESSOURCE

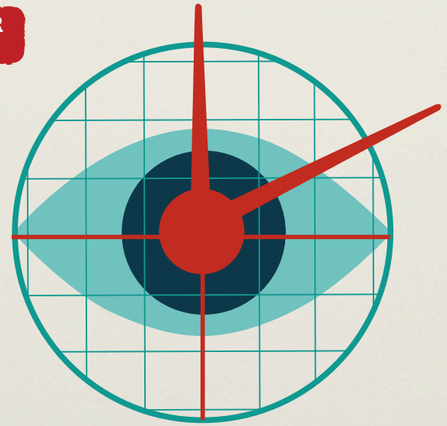
Ressource für Tabletop-Übung - Melden von Vorfällen

In dieser umfassenden Tabletop-Übung für Mitarbeitende von Organisationen wird der richtige Umgang mit Vorfällen anhand von simulierten Sicherheitskrisen gezeigt. Die Übung richtet sich an Teilnehmende, unabhängig von deren technischen Vorkenntnissen. Schwerpunkte sind die Identifizierung von Rollen, die Entscheidungsfindung und die Teamkoordination. Bei den Tabletop-Übungen müssen die in einer Checkliste enthaltenen Reaktionsmaßnahmen richtig angeordnet werden. Darüber hinaus werden realistische Szenarien mit Komplikationen simuliert. Die Teilnehmenden erlernen in praktischen Übungen und strukturierten Nachbesprechungen bewährte Verfahren zum Reagieren auf Vorfälle, die funktionsübergreifende Kommunikation sowie die Anpassung von Strategien bei Sicherheitsvorfällen.

Zwei Ressourcen/Digital-Signage-Elemente zum Herunterladen

- **Ein Bericht, gemeinsamer Schutz:** Poster zur Bedeutung der unmittelbaren Meldung verdächtiger E-Mails zum Schutz von personenbezogenen Daten, Teammitgliedern und Kundendaten
- **Phishing, physische Sicherheit und Datenschutzverletzungen – ein wichtiges Thema:** Infografik mit einer Erinnerung, warum das sofortige Melden von Sicherheitsbedenken verhindern kann, dass sich aus kleinen Problemen gravierende Vorfälle entwickeln

RESSOURCEN FÜR WOCHE 4



Weitergabe von Content

Im Folgenden finden Sie ein Beispiel für eine E-Mail von Teammitglied „Späherin“, die Sie bei der Weitergabe von Audiocast und Spiel für diese Woche verwenden können:

Vorgeschlagene Betreffzeile:
[AUFTRAG FÜR WOCHE 4] **Informationen für das Team**

knowbe4

Informationen für das Team

MONAT DER CYBERSICHERHEIT 2026 | AUFTRAG FÜR WOCHE 4

An alle Agentinnen und Agenten,

hier ist die **Späherin** mit der abschließenden Lagebesprechung.

Unser Auftrag kann nur gelingen, wenn die APR weiß, was vor Ort passiert.

Das Melden von Vorfällen hat nichts mit Verpfeifen zu tun. Durch Meldungen erhalten unsere Teams wichtige Informationen, um uns zu schützen und Akteurinnen und Akteure mit schlechten Absichten fernzuhalten.

Hier sind die vierten und letzten Anweisungen:

DER AUFTRAG:

Hören Sie sich den Audiocast „Hacking-sichere Gewohnheiten: Reporting“ an. Absolvieren Sie einen Entscheidungsfindungsprozess, in dem Sie Bedrohungen in Echtzeit analysieren.

Zu Teil 1: (https://training.knowbe4.com/modstore/view/ad7bb017-916b-442f-b1e7-4f96bf6b202f)

Spielen Sie das Spiel „Das Streben nach Datenschutz“. Reisen Sie (virtuell) um die Welt und testen Sie Ihr Wissen rund um Datensicherheit, um zu erfahren, was bei einer potenziellen Datenschutzverletzung auf dem Spiel steht.

Zu Teil 2: (https://training.knowbe4.com/modstore/view/a5ec90a8-956b-4675-8c63-c336812752e7)

Wenden Sie sich bei Fragen an **[Kontaktperson, E-Mail-Adresse o. ä. einfügen]**.

Ende der Anweisungen.

AUFTRAGSNACHBESPRECHUNG:

Denken Sie stets an die Personalrisiken

Die Führungsriege der APR ist sich sicher, dass Sie mit diesem Dossier und den bereitgestellten Ressourcen Ihrem Team die Kompetenzen und Fähigkeiten vermitteln konnten, um Cyberbedrohungen aller Art zu stoppen.

Der Aufbau und die Wahrung einer starken Sicherheitskultur ist eine fortlaufende Aufgabe. Nur mit einer Strategie, die nachhaltige Verhaltensänderungen bewirkt, bekommen Sie Risiken in Zusammenhang mit dem Faktor Mensch in den Griff und verwandeln die größte Angriffsfläche Ihrer Organisation – Ihre Mitarbeitenden – in Ihre stärkste Verteidigungslinie.

Nutzen Sie diese Ressourcen als Ergänzung zu Ihrem Security Awareness Training. Melden Sie sich bei uns, wenn Sie erfahren möchten, wie KnowBe4 Sie bei den nächsten Schritten unterstützen kann.

Folgen Sie @KnowBe4 in Social Media, wenn Sie an weiteren Ressourcen, Tipps und News zum Monat der Cybersicherheit interessiert sind. Über die Hashtags #CyberAware und #CyberSecMonth bleiben Sie im Monat der Cybersicherheit auf dem Laufenden.

knowbe4