SIEYA[at]School

SIEMENS

Methodisch-didaktische Handreichung

Cybersicherheit

Informatik

Sekundarstufe I

Inhaltsverzeichnis

1. Fachliche Ausgangslage und Relevanz

Digitale Technologien prägen heute nahezu alle Lebensbereiche – von Kommunikation und Bildung über Wirtschaft und Verwaltung bis hin zu kritischen Infrastrukturen wie Energie, Gesundheit und Verkehr. Mit dieser zunehmenden Vernetzung wächst zugleich die Angriffsfläche für Cyberattacken. Cybersicherheit – also der Schutz von Systemen, Netzwerken und Daten vor digitalen Bedrohungen – ist daher zu einer zentralen gesellschaftlichen, wirtschaftlichen und politischen Herausforderung geworden.

Cyberangriffe reichen von Phishing-Mails und Ransomware bis hin zu gezielten Attacken auf Unternehmen oder staatliche Einrichtungen. Die Folgen können gravierend sein: finanzielle Schäden, Datenverluste, Produktionsausfälle oder Gefährdungen der öffentlichen Sicherheit. Gleichzeitig entwickeln sich Angriffsmethoden kontinuierlich weiter, sodass Sicherheitsstrategien immer wieder angepasst und neue Schutzmechanismen etabliert werden müssen.

Cybersicherheit ist längst kein Nischenthema mehr, sondern betrifft alle: Privatpersonen, die ihre Geräte und Daten schützen müssen, Unternehmen, die sichere IT-Infrastrukturen benötigen und Staaten, die ihre kritischen Systeme verteidigen. Der Bereich umfasst ein breites Spektrum – von technischer Prävention (z. B. Firewalls, Verschlüsselung, Zugriffskontrollen) über organisatorische Maßnahmen (Sicherheitskonzepte, Schulungen) bis hin zu rechtlichen und ethischen Fragestellungen.

Auch im schulischen Kontext bietet das Thema vielfältige Anknüpfungspunkte: Schüler:innen lernen praxisnah, wie digitale Geräte und Netzwerke funktionieren, wo Gefahren entstehen und wie man ihnen begegnet. Dabei erwerben sie grundlegende digitale Kompetenzen wie das Erkennen von Bedrohungen, den verantwortungsvollen Umgang mit Passwörtern und Daten sowie ein kritisches Bewusstsein für Datenschutz und Privatsphäre.

Mit Blick auf die berufliche Orientierung eröffnet Cybersicherheit zahlreiche Perspektiven: IT-Sicherheitsexpert:innen, Analyst:innen für Cyberbedrohungen oder Fachkräfte für Datenschutz und IT-Compliance gehören zu stark nachgefragten Berufsprofilen. Kenntnisse im Bereich Cybersicherheit sind zudem in fast allen Berufsfeldern eine unverzichtbare Zusatzqualifikation.

Die Auseinandersetzung mit Cybersicherheit macht deutlich, wie wichtig ein reflektierter und verantwortungsvoller Umgang mit digitalen Technologien ist. Sie sensibilisiert für die Risiken einer vernetzten Welt, zeigt aber zugleich, dass Schutzmaßnahmen möglich und gestaltbar sind – und dass jede:r dazu beitragen kann, digitale Räume sicherer zu machen.

2. Verortung in den Rahmenlehrplänen des Faches Informatik (Sek I)

In den aktuellen Bildungsplänen mehrerer Bundesländer finden sich klare Anknüpfungspunkte zum Thema Cybersicherheit, insbesondere in den Fächern Informatik und Medienbildung, aber auch in Fächern mit digitalisierungs- oder gesellschaftsbezogenen Inhalten.

Im hessischen Lehrplan für Informatik in der Sekundarstufe I wird die Auseinandersetzung mit Datenschutz, Persönlichkeits- und Urheberrecht als grundlegende Kompetenz hervorgehoben. Schüler:innen sollen Gefahren für die Datensicherheit in selbst genutzten Informatiksystemen erkennen, geeignete Schutzmaßnahmen anwenden und Chancen wie Risiken der Internetnutzung kritisch reflektieren. Dazu gehört auch das Wissen um die Erhebung, Speicherung und Verwertung personenbezogener Daten in Datenbanken (Hessisches Kultusministerium, 2021).

Der bayerische Lehrplan für Informatik fordert die Lernenden dazu auf, die Chancen und Risiken der automatischen Auswertung großer Datenmengen zu beurteilen – auch in Hinblick auf gesellschaftliche

Auswirkungen. Besondere Relevanz hat hier die Reflexion des Umgangs mit persönlichen Daten im Internet sowie die Fähigkeit, eigenständig Vorkehrungen zum Schutz der Privatsphäre zu treffen (ISB, 2025).

In Mecklenburg-Vorpommern sind Inhalte zur Informatik und Medienbildung ebenfalls eng mit Cybersicherheit verknüpft. Schüler:innen sollen ihre Rolle als „Datenlieferanten" erkennen und sowohl Potenziale als auch Risiken maschineller Datenauswertung einschätzen. Gleichzeitig erwerben sie grundlegendes Wissen über Prinzipien der Datenübertragung im Internet, etwa Adressierung, Routing oder Verschlüsselungsverfahren – eine wichtige Grundlage, um Gefahrenlagen im digitalen Raum zu verstehen (Ministerium für Bildung, Wissenschaft und Kultur des Landes Mecklenburg-Vorpommern, 2019).

Der rheinlandpfälzische Lehrplan für Informatik in der Sekundarstufe I zielt auf die Sensibilisierung für einen rechtlich einwandfreien Umgang mit digitalen Informationen. Anhand von Fallstudien werden Fragen des Urheberrechts, der Nutzung personenbezogener Daten und der Kommunikationssicherheit behandelt. Zudem sollen die Schüler:innen erste Verschlüsselungsverfahren kennenlernen, um Lösungsansätze für Sicherheitsprobleme praktisch zu erproben (Ministerium für Bildung, Wissenschaft, Jugend und Kultur, o.J).

Deutlich wird, dass Cybersicherheit in den Lehrplänen auf mehreren Ebenen verankert ist:

- **Technische Ebene:** Grundwissen über Datenübertragung, Verschlüsselung und Sicherheitstechnologien.
- **Rechtliche Ebene:** Auseinandersetzung mit Datenschutz, Urheberrecht und Persönlichkeitsrechten.
- **Gesellschaftliche Ebene:** Reflexion über Chancen und Risiken von Datenverarbeitung, Big Data und digitaler Vernetzung.
- **Handlungsorientierte Ebene:** Anwendung von Schutzmaßnahmen im Alltag und verantwortungsbewusster Umgang mit Daten.

Diese Kombination verdeutlicht, dass Cybersicherheit im schulischen Kontext nicht nur technisches Wissen vermittelt, sondern auch gesellschaftliche, rechtliche und ethische Fragestellungen einschließt. Damit leistet das Thema einen wichtigen Beitrag zur Förderung von Analyse-, Urteils- und Handlungskompetenzen in einem zentralen Zukunftsfeld. In der hier skizzierten Stunde wird insbesondere die technische und die handlungsorientierte Ebene berücksichtigt.

3. Berufsfeldkunde im Kontext von „Cybersicherheit"

Fachinformatiker:in für Systemintegration

Allgemeines Berufsbild:

Fachinformatiker:innen für Systemintegration sind Expert:innen für die Planung, den Aufbau und die Wartung komplexer IT-Infrastrukturen. Sie analysieren die Anforderungen von Unternehmen oder Behörden, entwickeln passende Lösungen und setzen diese in Form von Netzwerken, Servern und Arbeitsplätzen um. Neben der Einrichtung von Hard- und Software gehört auch die kontinuierliche Betreuung und Optimierung der Systeme zu ihren Aufgaben. Treten Störungen auf, sind sie für die Fehleranalyse und -behebung zuständig und dokumentieren ihre Arbeitsschritte, um die IT-Landschaft langfristig stabil und effizient zu halten. Dabei arbeiten sie eng mit Anwender:innen, IT-Support-Teams und Softwareentwickler:innen zusammen. Der Einstieg erfolgt in der Regel über eine duale Ausbildung zum:zur Fachinformatiker:in (Schwerpunkt Systemintegration). Alternativ bieten auch Studiengänge wie Informatik oder Wirtschaftsinformatik Zugang. Über Weiterbildungen im IT-Bereich oder über Quereinstiege mit Berufserfahrung in der IT können ebenfalls Wege in dieses Berufsfeld führen.

Rolle im Kontext Cybersicherheit:

Im Bereich Cybersicherheit kommt den Fachinformatiker:innen für Systemintegration eine Schlüsselrolle zu: Sie gestalten die IT-Architektur so, dass Sicherheitsrisiken minimiert werden. Dazu richten sie Firewalls, Antivirensoftware und Zugriffsrechte ein, überwachen die Systeme auf verdächtige Aktivitäten und schulen Mitarbeitende im sicheren Umgang mit IT. Sie sind häufig die erste Anlaufstelle bei Sicherheitsvorfällen und arbeiten an der Entwicklung von Strategien, um Systeme widerstandsfähiger gegen Angriffe zu machen. Durch ihr technisches Wissen und ihren Überblick über die gesamte Systemlandschaft tragen sie entscheidend dazu bei, dass Organisationen vor Datenverlust, Sabotage oder unerlaubten Zugriffen geschützt sind.

IT-Sicherheitsanalyst:in / Cybersecurity Analyst

Allgemeines Berufsbild:

IT-Sicherheitsanalyst:innen überwachen kontinuierlich die Netzwerke und Systeme eines Unternehmens, um Sicherheitsbedrohungen frühzeitig zu erkennen. Sie nutzen spezielle Analysetools, um Datenströme auszuwerten, Schwachstellen zu identifizieren und auffällige Aktivitäten zu untersuchen. Darüber hinaus entwickeln sie Sicherheitsrichtlinien, führen Risikoanalysen durch und erstellen Notfall- sowie Wiederherstellungspläne. Ihre Arbeit umfasst sowohl die technische Ebene (z. B. Angriffserkennung, Monitoring, Incident Response) als auch die organisatorische Ebene (z. B. Sensibilisierung von Mitarbeitenden, Compliance mit Datenschutzvorgaben). Der Weg in diesen Beruf führt häufig über ein Studium in Informatik, IT-Sicherheit oder Wirtschaftsinformatik. Es gibt mittlerweile auch spezialisierte Bachelor- und Masterstudiengänge in Cybersecurity. Zudem ist ein Einstieg über eine abgeschlossene IT-Ausbildung mit anschließenden Weiterbildungen im Bereich IT-Sicherheit möglich. Auch Quereinsteiger:innen mit fundierten IT-Kenntnissen und Zertifizierungen können in dieses Berufsfeld gelangen.

Rolle im Kontext Cybersicherheit:

Sicherheitsanalyst:innen sind die Wächter:innen des digitalen Raums. Sie spezialisieren sich darauf, Angriffe und Bedrohungen möglichst in Echtzeit zu erkennen, zu analysieren und einzudämmen. Durch ihre Analysen von Angriffsmustern und Schwachstellen schaffen sie die Grundlage für die Weiterentwicklung von Sicherheitsmaßnahmen. Ihr Wissen ist entscheidend, um Bedrohungen wie Schadsoftware, Phishing, Ransomware oder unbefugte Zugriffe abzuwehren. Anders als IT-Forensiker:innen, die Angriffe im Nachhinein untersuchen, arbeiten Sicherheitsanalyst:innen präventiv und proaktiv, um Bedrohungen frühzeitig zu erkennen und Sicherheitsvorfälle möglichst zu verhindern. In vielen Organisationen bilden sie damit das Herzstück der Cybersecurity-Abteilung, da sie für die kontinuierliche Absicherung des digitalen Betriebs verantwortlich sind.

Penetration Tester / Ethical Hacker

Allgemeines Berufsbild:

Penetration Tester:innen, auch Ethical Hacker genannt, sind hochspezialisierte Fachkräfte, die im Auftrag von Unternehmen Angriffe auf deren IT-Systeme simulieren. Ziel ist es, Sicherheitslücken und Schwachstellen aufzudecken, bevor sie von Cyberkriminellen ausgenutzt werden können. Sie nutzen dafür Methoden und Werkzeuge, die auch echte Angreifer einsetzen würden, dokumentieren die Ergebnisse und geben konkrete Handlungsempfehlungen. Neben technischen Tests beraten sie Unternehmen auch strategisch zur Stärkung der IT-Sicherheit. In diesen Beruf führt in der Regel ein Studium im Bereich Informatik, IT-Sicherheit oder Cybersecurity. Ergänzend sind anerkannte Zertifizierungen wie CEH (Certified

Ethical Hacker) oder OSCP (Offensive Security Certified Professional) wichtig. Manche Penetration Tester:innen kommen auch über eine IT-Ausbildung mit Spezialisierung in Netzwerktechnik oder IT-Sicherheit in das Feld.

Rolle im Kontext Cybersicherheit:

Ethical Hacker:innen tragen aktiv zur Prävention bei, indem sie IT-Systeme, Anwendungen und Netzwerke gezielt „auf die Probe stellen". Sie entwickeln realistische Angriffsszenarien, spielen diese durch und zeigen so die tatsächliche Widerstandsfähigkeit einer Organisation gegenüber Cyberangriffen. Auf diese Weise unterstützen sie Unternehmen dabei, Sicherheitslücken schnell zu schließen und ihre Systeme nachhaltig zu schützen. Ihr Beitrag ist besonders wertvoll, weil er eine praxisnahe Sicht auf die IT-Sicherheit eröffnet und verdeutlicht, wie Angreifer tatsächlich vorgehen würden.

IT-Forensiker:in

Allgemeines Berufsbild:

IT-Forensiker:innen beschäftigen sich mit der Untersuchung von Cyberangriffen und IT-Sicherheitsvorfällen. Sie sichern digitale Spuren, analysieren Daten und rekonstruieren, wie ein Angriff stattgefunden hat. Dabei arbeiten sie häufig mit spezialisierten Tools, um gelöschte oder verschlüsselte Daten wiederherzustellen. Ihre Arbeit ist nicht nur für Unternehmen von Bedeutung, sondern auch für Ermittlungsbehörden, da sie gerichtsfeste Beweise liefern können. IT-Forensiker:innen benötigen daher neben technischem Know-how auch ein fundiertes Verständnis rechtlicher Rahmenbedingungen. Der Einstieg erfolgt meist über ein Studium der Informatik, IT-Sicherheit oder spezieller Studiengänge wie Digitale Forensik oder Cybercrime. Es gibt auch Masterprogramme, die auf IT-Forensik spezialisiert sind. Alternativ ist ein Weg über eine IT-Ausbildung mit anschließender Weiterbildung oder Spezialisierung im Bereich IT-Forensik möglich.

Rolle im Kontext Cybersicherheit:

Im Bereich der Cybersicherheit übernehmen IT-Forensiker:innen die Rolle von digitalen Ermittler:innen. Sie helfen, nach einem Angriff die Ursachen zu verstehen, Täter:innen zu identifizieren und Sicherheitslücken zu schließen. Ihre Analysen tragen dazu bei, aus Vorfällen zu lernen und die Resilienz von Systemen zu erhöhen. Darüber hinaus leisten sie einen wichtigen Beitrag im juristischen Kontext, indem sie Beweise sichern und aufbereiten, die in Gerichtsverfahren genutzt werden können. Im Gegensatz zu IT-Sicherheitsanalyst:innen, die Bedrohungen in Echtzeit erkennen und abwehren, arbeiten IT-Forensiker:innen reaktiv und detailorientiert: Sie kommen in der Regel nach einem Angriff zum Einsatz, um die Spuren zu sichern und den Tathergang zu rekonstruieren.

4. Unterrichtsverlauf: Cyberattacken und Datensicherheit – warum Daten so wertvoll sind und wer sie schützt

Empfohlene Klassenstufen: 7/8/9
Länge: 90 Minuten

Ziel der Stunde:

Die Schüler:innen erkennen den Wert persönlicher Daten im digitalen Raum und reflektieren Risiken von Cyberangriffen. Sie erarbeiten konkrete Strategien zum Schutz eigener Daten und lernen verschiedene Berufsprofile kennen, die sich professionell mit Cybersicherheit befassen.

Phase/Zeit	Lehrkräfte- / Lernendenverhalten	Methodisch-didaktische Hinweise	Sozialform / Medien
Einstieg **20 Minuten**	**Impuls:** „Ein Hacker hat sich in einen großen Pharmakonzern eingeschlichen und droht, Millionen von Daten zu stehlen. Scanne den QR-Code am Smartboard oder öffne den Link und hilf dem IT-Team beim Abwehren der Attacke." Die Schüler:innen spielen das Spiel am Smartphone/Tablet/Laptop. Anschließend stellt die Lehrkraft folgende **Impulse:** • „Bestimmt hast du schon einmal von genau solchen Cyberangriffen in den Nachrichten oder auf Social Media gehört. Erzähle davon." • „Vielleicht hast du auch schon einmal eine verdächtige E-Mail erhalten. Berichte uns davon." Die Erfahrungen werden im Plenum diskutiert.	Erzeugung von Motivation, Aufmerksamkeit und Interesse Erste Hinführung zum Stundenthema Aktivieren von Vorerfahrungen	Einzelarbeit Plenum Smartphone/Tablet/Laptop M1: PowerPoint-Präsentation (Folien 1-2) https://sieya.de/game/cybersecurity
Zielangabe	„Heute wirst du lernen, welche Daten im Netz besonders wertvoll sind und wie du dich und deine Daten schützen kannst."	Transparenz	Plenum

Phase/Zeit	Lehrkräfte- / Lernendenverhalten	Methodisch-didaktische Hinweise	Sozialform / Medien
Erarbeitung **10 Minuten**	Am Smartboard erscheint der Satz: Daten sind das Gold der digitalen Welt (Folie 3). **Impuls:** „Lies das Statement. Vermute, warum Daten so wertvoll sind." Anschließend verteilt die Lehrkraft Kärtchen mit verschiedenen „Datensätzen" (z. B. Kreditkartendaten, E-Mail-Account, Gesundheitsdaten, Social-Media-Account, Passkopie). **Impuls:** „Was glaubst du, wie viel Cyberkriminelle im sogenannten Darknet – einem versteckten Teil des Internets, in dem man anonym handeln kann – ungefähr für so etwas zahlen? Diskutiere mit deinem Partner oder deiner Partnerin und notiere eure Schätzung auf der Karte." Die Schätzungen der Lernenden werden gegenübergestellt und diskutiert. Anschließend zeigt die Lehrkraft die vereinfachten realen Durchschnittswerte aus Studien (Folien 4 und 5). **Impulsfragen:** • „Vermute, warum diese Daten so viel wert sind." • „Überlege, welche Daten bei Cyberangriffen besonders interessant sein könnten." • „Überlege: Was bedeutet das für uns? Welche Daten sind besonders schützenswert? Warum sollten wir unsere Daten schützen?"	Konzeptverständnis aufbauen und Visualisierung Moderierendes Unterrichtsgespräch Lebensweltbezug Beispielhafte Liste: • Kreditkartendaten • Zugangsdaten zu einem Streaming-Account • E-Mail-Konto • Gesundheitsakte • Personalausweis/Passkopie • Gehacktes Social-Media-Profil • Zugangsdaten zu einem Social-Media-Profil	Plenum Partnerarbeit M1: PowerPoint-Präsentation (Folien 3-5) M2: Schätzkarten

Phase/Zeit	Lehrkräfte- / Lernendenverhalten	Methodisch-didaktische Hinweise	Sozialform / Medien
Arbeitsphase **20 Minuten**	**Impuls:** „Damit du deine Daten besser schützen kannst, wirst du dir nun in Gruppen Maßnahmen zum Datenschutz und zur IT-Sicherheit erarbeiten." Die Lehrkraft teilt die Lernenden in Gruppen ein und verteilt die folgenden Themen: • Starke Passwörter und Zwei-Faktor-Authentifizierung • Vorsicht vor Phishing-Mails und Fake-Seiten • Datenschutz in sozialen Netzwerken (Privatsphäre-Einstellungen) • Technische Maßnahmen (Firewall, Virenschutz, Updates) Die Lernenden erarbeiten sich jeweils das Themenfeld und formulieren die wichtigsten Tipps zum Datenschutz, indem sie die wichtigsten Erkenntnisse auf den Schutzschildern festhalten.	Kooperatives Lernen Erarbeitung von Lösungsstrategien Lebensweltbezug	Gruppenarbeit M3: Infokarten und Schutzschilder
Reflexion **10 Minuten**	Die Lernenden präsentieren jeweils in einem kurzen Pitch ihre Ergebnisse. Die erarbeiteten Tipps werden auf eine gemeinsame Cybersicherheits-Wand übertragen. Hier werden nach jedem Pitch die Schutzschilder der einzelnen Gruppen gesammelt.	Reflektieren von Lösungen Wertschätzung von Schüler:innenleistungen Sicherung des kollektiven Wissens der Klasse	Plenum
Vertiefung **25 Minuten**	**Impuls:** „Wir haben jetzt bereits darüber gesprochen, wie du dich selbst und deine Daten besser schützen kannst. Allerdings hast nicht nur du als Privatperson eine Herausforderung, wenn es um Cybersicherheit geht. Auch Unternehmen müssen sich gut schützen, denn auch ihre Daten sind sehr wertvoll. Überlege, warum es wichtig ist, dass Unternehmen ihre Daten schützen."	Transfer Berufsorientierung und Zukunftsbezug Gruppenpuzzle Arbeitsteiliges Lernen	Gruppenarbeit M4: Placemat, Berufekarten, Berufsprofil zum Ausfüllen

Phase/Zeit	Lehrkräfte- / Lernendenverhalten	Methodisch-didaktische Hinweise	Sozialform / Medien
	Die Schüler:innen äußern sich dazu, die Lehrkraft geht ggf. auf Aspekte wie kritische Infrastruktur, Datenschutz, Produktionsprozesse und Unternehmensgeheimnisse ein. **Impuls:** „Genau deswegen gibt es in Unternehmen häufig verschiedene Personen, die sich um Datenschutz und Datensicherheit kümmern." Die Lehrkraft teilt die Lernenden in Expertengruppen ein. Jede Expertengruppe erhält einen Beruf, inklusive einer kurzen Beschreibung, Fähigkeiten und Zuständigkeiten. Die Gruppen erarbeiten sich ein kurzes Berufsprofil. Anschließend bilden sich neue Gruppen: Aus jeder Expertengruppe kommt jeweils eine Person in die Stammgruppe. Die Lernenden tauschen sich in den Stammgruppen über die verschiedenen Berufe aus und erstellen ein Placemat. Es entsteht eine Übersicht mit verschiedenen Berufen, die zusammen ein Cybersicherheits-Team im Unternehmen bilden.		
Sicherung **5 Minuten**	**Impuls**: „Wir haben heute verschiedene Tipps zusammengetragen, wie man sich und seine Daten im Netz besser schützen kann. Nenne den Tipp, den du besonders wichtig findest. Begründe deine Entscheidung." Es wird ein kurzes Blitzlicht durchgeführt und die Lernenden erläutern ihre Wahl.	Sichtbarkeit der Ergebnisse Festhalten wichtiger Begriffe Blitzlicht	Plenum

Methodisch-didaktische Umsetzung der Stunde

Die Stunde ist so angelegt, dass die Schüler:innen auf mehreren Ebenen angesprochen werden: kognitiv, handlungsorientiert und im Hinblick auf ihre zukünftige Berufsorientierung. Der spielerische Einstieg mit einer Cyberattacke spricht die Lebenswelt der Jugendlichen direkt an, da Cyberangriffe und Phishing mittlerweile Themen sind, mit denen sie sowohl in den Medien als auch persönlich in Kontakt kommen können. Dadurch wird Motivation erzeugt und ein unmittelbarer Alltagsbezug hergestellt.

In der Erarbeitungsphase wird der abstrakte „Wert von Daten" greifbar gemacht, indem die Schüler:innen die ökonomische Dimension einschätzen und anschließend mit realen Vergleichswerten konfrontiert werden. Das Schätzspiel sorgt dabei nicht nur für Aktivierung und Überraschung, sondern verdeutlicht, dass Daten als Ware gehandelt werden und einen erheblichen Stellenwert besitzen. Auf diese Weise wird ein Bewusstsein für die Schutzwürdigkeit persönlicher Informationen geschaffen.

Die Arbeitsphase knüpft daran an und fördert durch kooperative Lernformen die eigenständige Auseinandersetzung mit zentralen Maßnahmen der Cybersicherheit. Durch die Gruppenarbeit werden nicht nur fachliche Inhalte erarbeitet, sondern auch kommunikative und soziale Kompetenzen gestärkt. Gleichzeitig lernen die Schüler:innen konkrete Handlungsstrategien kennen, die sie in ihrem Alltag direkt umsetzen können, womit der Lebensweltbezug konsequent fortgeführt wird.

Die Reflexion bietet den Lernenden die Möglichkeit, ihre Ergebnisse zu präsentieren und in einer gemeinsamen Übersicht sichtbar zu machen. Damit wird die Bedeutung der individuellen Beiträge gewürdigt und gleichzeitig das kollektive Wissen der Klasse gesichert.

Besonders bedeutsam ist die Vertiefung, in der die Perspektive von der individuellen Datensicherheit auf die berufliche Ebene erweitert wird. Das Gruppenpuzzle ermöglicht es den Schüler:innen, verschiedene Berufsprofile im Bereich Cybersicherheit kennenzulernen und einzuordnen. Dadurch wird ein zentrales Ziel der Berufsorientierung umgesetzt: Jugendliche sollen berufliche Tätigkeitsfelder entdecken, die gesellschaftlich hochrelevant sind und in einem wachsenden Zukunftsmarkt liegen.

Die abschließende Sicherung greift die persönlichen Einschätzungen der Lernenden noch einmal auf und stellt eine Rückbindung an ihre individuellen Lebenswelten sicher. Damit werden die wesentlichen Erkenntnisse nicht nur fachlich, sondern auch persönlich bedeutsam verankert. Insgesamt verbindet die Stunde auf diese Weise anschaulich die Themen Digitalisierung, Datensicherheit und Berufsorientierung.

5. Arbeitsmaterialien

Cyberattacken und Datensicherheit – warum Daten so wertvoll sind und wer sie schützt

Kreditkartendaten

Ich schätze, Kreditkartendaten aus Deutschland sind _____ Euro wert.

Streaming-Dienste

Ich schätze, Zugangsdaten zu Streaming-Diensten sind _____ Euro wert.

E-Mail-Konto

Ich schätze, Zugangsdaten zum E-Mail-Konto sind _____ Euro wert.

Gesundheitsakte

Ich schätze, Gesundheitsdaten sind _____ Euro wert.

Personalausweis

Ich schätze, eine Kopie vom Personalausweis ist _____ Euro wert.

Social-Media-Profil

Ich schätze, die Zugangsdaten zu einem Social-Media-Profil sind_____ Euro wert.

Cybersicherheit und Datenschutz

Starke Passwörter und Zwei-Faktor-Authentifizierung

Viele Menschen verwenden immer noch unsichere Passwörter wie „123456“ oder „Passwort“. Für Kriminelle sind solche Zugänge ein gefundenes Fressen: Mit speziellen Programmen können sie Millionen Kombinationen pro Sekunde ausprobieren. Starke Passwörter bestehen aus mindestens 12 Zeichen und enthalten Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Ein gutes Passwort ist schwer zu erraten, aber für dich noch merkbar – z. B. indem du dir einen Satz überlegst und die Anfangsbuchstaben benutzt: „Meine Oma geht jeden Samstag einkaufen und kauft 5 Äpfel!“ → **MogjSeuk5Ä!**

Doch selbst das sicherste Passwort kann gestohlen werden, z. B. wenn eine Firma gehackt wird. Deshalb gibt es die **Zwei-Faktor-Authentifizierung (2FA)**. Hier musst du beim Login nicht nur dein Passwort eingeben, sondern auch einen zweiten „Schlüssel“. Das kann ein Code sein, der per SMS oder App an dein Handy geschickt wird. So brauchen Angreifer nicht nur dein Passwort, sondern auch Zugriff auf dein Gerät. Dadurch wird dein Konto viel sicherer.

Erstelle gemeinsam mit deiner Gruppe eine Übersicht mit den wichtigsten Tipps rund um starke Passwörter und Zwei-Faktor-Authentifizierung. Beantworte dazu folgende Fragen zum Text und halte deine Erkenntnisse auf den Schutzschildern schriftlich fest.

1. Nenne zwei Eigenschaften eines sicheren Passworts.
2. Was ist der Vorteil der Zwei-Faktor-Authentifizierung?
3. Manche finden die Zwei-Faktor-Authentifizierung „nervig“. Würdest du sie trotzdem nutzen? Begründe.
4. Überlege: Warum könnte es gefährlich sein, überall das gleiche Passwort zu verwenden?

Cybersicherheit und Datenschutz

Vorsicht vor Phishing-Mails und Fake-Seiten

Phishing ist eine der häufigsten Methoden von Internetkriminellen. Dabei versuchen sie, dich über gefälschte E-Mails oder Webseiten dazu zu bringen, deine Daten preiszugeben. Eine typische Phishing-Mail sieht oft so aus, als käme sie von deiner Bank, einem Paketdienst oder sogar von deiner Schule. Darin steht zum Beispiel: „Ihr Konto ist gesperrt – klicken Sie hier!“ Klickst du auf den Link, landest du auf einer gefälschten Website. Gibst du dort dein Passwort ein, landet es direkt bei den Betrügern.

Manchmal sind Phishing-Mails leicht zu erkennen, z. B. durch Rechtschreibfehler oder eine seltsame Absenderadresse. Andere sind sehr gut gemacht und sehen täuschend echt aus. Darum ist Vorsicht wichtig: Niemals leichtfertig auf Links klicken, sondern lieber direkt auf die offizielle Seite der Bank gehen oder im Zweifel telefonisch nachfragen.

Erstelle gemeinsam mit deiner Gruppe eine Übersicht mit den wichtigsten Tipps rund um Phishing-Mails und Fake-Seiten. Beantworte dazu folgende Fragen zum Text und halte deine Erkenntnisse auf den Schutzschildern schriftlich fest.

1. Was ist das Ziel von Phishing-Mails?
2. Nenne zwei typische Merkmale, an denen du eine Phishing-Mail erkennen kannst.
3. Stell dir vor, du bist unsicher, ob eine Mail echt ist. Wie würdest du vorgehen?
4. Manche Menschen denken: „Mir passiert sowas nicht.“ Warum kann diese Einstellung gefährlich sein?

Cybersicherheit und Datenschutz

Datenschutz in sozialen Netzwerken

Soziale Netzwerke wie Instagram, TikTok oder Snapchat gehören zum Alltag vieler Jugendlicher. Sie bieten Unterhaltung, Kontakt zu Freunden und Informationen. Gleichzeitig werden dort jedoch viele persönliche Daten gesammelt: Welche Bilder du postest, mit wem du schreibst, welche Inhalte du likest. Diese Daten sind wertvoll für die Unternehmen, weil sie damit Werbung passgenau auf dich zuschneiden können.

Auch andere Nutzer:innen können deine Daten sehen. Fotos, Kommentare oder persönliche Infos können schnell in die falschen Hände geraten – zum Beispiel von Fremden oder sogar Mitschüler:innen, die dich ärgern wollen. Darum ist es wichtig, die **Privatsphäre-Einstellungen** zu prüfen: Wer darf deine Beiträge sehen? Wer kann dir Nachrichten schicken? Zusätzlich solltest du dir überlegen, ob du wirklich jedes Detail aus deinem Leben teilen willst. Denn: Was einmal im Internet steht, bleibt oft sehr lange auffindbar.

Erstelle gemeinsam mit deiner Gruppe eine Übersicht mit den wichtigsten Tipps rund um Datenschutz in sozialen Netzwerken. Beantworte dazu folgende Fragen zum Text und halte deine Erkenntnisse auf den Schutzschildern schriftlich fest.

1. Welche Daten sammeln soziale Netzwerke über dich?
2. Was kannst du mit Privatsphäre-Einstellungen schützen?
3. Überlege: Welche Infos würdest du niemals öffentlich posten – und warum?
4. Manche sagen: „Wenn man nichts zu verbergen hat, braucht man auch keinen Datenschutz.“ Was hältst du von dieser Aussage?

Cybersicherheit und Datenschutz

Technische Maßnahmen (Firewall, Virenschutz, Updates)

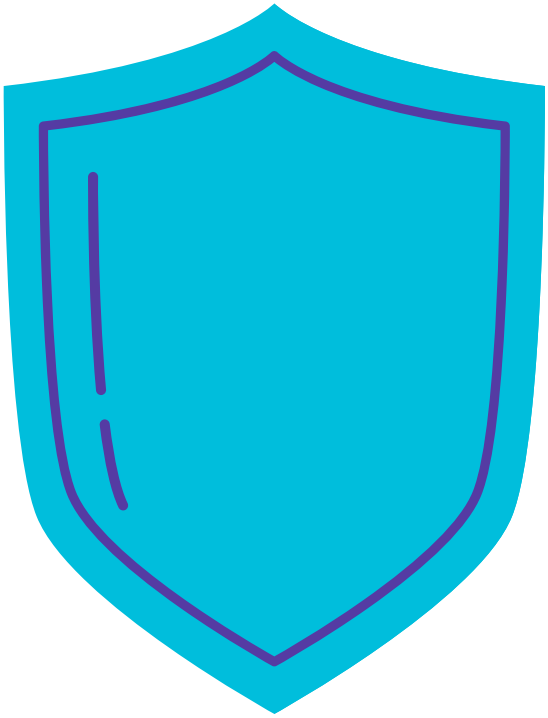
Nicht nur dein Verhalten, auch die Technik schützt dich im Internet. Eine Firewall ist wie ein Türsteher: Sie überwacht die Daten, die in dein Gerät hinein- oder herausgehen, und blockiert verdächtige Verbindungen.

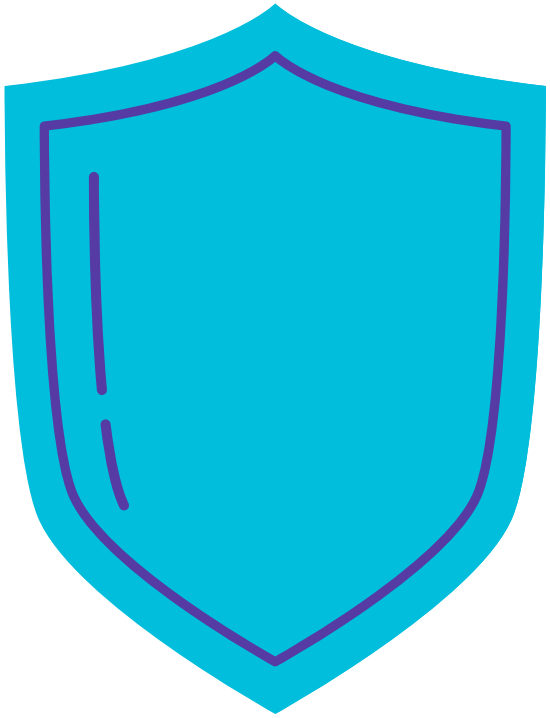
Ein Virenschutzprogramm prüft Dateien, Programme und E-Mails auf bekannte Schadsoftware. So können viele Angriffe schon gestoppt werden, bevor sie Schaden anrichten.

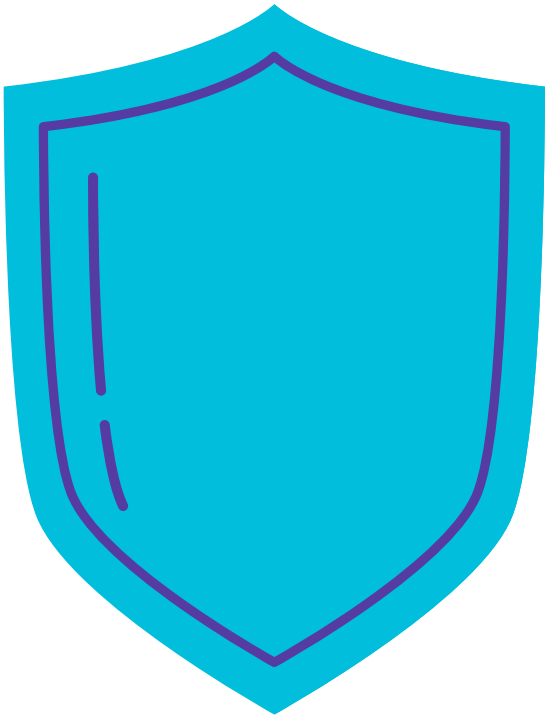
Wichtig sind auch Updates. Hersteller von Apps und Betriebssystemen schließen damit regelmäßig Sicherheitslücken. Wer Updates ignoriert, hat oft offene „Einfallstore" für Hacker. Deshalb gilt: Immer alles up-to-date halten. Auch sichere WLAN-Verschlüsselung (z. B. WPA2) und regelmäßige Backups gehören zu den grundlegenden Maßnahmen der IT-Sicherheit.

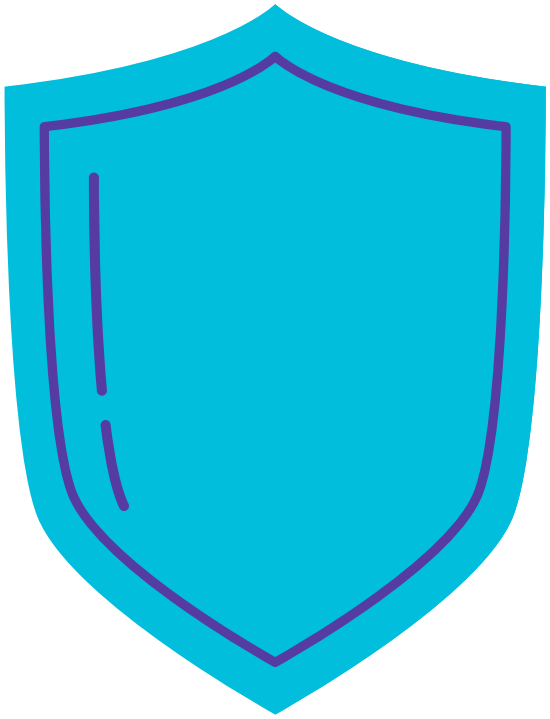
Erstelle gemeinsam mit deiner Gruppe eine Übersicht mit den wichtigsten Tipps rund um technische Maßnahmen. Beantworte dazu folgende Fragen zum Text und halte deine Erkenntnisse auf den Schutzschildern schriftlich fest.

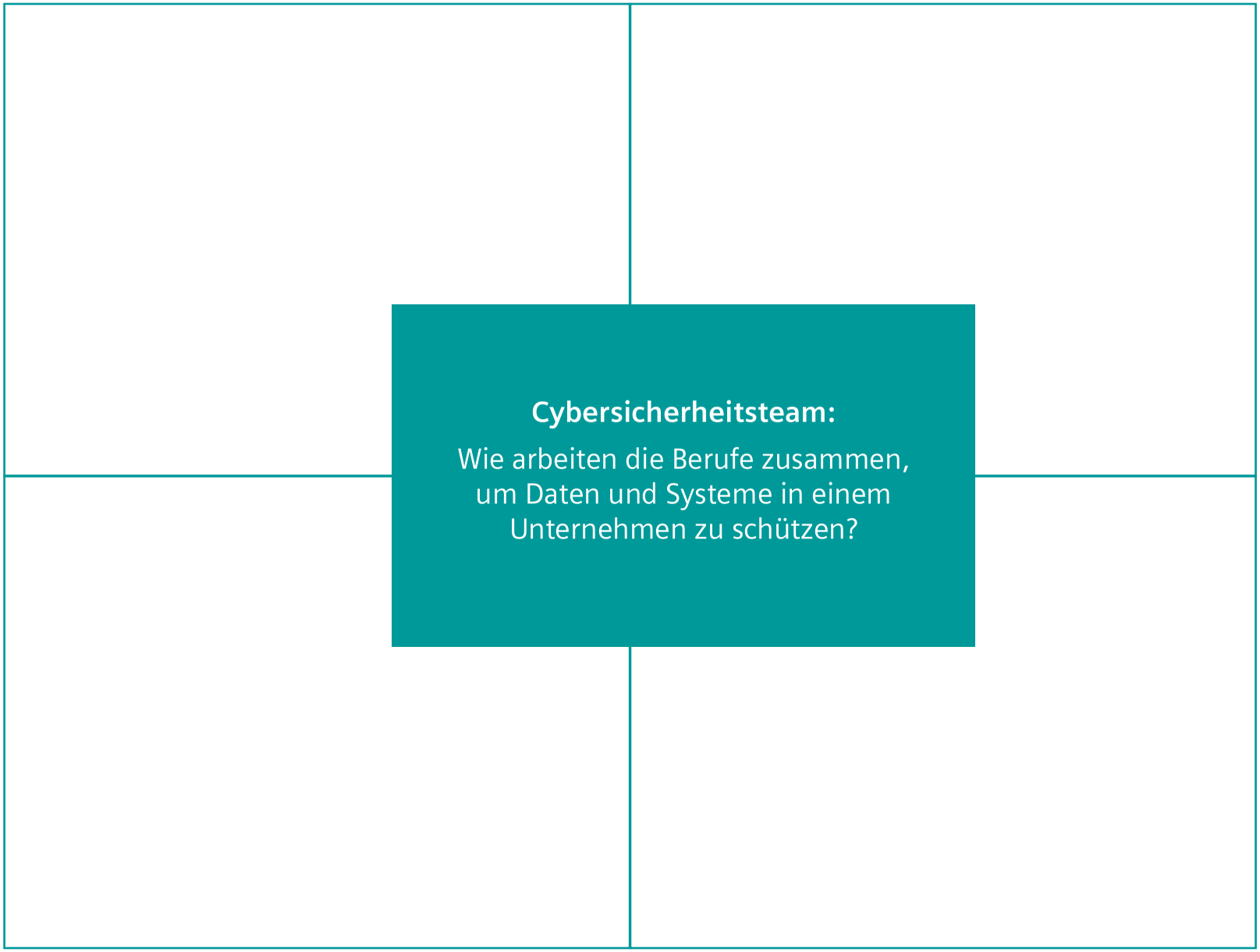
1. Was ist die Aufgabe einer Firewall?
2. Warum sind Updates für die Sicherheit so wichtig?
3. Manche Nutzer schalten Updates ab, weil sie Zeit kosten. Was hältst du davon?
4. Stell dir vor, deine Eltern meinen: „Wir brauchen keinen Virenschutz, wir klicken ja nichts Gefährliches an." Wie würdest du antworten?





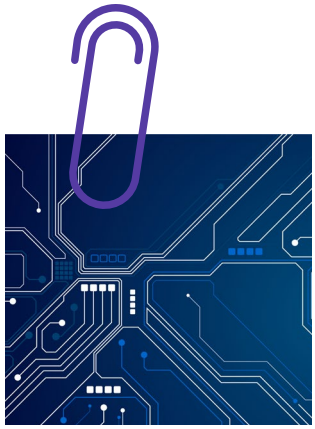





Cybersicherheitsteam:
Wie arbeiten die Berufe zusammen, um Daten und Systeme in einem Unternehmen zu schützen?

Berufe in der Cybersicherheit

1 **Lest das Fallbeispiel durch.**



Fachinformatiker:in für Systemintegration

Fachinformatiker:innen für Systemintegration kümmern sich darum, dass die gesamte IT-Infrastruktur in einem Unternehmen zuverlässig läuft. Sie planen, installieren und pflegen Computer, Netzwerke, Server und Software. Wenn zum Beispiel in einer Firma alle Mitarbeiter:innen gleichzeitig ins Internet gehen, E-Mails verschicken oder gemeinsam an Projekten arbeiten, sorgt der Fachinformatiker oder die Fachinformatikerin dafür, dass das Netzwerk stabil bleibt und keine Daten verloren gehen. Ein wichtiger Teil der Arbeit ist außerdem die Fehleranalyse: Sie sprechen mit den Beschäftigten, finden die Ursachen von Software- und Hardware-Problemen und beheben sie.

Darüber hinaus konzipieren und realisieren Fachinformatiker:innen für Systemintegration komplexe, oft kundenspezifische IT-Systeme. In ihrer Ausbildung lernen sie, wie unterschiedliche Systeme geplant, integriert, in Betrieb genommen und gewartet werden. Dazu gehört nicht nur klassische Unternehmens-IT, sondern je nach Einsatzbereich auch das Betreiben von Systemen der Gebäude-, Automatisierungs- oder Energietechnik.

Auch die Sicherheit der Systeme gehört zu ihren Aufgaben. Sie richten Firewalls ein, spielen regelmäßig Updates ein und achten darauf, dass nur befugte Personen Zugriff auf bestimmte Daten haben. In großen Unternehmen sind Fachinformatiker:innen außerdem in die Planung neuer IT-Projekte eingebunden: Wenn zum Beispiel eine Firma eine neue Software einführen möchte, beraten sie, welche Technik nötig ist, testen verschiedene Lösungen und schulen anschließend die Mitarbeiter:innen. Mit Beratung und Schulungen vermitteln manche Fachinformatiker:innen ihr Wissen sogar im Außendienst an verschiedene Unternehmen.

Typische Fähigkeiten sind technisches Verständnis, eine strukturierte Arbeitsweise, Geduld beim Lösen von Problemen und die Fähigkeit, auch komplizierte technische Zusammenhänge verständlich zu erklären.

Berufe in der Cybersicherheit

1 **Lest das Fallbeispiel durch.**

IT-Forensiker:in

IT-Forensiker:innen kommen ins Spiel, wenn ein Angriff bereits passiert ist. Sie sind so etwas wie Detektiv:innen für digitale Spuren. Ihre Aufgabe ist es, herauszufinden, wie die Täter:innen vorgegangen sind, welche Daten gestohlen wurden und ob man die Täter:innen eventuell identifizieren kann.

Ein Beispiel: Nach einem Hackerangriff steht ein Unternehmen vor der Frage, ob wichtige Kundendaten abgeflossen sind. Die IT-Forensiker:innen untersuchen die betroffenen Computer und Server, sichern digitale Beweise und rekonstruieren die Abläufe. Dabei achten sie darauf, die Daten so zu sichern, dass sie auch vor Gericht verwendet werden können.

Neben der Analyse spielt auch die Prävention eine Rolle: IT-Forensiker:innen geben Empfehlungen, wie man ähnliche Vorfälle in Zukunft verhindern kann. Sie arbeiten eng mit der Polizei, mit Rechtsabteilungen oder auch mit den Sicherheitsanalyst:innen im Unternehmen zusammen.

Für diesen Beruf sind neben technischem Fachwissen auch Sorgfalt, Genauigkeit und ein gutes Verständnis für rechtliche Rahmenbedingungen wichtig. Außerdem müssen Forensiker:innen in der Lage sein, komplexe technische Abläufe Schritt für Schritt zu erklären – sei es vor Gericht, vor der Geschäftsführung oder in Berichten.

Berufe in der Cybersicherheit

1 **Lest das Fallbeispiel durch.**

Penetration Tester / Ethical Hacker

Penetration Tester, auch „Ethical Hacker“ genannt, versuchen ganz bewusst, in die Systeme eines Unternehmens einzubrechen – allerdings mit einer offiziellen Erlaubnis. Ihr Ziel ist es nicht, Schaden anzurichten, sondern Schwachstellen aufzudecken, bevor echte Kriminelle sie ausnutzen.

Ein Beispiel: Ein Penetration Tester bekommt den Auftrag, die IT-Systeme einer Bank zu prüfen. Er oder sie versucht dann, Passwörter zu knacken, unsichere Programme zu finden oder sich über das Firmennetzwerk Zugriff auf sensible Daten zu verschaffen. Gelingt das, wird das Unternehmen sofort informiert und erhält Tipps, wie diese Lücken geschlossen werden können.

Die Arbeit erfordert ein tiefes technisches Wissen über Netzwerke, Betriebssysteme und Programmiersprachen. Gleichzeitig braucht man Kreativität und Einfallsreichtum, um immer wieder neue Angriffswege zu finden. Viele Penetration Tester arbeiten in Teams, weil unterschiedliche Expert:innen verschiedene Arten von Angriffen testen können – vom Email-Betrug (Phishing) über unsichere Apps bis hin zu Angriffen auf WLAN Netze.

Wichtig ist auch die Kommunikation: Ein Ethical Hacker muss den Verantwortlichen im Unternehmen verständlich erklären können, wo die Schwachstellen liegen und welche Schutzmaßnahmen nötig sind.

Berufe in der Cybersicherheit

1 **Lest das Fallbeispiel durch.**

IT-Sicherheitsanalyst:in / Cybersecurity Analyst

IT-Sicherheitsanalyst:innen überwachen die Sicherheit der Systeme und Netzwerke in einem Unternehmen. Ihre Hauptaufgabe ist es, Angriffe zu verhindern und Schwachstellen zu erkennen, bevor sie ausgenutzt werden können. Dafür arbeiten sie oft mit speziellen Programmen, die das gesamte Netzwerk auf ungewöhnliche Aktivitäten hin untersuchen.

Ein Beispiel: Wenn sich jemand nachts von einem unbekannten Standort ins Firmennetzwerk einloggen will, kann das ein Hinweis auf einen Hackerangriff sein. Der Sicherheitsanalyst oder die Sicherheitsanalystin prüft diesen Vorfall sofort und entscheidet, ob es sich nur um einen Irrtum handelt oder ob ein Angriff läuft.

Neben der Überwachung gehört auch die Analyse von Vorfällen zu ihrem Alltag. Wenn ein Angriff erfolgreich war, müssen sie herausfinden, wie es dazu kommen konnte und wie man solche Probleme in Zukunft vermeidet. IT-Sicherheitsanalyst:innen beraten außerdem Software-Entwickler:innen und Fachinformatiker:innen dabei, Systeme sicher aufzubauen und bestehende Sicherheitskonzepte weiterzuentwickeln. Dazu entwickeln sie Richtlinien, führen Risikoanalysen durch und erstellen Notfall- sowie Wiederherstellungspläne.

Ihre Arbeit umfasst sowohl die technische Ebene (z. B. Angriffserkennung, Monitoring, Incident Response) als auch die organisatorische Ebene (z. B. Sensibilisierung von Mitarbeitenden, Einhalten von Sicherheitsstandards und Datenschutzvorgaben).

Für diese Arbeit brauchen IT-Sicherheitsanalyst:innen ein gutes technisches Verständnis, aber auch analytisches Denken, Verantwortungsbewusstsein und Teamfähigkeit. Sie müssen Bedrohungen schnell einschätzen und passende Gegenmaßnahmen vorschlagen können.

Berufe in der Cybersicherheit

2 Bearbeite den folgenden Steckbrief, indem du die Informationen aus dem Text nutzt.

a) Berufsbezeichnung

b) Zentrale Aufgaben in diesem Beruf

Was macht man in diesem Beruf? Wofür ist man verantwortlich?

c) Wichtige Fähigkeiten und Interessen

Was sollte man können oder gerne tun, um diesen Beruf gut auszuüben?

6. Musterlösung Lernspiel Cybersecurity

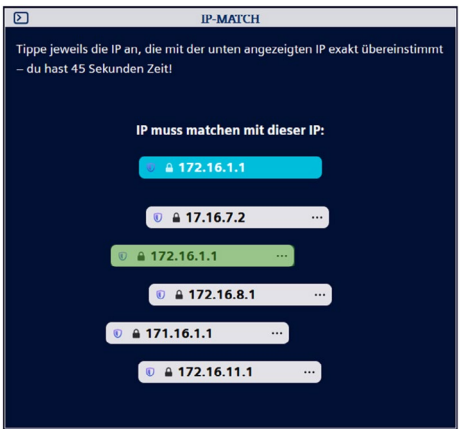
Im Spiel Cybersecurity: Hack-Attack übernehmen die Schüler:innen die Verantwortung für die IT-Sicherheit bei einem Pharmaunternehmen. Ein Hackerangriff bedroht die Produktion lebenswichtiger Medikamente – und es bleiben nur 10 Minuten, um ihn abzuwehren.

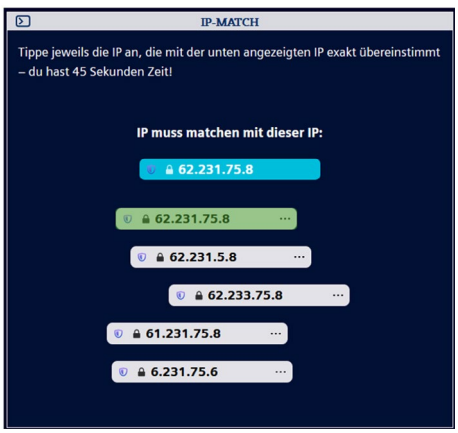
Über eine Kommandozeile geben die Spieler:innen Befehle ein und müssen in drei zeitkritischen Herausforderungen (1) IP-Adressen zuordnen, (2) auffälligen Datenverkehr identifizieren und ein (3) infiziertes Gerät blockieren.

Das Spiel ist gewonnen, wenn alle Aufgaben innerhalb der Zeitlimits gelöst und der Angriff rechtzeitig gestoppt wird – nur dann bleibt die Medikamentenversorgung gesichert.

Herausforderung 1: IP-Match (IP-Adressen zuordnen)

Zeit: 45 Sekunden



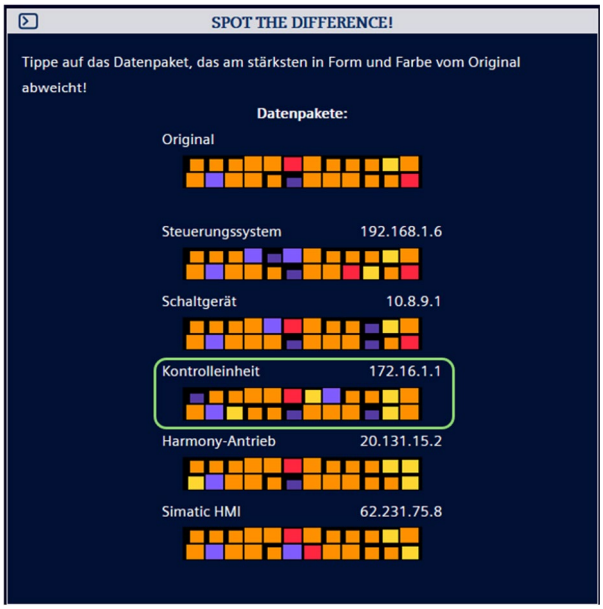


Herausforderung 2: Spot The Difference! (auffälligen Datenverkehr identifizieren)

Level:

Leicht: 35 Sekunden Zeit
Mittel: 20 Sekunden Zeit
Schwer: 20 Sekunden Zeit und sich bewegende Strukturen

Lösung (bei allen Leveln gleich):



Herausforderung 3: Keep It Moving! (infiziertes Gerät blockieren)

Zeit: 40 Sekunden

Da die eingefrorenen Teile im Raster zufällig erscheinen, gibt es hier keine feste Musterlösung. Jedes Mal tauchen mehrere Kombinationen aus drei Zeichen (Buchstaben oder Zahlen) an unterschiedlichen Positionen auf. Insgesamt sind fünf stillstehende Teile zu finden.

Tipp: Am besten funktioniert es, Zeile für Zeile durchzusehen.

Eine mögliche Lösung könnte zum Beispiel so aussehen:

Herausgeber: Siemens AG

People & Organization
Siemens Professional Education
Otto-Hahn Ring 6
81739 München
Deutschland

E-Mail: marketing.spe@siemens.com
Internet: www.ausbildung.siemens.com

Registergericht:
Berlin-Charlottenburg, HRB 12300
München, HRB 6684
WEEE-Reg.-Nr. DE 23691322

SIEMENS