FITNESS

Ein
Cyber Security-Spiel
für die Klassen
9 bis 11

DAS GEHACKTE LABOR

Handreichung für Lehrkräfte

EDUCESK

Impressum

Konzeption und Umsetzung: Helliwood media & education im fjs e. V.
Autor:innen: Leonie Mühlbauer, Benjamin Beuster, Natascha Pauls, Jutta Schneider
Gestaltung und Satz: Christiane Herold

Bildnachweis: shutterstock.com: Dmytro Tyshchenko; BearFotos; Thapana_Studio; Jacob Lund; srzaitsev; ESB Professional und eigene

1. Auflage

Berlin, 2023

ÜBERBLICK

DAS GEHACKTE LABOR ist ein Cyber Security-Spiel, bei dem die Teilnehmenden die Aufgabe haben, als Team einen fiktiven, aber praxisnahen Fall eines Cyber-Angriffs aufzuklären.

Dabei lernen sie zum einen wichtige Sicherheitskonzepte wie Verschlüsselung und den Schutz sensibler Daten und Infrastruktur kennen und erfahren zum anderen, von welchen potenziellen Sicherheitslücken Gefahren ausgehen. Durch das gewählte Szenario erkennen die Teilnehmenden die hohe Relevanz des Themas Cyber Security für Gesellschaft und Wirtschaft und stellen Bezüge zu ihrer eigenen beruflichen Zukunft her.

Für den fiktiven Fall schlüpfen sie nach Art eines Krimi-Dinners in die Rollen der Angestellten eines Labors und müssen herausfinden, wie es passieren konnte, dass einer von ihnen in den Sicherheitsbereich eingebrochen ist und nun die gesamten Forschungsergebnisse in Gefahr sind.

Jede Rolle hat eine eigene Geschichte und ein Alibi – aber auch ein Motiv. Die Teilnehmenden sammeln durch gegenseitige Befragung und Durchsuchen von Beweismaterialien Hinweise und lösen Rätsel, um die Sicherheitslücken aufzudecken und um den Täter oder die Täterin zu identifizieren.

Dabei gibt ihnen das Spiel die Möglichkeit, mehr über Cyber Security zu erfahren. Sie lernen beispielhaft, welche Sicherheitslücken es in den Systemen eines Unternehmens gibt und wie diese ausgenutzt werden können.

EINLEITUNG

Unsere Welt ist durch Technologien hoch vernetzt. Wir möchten sicher mit der Bahn und dem Auto unterwegs sein, brauchen einen sicheren Zahlungsverkehr, wollen auf verschlüsseltem Wege kommunizieren und gleichzeitig gut digital arbeiten können.

Nahezu jedes Unternehmen baut auf digitale Systeme, um effizienter zu operieren, und speichert dabei wertvolle Informationen digital ab. Auch die Politik, Verwaltung und Behörden setzen vermehrt auf digitale Prozesse, um effektiver zu agieren und Dienstleistungen zu verbessern. Gleichzeitig kommen im privaten Bereich ganz selbstverständlich eine Fülle von smarten Geräten zum Einsatz und wir nutzen Technologie, um unser Leben bequemer und unterhaltsamer zu machen.

Cyber Security geht uns alle an

Unsere hoch vernetzte Welt birgt dabei nicht nur unglaubliche Chancen, sondern auch ernsthafte Risiken im Kontext von Cyber Security. Ohne digitale Sicherheitssysteme und Schutzmechanismen wären wir anfällig für eine Vielzahl von Bedrohungen. Cyber-Angreifer könnten nicht nur persönliche Daten stehlen, sondern auch ganze Systeme lahmlegen und erhebliche finanzielle und zeitliche Verluste verursachen. Unsere kritische Infrastruktur könnte gefährdet sein, was weitreichende Auswirkungen auf das öffentliche Leben hätte. Unsicherheiten im digitalen Raum könnten das Vertrauen in Technologie untergraben und die Funktionalität unserer modernen Gesellschaft beeinträchtigen.

Die Bedeutung von Cyber Security erstreckt sich über alle Ebenen, von Einzelpersonen bis hin zu Unternehmen, Behörden und politischen Institutionen. Indem wir uns der Risiken bewusst werden und angemessene Schutzmechanismen etablieren, schützen wir nicht nur unsere eigenen Interessen, sondern tragen auch dazu bei, die Stabilität und Sicherheit unserer vernetzten Welt zu gewährleisten.

Ein Berufsfeld mit Zukunft

Die Nachfrage nach Cyber Security-Spezialisten wird immer größer. Unternehmen, Behörden und Organisationen benötigen Expertinnen und Experten, die in der Lage sind, ihre digitalen Systeme und Daten vor Angriffen zu schützen.

Gleichzeitig ist grundlegendes Wissen über Cyber Security für jeden Einzelnen von uns von entscheidender Bedeutung. Das Verständnis für sicheres Verhalten und der Umgang mit persönlichen Informationen oder sensiblen Daten sind Fähigkeiten, die in nahezu jedem Berufsfeld und in unserer zunehmend digitalisierten Arbeitswelt gefragt sind.

Indem Schülerinnen und Schüler sich mit Cyber Security auseinandersetzen, legen sie den Grundstein für eine kompetente und sichere digitale Zukunft – sowohl für sich selbst als auch für die Gesellschaft im Ganzen.

Das Unterrichtsmaterial

Das Lernmodul DAS GEHACKTE LABOR bietet über ein Rollenspiel in Form eines Krimi-Szenarios einen niedrigschwelligen und gleichzeitig anregenden Einstieg in das Thema Cyber Security.

Im Fokus steht dabei die Vermittlung wichtiger Sicherheits-Grundprinzipien, die in der heutigen vernetzten Welt von entscheidender Bedeutung sind. Die Schülerinnen und Schüler werden sensibilisiert, wie unter anderem kleine Nachlässigkeiten weitreichende Folgen haben können und mit welchen Methoden man seine eigenen Daten, aber auch ein Unternehmen schützen kann. Das Ziel ist, jungen Menschen nicht nur die technische Seite der Cyber Security näherzubringen, sondern sie auch für die Bedeutung dieser Thematik im Alltag und im Berufsfeld zu sensibilisieren.

Das Lernmodul soll sie dazu befähigen, sich sicher und verantwortungsbewusst in der digitalen Welt zu bewegen, sei es als zukünftige Cyber Security-Experten oder als informierte Mitglieder unserer vernetzten Gesellschaft.

KOMPETENZEN

Mit dem Thema IT-Sicherheit knüpft das Lernmodul an die Anforderungen der Rahmenlehrpläne der Länder unter anderem im Fach Informatik und im Bereich digitale Kompetenzen an. Die Schülerinnen und Schüler reflektieren Risiken und Gefahren in digitalen Umgebungen und entwickeln Strategien zum Schutz vor diesen Gefahren.

Die Schülerinnen und Schüler erkennen, wie scheinbar kleine und unbedeutende Nachlässigkeiten in der digitalen Welt zu weitreichenden und ernsthaften Konsequenzen außerhalb ihres persönlichen Umfelds führen können.

Fach- und Methodenkompetenz	Die Schülerinnen und Schüler / erkennen verschiedene Arten von Cyber-Bedrohungen und wie diese funktionieren. / erkennen die Relevanz von Sicherheitsvorkehrungen. / verstehen, warum Verschlüsslung sinnvoll ist. / lernen, welche Sicherheitslücken es in Systemen eines Unternehmens gibt und wie diese ausgenutzt werden können. / erarbeiten methodisch, wie man sich vor Cyber-Angriffen schützen kann.
Aktivitäts- und Handlungskompetenz	Die Schülerinnen und Schüler / analysieren gemeinsam ein simuliertes Cyber-Sicherheitsproblem und entwickeln Problemlösungskompetenz. / identifizieren Sicherheitslücken. / erhalten ein umfassendes Bild von Cyber-Sicherheitsfragen und können dieses Wissen lösungsorientiert anwenden.
Sozial-kommunikative Kompetenz	Die Schülerinnen und Schüler / arbeiten gemeinsam als Team, hören verschiedene Meinungen und Sichtweisen und kombinieren Informationen. / tauschen sich aus und sprechen über Hinweise, um den Tathergang zu rekonstruieren. / denken kritisch und treffen fundierte Entscheidungen im simulierten digitalen Raum.
Personale Kompetenz	Die Schülerinnen und Schüler / üben ihre kritische Denkfähigkeit zum Thema Cyber Security. / entwickeln ein tieferes Verständnis, wie ihre eigenen Handlungen die Sicherheit ihrer digitalen Umgebung beeinflussen können. / werden zu bewussten und kritischen Akteuren der digitalen Welt. / praktizieren zukünftig sicherheitsbewussteres Verhalten, um ihre digitale Privatsphäre zu schützen.

SPIELÜBERSICHT

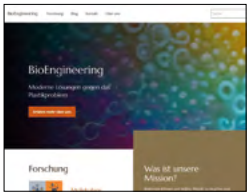
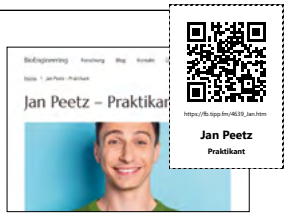
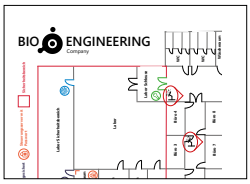
DAS GEHACKTE LABOR

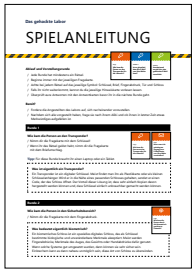
Thema	Cyber Security
Methode	Rollenspiel (Krimi-Dinner)
Klassenstufen	9. – 11. Klasse
Anzahl Mitspieler:innen	mindestens 8 pro Gruppe
Zeitaufwand	Unterrichtseinheit: 90 Minuten / Spieldauer: 60 Minuten
Räumliche Voraussetzungen	Gruppentische, ggf. zusätzliche Räume je nach Gruppenstärke und Lautstärke
Kurzbeschreibung	**Spielidee** Das gehackte Labor ist ein interaktiver Workshop, bei dem die Teilnehmenden in die Rollen der Angestellten eines Labors schlüpfen und gemeinsam einen Cyber-Kriminalfall lösen müssen. Denn einer unter ihnen ist der Täter oder die Täterin. Jetzt heißt es geschickt zu kombinieren und im Team Beweismaterialien zu sichten, um herauszufinden, wie jemand von ihnen in den Sicherheitsbereich des Labors einbrechen und wichtige Forschungsergebnisse stehen konnte. **Spielziel** Jeder Charakter hat eine eigene Geschichte und ein Alibi - aber auch ein Motiv. Die Teilnehmenden müssen insgesamt fünf Rätsel lösen und dabei durch gegenseitige Befragung und Durchsuchen von Hinweisen den Tathergang rekonstruieren, um die Täterin oder den Täter zu identifizieren und die Sicherheitslücken im Labor aufzudecken.
Vorbereitung	/ Arbeitsmaterialien (Stifte, Post-its, Grundriss) bereitlegen / Kartenstapel mit Frage-, Hinweis-, Antwortkarten in der richtigen Reihenfolge pro Gruppe bereitlegen. / QR-Codes zu den Rollenbeschreibungen aufhängen (ggf. im Raum verteilen) / Laptops vorbereiten (W-LAN, Webseiten aufrufen)

MATERIAL

Zur Durchführung des Rollenspiels werden sowohl analoge als auch digitale Materialien benötigt.

Sie finden diese gesammelt unter:
https://fb.tipp.fm/4642_Material.htm

Webseite des Labors	Die Webseite des Labors beinhaltet die Hintergrundgeschichte des Falles im Menüpunkt „Blog“, sowie eine Übersicht der Angestellten im Menüpunkt „Über uns“. Diese dient zu Beginn dazu, die Geschichte und die Rollen allen kurz vorzustellen.	 https://fb.tipp.fm/4632_Webseite.htm
Rollen-beschreibungen	Zu jeder Rolle gibt es eine digitale Beschreibung, die über einen QR-Code abrufbar ist. Jeder Angestellte des Labors hat eine eigene Hintergrundgeschichte, ein Motiv, ein Gerücht sowie ein Alibi für eine andere Person und einen Hinweis zur Lösung des Krimis.	
Namensschilder der Rollen	Damit die Teilnehmenden wissen, wer welche Rolle spielt, sollte jeder ein Namensschild erhalten, ob selbst geschrieben oder ausgedruckt, siehe Vorlage.	
Grundriss des Labors	Der Grundriss des Labors dient zur Orientierung für alle Teilnehmenden. Darauf sind die verschiedenen Stationen abgebildet, an denen die Sicherheitslücken aufgetreten sind. Die Symbole korrespondieren mit den Symbolen auf den Frage-, Hinweis- und Antwortkarten und zeigen an, wann welches Rätsel gelöst werden sollte. Die Teilnehmenden fangen an.	

Spielanleitung für die Rolle des Kommissar	Die Spielleitung übernimmt die Kommissarin oder der Kommissar. Um diese Rolle auszuführen, gibt es neben der Rollenbeschreibung eine Spielanleitung, welche Schritt für Schritt durch die verschiedenen Rätsel zu den Sicherheitslücken führt. Diese Spielanleitung ist nur für die Kommissarin oder den Kommissar. Sie enthält auch wichtige Begriffe, die im Laufe des Spiels geklärt werden sollten.	
Frage-, Hinweis-, Antwortkarten	Zu jedem der fünf Rätsel gibt es jeweils eine Frage-, sowie Hinweis- und Antwortkarte. Sie sind mit Symbolen gekennzeichnet, die sich auch auf dem Grundriss des Labors wiederfinden.	  https://fb.tipp.fm/4799_Spielkarten.htm
Outlook E-Mail-Konto	Eines der Rätsel führt zu einem E-Mail-Postfach. Es bietet sich an, auf einem oder zwei Laptops bereits die Webseite www.outlook.de (noch unangemeldet) geöffnet zu haben.	https://outlook.live.com/ Benutzer: h.waltz-labor@it-fitness.de Passwort: KlaraJulianElias#42
Instapost-Konto	Ein weiteres Rätsel führt auf ein fiktives „Instapost-Konto“. Diese Seite rufen die Teilnehmenden an geeigneter Stelle selbst auf. Der Hinweis auf das Konto befindet sich in einer der Rollenbeschreibungen.	 https://fb.tipp.fm/4633_Instapost.htm
Post-its, Stifte, Laptops	Pro Gruppe sollten 2-3 Laptops zur Verfügung stehen, da die Teilnehmenden für einige der Rätsel die Laborwebseite, das Instapost-Konto sowie ein Outlook-Postfach aufrufen müssen. Die Webseite des Labors sollte bereits zu Spielbeginn geöffnet sein. Um Notizen machen zu können, sollten außerdem Zettel und Stifte bereit liegen.	

ÜBERSICHT FÜR DEN LEHRERTISCH

Zeit	Phase	Inhalt	Sozialform	Medien/Material
10‘	Sensibilisierung	**Thematisches Warm-Up** Einführung in Cyber Security	Plenum	
10‘	Arbeitsphase	**Spielanleitung (ca. 10 min)** / Einführung in das Szenario / Teilnehmer:innen (TN) erhalten Rollen, scannen QR-Code und lesen sich ihre Rollenbeschreibung durch	Plenum /Einzeln	Laborwebseite, QR-Codes, Namensschilder, Spielanleitung für Kommissar
	Ggf. Raumwechsel, Verteilung auf Gruppenräume			
15‘		**Wer ist wer?** / Start 60-Minuten-Timer / TN stellen sich einander vor / TN verbreiten ein Gerücht / TN entlasten jemanden mit einem Alibi	Gruppenarbeit	Grundriss, Rollenbeschreibungen
40‘		**Runde 1 bis 4** siehe Spielanleitung für Kommissar	Gruppenarbeit	Frage-, Hinweis-, Antwortkarten zu Runde 1 bis 4 www.outlook.de
5‘		**Abstimmung und Ende** TN stimmen ab, wer der Täter oder die Täterin war Der oder die Angeklagte legt ein Geständnis ab	Gruppenarbeit	
	Ggf. Raumwechsel zurück ins Plenum			
10´	Reflexion	**Tathergang rekonstruieren** Wie konnte der Vorfall passieren? Welche Sicherheitslücken gab es? **Vier Grundprinzipien der IT-Sicherheit** Vier-Augen-Prinzip, Zero Trust, Datensparsamkeit, Überprüfbarkeit	Plenum	

UNTERRICHTSABLAUF

Ein Krimi-Dinner ist eine Art Rollenspiel, bei dem die Teilnehmenden in die Rollen verschiedener Charaktere schlüpfen, um gemeinsam einen Fall aufzuklären. Dabei stoßen sie auf eine Reihe von Rätsel, die sie lösen müssen, um den Tathergang nachvollziehen zu können und den Täter oder die Täterin zu identifizieren.

Als Unterrichtsmethode verwendet, ermöglicht ein Krimi-Dinner es den Teilnehmenden, sich aktiv mit einem Thema auseinanderzusetzen und dabei Kernkompetenzen wie Kommunikationsfähigkeit, Kollaborationsfähigkeit, analytisches Denken und Problemlösungskompetenz zu entwickeln und zu vertiefen. Obwohl einer von ihnen den Täter oder die Täterin darstellt, müssen die Teilnehmenden zusammenarbeiten, um die ihnen bekannten Informationen zu kombinieren, weitere Hinweise zu entdecken und schließlich den Tathergang zu rekonstruieren. Dabei ist jede und jeder wichtig und auch zurückhaltende Teilnehmende werden einbezogen. Durch die realitätsnahe Auseinandersetzung mit dem Thema werden Konzepte, Probleme und Begriffe spielerisch aufgenommen.

Gruppenzusammenstellung und Rollenverteilung
Der Kriminalfall ist darauf ausgelegt, dass mindestens sieben Personen in die Rollen verschiedener Mitarbeitenden des Labors schlüpfen. Die Rolle einer achten Person, die des Kommissars, gibt die Möglichkeit den Kriminalfall zu moderieren. Je nach Lernstärke der Klasse benötigen die Teilnehmenden mehr oder weniger Betreuung durch eine Lehrkraft. Daher kann die Rolle der Moderation von einer Lehrkraft oder, in höheren Jahrgangsstufen, auch von einer gewählten Person aus der Klasse ausgefüllt werden. In diesem Fall ist die Mindestanzahl pro Gruppe acht Personen.

Differenzierung
Jede Rolle kann von bis zu zwei Personen gespielt werden, wobei es sich am meisten anbietet, zunächst die Rolle des Kommissars doppelt zu besetzen.

Sensibilisierung

10' Beginnen Sie das Lernmodul mit einem Brainstorming, z.B. mit der Frage, was sich hinter dem Begriff „Cyber Security" verbirgt. Dokumentieren Sie die Assoziationen der Schülerinnen und Schüler an der Tafel oder an einer Wand. Reflektieren Sie mit ihnen, dass Cyber Security jeden betrifft. Nutzen Sie dabei praktische Beispiele aus Ihrem Erfahrungsraum oder bekannte Fälle aus den Medien. Beziehen Sie auch die Erfahrungen der Schülerinnen und Schüler ein und fragen Sie, wer im eigenen Umfeld z.B. bei Instagram etc. schon einmal gehackt wurde.

Arbeitsphase

70' **Einführung in das Szenario**
Öffnen Sie die **Webseite** des Labors am Whiteboard und erklären Sie mithilfe der Hintergrundgeschichte, was im Labor passiert ist. Erläutern Sie die Aufgabe und die beiden zentralen Fragestellungen:

- Welche fünf Sicherheitslücken gab es?
- Wer war die Täterin oder der Täter?

Stellen Sie danach die sieben Charaktere des Labors mithilfe der **Unterseite „Über uns"** kurz vor und weisen auf die achte Rolle des Kommissars hin. Lassen Sie die Schülerinnen und Schüler ihre Wunschrolle wählen. Die Teilnehmenden scannen den zu ihrer Rolle gehörigen **QR-Code** mit ihrem Smartphone ab, um ihre Rollenbeschreibung zu erhalten. Geben Sie den Teilnehmenden Zeit, sich mit ihrer Rolle vertraut zu machen und achten sie darauf, dass jeder wirklich nur seine eigene Rolle liest, damit noch keine Motive, Gerüchte oder Alibis verbreitet werden.

Tipp: Achten Sie darauf, dass die Rolle des Kommissars von einer Person übernommen wird, die die Gruppe führen und anleiten kann.

Spielstart
Starten Sie einen 60-Minuten-Timer. Das Kriminalspiel beginnt. Die Person in der Kommissarenrolle nutzt die **Spielanleitung** und führt die Gruppe durch die einzelnen Schritte des Spiels und von Rätsel zu Rätsel. Zu Beginn erkunden die Schülerinnen und Schüler gemeinsam den **Grundriss des Labors** und stellen sich kurz in ihrer Rolle gegenseitig vor.

Spielablauf
Nachdem sich alle einen Überblick über das Labor und die verschiedenen Rollen verschafft haben, gilt es, die Sicherheitslücken in vier Spielrunden mit insgesamt fünf Rätseln (1 Rätsel = 1 Sicherheitslücke: Schlüssel, Brief, Fingerabdruck, Tür, Schloss) aufzudecken. Hierzu nutzt die Gruppe die **Fragekarten** und bei Bedarf die zugehörigen **Hinweis- und Antwortkarten**.

Spielende
Nachdem alle Sicherheitslücken aufgedeckt wurden, versuchen die Schülerinnen und Schüler zuletzt durch Abstimmung, den Täter zu entlarven. Dazu nennt jede Person einen Hauptverdächtigen. Der Kommissar notiert sich die Nennungen und spricht am Ende den am häufigsten verdächtigten Charakter an. Ist dieser unschuldig, teilt er dies der Runde mit und ein zweiter Verdächtiger darf angesprochen werden. Wird der tatsächliche Täter, der Koch Jochen Pfeffer, angesprochen, gibt er sich geschlagen und trägt sein Motiv sowie den Tathergang vor, die in seiner Personenbeschreibung enthalten sind. In diesem Fall haben der Kommissar und das Labor gewonnen. Werden jedoch zwei Mal unschuldige Charaktere beschuldigt, hat der Täter gewonnen, darf sich zu erkennen geben und auch hier sein Motiv und den Tathergang schildern.

Reflexion

10' Holen Sie die Gruppen wieder zusammen und reflektieren Sie gemeinsam mit den Schülerinnen und Schülern die aufgetretenen Sicherheitslücken:

E-Mail-Postfach wurde gehackt
Das E-Mail-Konto der Laborleitung wurde gehackt und benutzt, um die Rezeptionistin, die zuständig für die Ausgabe der Transponder ist, dazu anzuweisen, fälschlicherweise einen Transponder an einen Kurier zu übergeben. Obwohl die Laborleitung mitgeteilt hatte, während ihres Urlaubes keine E-Mails verschicken zu können, wurde der Ursprung der E-Mail und die darin enthaltene Bitte der Laborleitung nicht hinterfragt. Somit konnte sich der Täter Zugang zum Laborbereich verschaffen.

Passwort wurde über Social Media geteilt
Zugang zum E-Mail-Konto erhielt der Täter dadurch, dass die Laborleitung ihr Passwort auf einem Notizzettel an ihrem Schreibtisch notiert hatte. Da eine Mitarbeiterin des Labors ein Foto des Schreibtisches bei Social Media teilte, war das Passwort öffentlich einsehbar. Zudem setzt sich das Passwort aus den Namen der Kinder der Laborleitung sowie ihrem Alter zusammen und ist somit nicht ausreichend verschlüsselt.

Biometrisch gesicherte Tür wurde blockiert
Obwohl der Zugang zum Sicherheitsbereich des Labors mit einem biometrischen Schloss gesichert ist, wurde dieses von einer Mitarbeiterin aus Bequemlichkeit außer Kraft gesetzt. Da die Tür von einem Stuhl offengehalten wird, konnte der Täter das biometrische Schloss umgehen und so in den Sicherheitsbereich eindringen.

Überwachungskamera ist im Internet einsehbar
Bei der Überwachungskamera, die auf das PIN-Eingabefeld des Serverraums gerichtet ist, handelt es sich um eine Webcam, welche mit dem Internet verbunden ist. Die Aufzeichnungen sind öffentlich einsehbar, da sie auf einer Unterseite der Laborwebseite ausgestrahlt werden. Der Link zu dieser Unterseite ist auch für Außenstehende leicht zu erraten und ermöglichte es dem Täter so, den aktuellen Code für die Sicherheitstür zu erhalten.

Schlüsselkarte wurde verlegt
Der Server, auf dem sich die Forschungsdateien befanden, ist nur mit einer Schlüsselkarte zugänglich. Die Aufbewahrung dieser Schlüsselkarte ist die Verantwortung des IT-Leiters, der sie jedoch in seinem Büro unbeaufsichtigt gelassen hatte. Damit hatte der Täter die Möglichkeit, die Schlüsselkarte zu entwenden, eine Kopie anzufertigen und sie zurückzulegen. Der IT-Leiter hat den zwischenzeitlichen Verlust der Karte nicht gemeldet, um seinen Fehler nicht eingestehen zu müssen.

Fazit
Ziehen Sie gemeinsam mit den Schülerinnen und Schülern ein Fazit: Eigentlich waren das Labor, der Sicherheitsbereich und die Forschungsdateien gut geschützt, aber wurden durch die gemeinsame Unachtsamkeit aller Mitarbeitenden kompromittiert.

Befragen Sie die Gruppen, ob es ihnen gelang, den Täter zu überführen. Stellen Sie anschließend die vier wichtigsten Prinzipien vor, durch die ein wirksamer Schutz vor Online-Angriffen sichergestellt werden kann und schreiben Sie diese an die Tafel:

Vier-Augen-Prinzip / Zero Trust / Datensparsamkeit / Überprüfbarkeit

Eine Erläuterung dieser Begriffe finden Sie im Abschnitt "Hintergrund". Lassen Sie jede Person jeweils ein Beispiel für einen wirksamen Schutz vor Onlineangriffen als Stichwort auf ein Post-It schreiben. Besprechen Sie mit der Klasse, in welche der vier genannten Kategorien das jeweilige Beispiel einsortiert werden soll.

HINTERGRUND

Was ist Cyber Security und warum ist es generell wichtig?

Cyber Security ist ein hochaktuelles Thema, das für die Arbeitswelt von großer Bedeutung ist. Denn in einem immer stärker vernetzten digitalen Umfeld müssen wir uns darauf verlassen können, dass unsere Daten und Systeme sicher sind. Ein Sicherheitsleck kann sowohl für Bildungseinrichtungen als auch für Unternehmen, Behörden oder Privatpersonen erhebliche Konsequenzen haben – von Datendiebstahl bis hin zum totalen Systemausfall. Durch gezieltes Abfangen von Passwörtern, Phishing-Mails oder Ransomware-Attacken können auch wichtige Informationen und personenbezogene Daten verloren gehen oder in falsche Hände geraten.

Wen betrifft Cyber Security?

Cyber Security scheint zunächst ein Thema zu sein, das insbesondere für Unternehmen von Bedeutung ist. Doch in der digitalen Welt von heute, in der fast alle Aspekte des öffentlichen und privaten Lebens mit dem Internet verbunden sind, mehren sich auch die Möglichkeiten für einen Cyber-Angriff. So sorgte beispielsweise 2019 ein Hackerangriff auf die Bundesregierung für Aufruhr, nachdem großflächig sensible Daten von Politikerinnen und Politikern gestohlen und anschließend im Internet bereitgestellt wurden. Die Veröffentlichung von privaten Daten wie Handynummern, Wohnadressen und Chat-Verläufen stellt dabei nicht nur eine Gefahr für die betroffenen Personen dar, sondern ist auch ein Angriff auf demokratische Institutionen. Wie verletzlich Institutionen des öffentlichen Lebens sein können, zeigte zudem ein Cyber-Angriff auf die Gemeinde Bitterfeld im Jahr 2021, welche daraufhin den Katastrophenfall ausrufen musste und mit langfristigen Folgen zu kämpfen hatte. Doch auch Privatpersonen können schnell und unerwartet Opfer eines Cyber-Angriffs werden, beispielsweise indem sie auf einen Link in einer gefälschten E-Mail klicken. In dem Glauben, sie käme von einem abonnierten Streamingdienst, geben sie unbewusst anschließend ihre Kontodaten preis.

Cyber Security ist somit nicht nur ein Thema für IT-Expertinnen und Experten in Unternehmen und der kritischen Infrastruktur, sondern sollte auch von der Gesellschaft und von Privatpersonen ernst genommen werden. Nur wer sich über Risiken und Schutzmaßnahmen informiert, kann bewusst handeln, um die digitale Sicherheit zu gewährleisten.

Vier Grundprinzipien

Cyber-Angriffe werden immer raffinierter und kommen immer häufiger vor. Es gibt verschiedene Ansätze und Methoden, um die Sicherheit der IT-Infrastruktur zu gewährleisten. Dazu gehören unter anderem die vier Grundprinzipien „Zero Trust", „Datensparsamkeit", „Vier-Augen-Prinzip" und „Überprüfbarkeit". Durch Befolgen dieser einfachen Prinzipien ist man sicher im Netz unterwegs.

1. Zero Trust

Das Prinzip Zero Trust bedeutet übersetzt so viel wie „vertraue niemandem". Es ist gleichzeitig das wichtigste Grundprinzip von Sicherheit und auch das am schwierigsten umzusetzende. Zero Trust bezieht sich auf den Grundsatz, niemals Daten preiszugeben, ohne sich zu vergewissern, dass die Quelle der Anfrage glaubwürdig ist, beispielsweise, wenn persönliche Daten auf Internetseiten oder in Apps eingegeben werden sollen.

Die Rechte der Konsumentinnen und Konsumenten werden in Europa sehr stark geschützt, unter anderem durch die Datenschutzgrundverordnung (DSGVO). Die Verordnung nimmt genau den Aspekt von Zero Trust zum Anlass, um den Abfluss persönlicher Daten zu verhindern oder widerrufbar zu machen.

2. Datensparsamkeit

Das beste Vorgehen ist, persönliche Daten nur dann preiszugeben, wenn es tatsächlich nötig ist. Für bestimmte Zwecke bietet es sich an, einen Klarnamen in einer E-Mail-Adresse zu verwenden, zum Beispiel bei Bewerbungen oder anderen persönlichen Anliegen. Um Konten zu verwalten oder bestimmte Dienste in Anspruch zu nehmen, kann jedoch auch eine zweite E-Mail-Adresse mit einem Pseudonym genutzt werden. Im Sinne der Datensparsamkeit sollte daher immer die Frage mitgedacht werden, ob eine Webseite oder App zwingend eine reale Adresse oder Zugriff auf andere sensible Informationen für eine Dienstleistung benötigt.

3. Vier-Augen-Prinzip

Das Vier-Augen-Prinzip ist ein bekanntes Konzept, das bei hochsicheren Systemen schon sehr lange Anwendung findet. In einem Cockpit eines Flugzeugs reisen stets zwei Personen, die in der Lage sind, das Flugzeug zu steuern. Der Ausfall einer Person führt nicht zwangsläufig in die Katastrophe.

Dieses einfache, aber anschauliche Beispiel lässt sich auch auf persönliche Daten im Internet übertragen.

Besonders sichere Systeme, wie zum Beispiel beim Onlinebanking, werden mit genau dieser Methode geschützt: Wird beispielsweise eine Überweisung getätigt, werden zwei Sicherheitsmerkmale, zum Beispiel ein Passwort in Verbindung mit einer SMS, benötigt. Diese Methode, auch Zwei-Faktor-Authentifizierung genannt, schützt das Konto auch dann, wenn eine andere Person an das Passwort gelangt.

Immer mehr Dienste im Internet setzen das Vier-Augen-Prinzip um. Das E-Mail-Konto ist in sehr vielen Fällen der Dreh- und Angelpunkt aller Internet-Accounts und sollte daher besonders beschützt werden. Viele Anbieter unterstützen daher die Authentifizierung mit der Zwei-Faktor-Methode. Wenn es eine Unterstützung dafür gibt, ist es empfehlenswert sie zu aktivieren.

4. Überprüfbarkeit

Bei dem Begriff Überprüfbarkeit handelt es sich darum, dass die Herkunft einer Nachricht überprüfbar wird, das heißt, ob sie wirklich von der richtigen Adresse gesendet wurde. Glücklicherweise ist dieses Prinzip in vielen Diensten und Webseiten bereits fest eingebaut. Erkannt werden kann es an einem kleinen Schloss-Symbol an der linken Seite der Adresszeile aller Browser.

Somit wird gekennzeichnet, dass die Verbindung einer Webseite nicht nur verschlüsselt ist, sondern auch, dass die Gegenstelle authentifiziert ist. Dadurch können Nutzerinnen und Nutzer sicher sein, dass sie die Internetseite sehen, die sie auch sehen wollen. Jede Seite, die sich nicht authentifizieren kann, wird automatisch blockiert.

Cyber Security in der Berufswelt

Die stetig fortschreitende Digitalisierung hat unsere Arbeitsweise transformiert und gleichzeitig neue Anfälligkeiten für Cyber-Angriffe geschaffen. Unternehmen sehen sich mit einer Vielzahl von Bedrohungen konfrontiert, die von Phishing-E-Mails bis hin zu hochentwickelten Ransomware-Angriffen reichen. Daher ist es unerlässlich, dass sowohl Arbeitgeber:innen als auch Arbeitnehmer:innen ein tiefes Verständnis für Cyber-Sicherheit entwickeln.

Das Thema Cyber Security konfrontiert uns tagtäglich mit Herausforderungen. Doch es hält große Chancen für junge Menschen hinsichtlich ihrer beruflichen Zukunft und der Förderung von IT-Skills für den künftigen Job vor – und zwar in verschiedener Hinsicht:

Zunächst sind IT-Spezialistinnen und -Spezialisten erforderlich, die Technologien und Tools zur Abwehr von Angriffen implementieren und gewissenhaft pflegen. Ihr Beitrag erstreckt sich nicht allein auf die Entwicklung und Instandhaltung von Schutzmaßnahmen. Vielmehr umfasst er auch die äußerst kritische Komponente der Reaktion auf Angriffe. Daher werden darüber hinaus Expertinnen und Experten benötigt, die das Wissen und die Fähigkeiten haben, um Schäden zu minimieren, Sicherheitsprotokolle auszuführen, forensische Analysen durchzuführen und Ursachen zu ermitteln.

Diese Analytikerinnen und Analytiker tragen dazu bei, die aktuellen Bedrohungen zu bewältigen und auch langfristig Strategien zur Verbesserung der Sicherheits-infrastruktur zu entwickeln.

Die Implementierung robuster Sicherheitsmaßnahmen und -richtlinien ist somit unerlässlich. Doch neben den IT-Spezialistinnen und Spezialisten muss noch eine weitere, weitaus wichtigere Komponente bedacht werden, um die Sicherheit eines Unternehmens zu gewährleisten: Der Mensch. In einer Zeit, in der nahezu jede Tätigkeit digitalisiert ist, sollte jede und jeder von uns ein Bewusstsein für Cyber-Sicherheit entwickeln. Alle Mitarbeitende eines Unternehmens müssen regelmäßig darin geschult werden, potenzielle Sicherheitslücken erkennen zu können und wissen, wie diese gemeldet werden sollten.

Mit einem grundlegenden Verständnis von Cyber Security, Cyber-Angriffen und Sicherheitslücken können wir alle zur kollektiven Stärkung von Sicherheitsmaßnahmen beitragen.

Letztlich ist ein ganzheitlicher Ansatz erforderlich, der Technologie, Prozesse und menschliches Verhalten berücksichtigt, um eine sichere Arbeitsumgebung zu gewährleisten. Investitionen in Cyber-Security sind also nicht nur eine Vorsichtsmaßnahme, sondern ein entscheidender Schritt, um die Integrität, Vertraulichkeit und Verfügbarkeit sensibler Informationen zu gewährleisten.

GELERNT IST GELERNT

Jetzt ist deine Meinung gefragt. Was hat dir an der heutigen Unterrichtsstunde gefallen?
Was hast du gelernt?

Beurteile dich selbst!			
Das Thema hat mir Spaß gemacht.			
Ich habe mich aktiv beteiligt.			
Die Aufgaben sind mir leicht gefallen.			
Ich habe viel Neues gelernt.			

Ich habe heute gelernt, dass:

Ich werde das nächste Mal mehr darauf achten, dass:

Besonders gefallen hat mir:

Weniger gefallen hat mir:

MUT TUT GUT!

In der Video-Reihe „Mut tut gut“ laden sich Kompetenzexperte Thomas Schmidt und Futurologe Max Thinius regelmäßig inspirierende Akteurinnen und Akteure ein, die mit ihren Projekten zukunftsorientiert arbeiten. Sie machen Mut und zeigen, wie wichtig es ist, sich stetig selbst weiterzubilden. Einen Themenschwerpunkt bildet Cyber Security.

Interview mit Andreas Rickert, Gründer von PHINEO

Wie verändert Technologie gesellschaftliches Engagement? Und welche Kompetenzen braucht es neben einer Portion Mut, um eine starke und lebendige Gesellschaft zu gestalten?

Darüber sprechen wir mit Andreas Rickert, einem der Gründer von PHINEO, Denkfabrik und Beratungshaus für gemeinnützige Organisationen und Unternehmen.

https://fb.tipp.fm/4130_Andreas_Rickert.htm

Interview mit Dr. Christian Hübenthal, Gründer von www.lagebild.media

Was genau bedeutet Cyber Security und warum betrifft dieses Thema jeden von uns im Privaten, aber auch unsere heutige Arbeitswelt und Gesellschaft?

Über das Thema Sicherheit in Zeiten der Digitalisierung sprechen wir mit Dr. Christian Hübenthal, Gründer von www.lagebild.media und Herausgeber der Publikation „Lagebild Sicherheit“. Am Ende des Gesprächs verrät der Experte einfache, aber wirkungsvolle Cyber Security Tipps, die jeder wissen sollte.

https://fb.tipp.fm/4133_Christian_H_benthal.htm

Mehr Videos der Reihe „Mut tut gut“ gibt es hier:
https://fb.tipp.fm/4134_Mut_tut_gut.htm

**Interview mit Cid Kiefer,
Informatik Consulting Systems GmbH**

Security ist aktueller denn je. Dabei sind es nicht nur die großen Konzerne, die Ziel von Hackerangriffen werden. Gerade kleinere Firmen und Mittelständler sind oft von Cyber Angriffen betroffen. Dabei gibt es viele Sicherheitsmaßnahmen, die man treffen kann und sollte, um sich zu schützen.

Über die verschiedenen Möglichkeiten und praktischen Tipps für alle, die sich im Internet bewegen, sprechen wir mit Cid Kiefer, Geschäftsführender Gesellschafter bei der Informatik Consulting Systems GmbH

https://fb.tipp.fm/4132_Cid_Kiefer.htm

**Interview mit Gerald Beuchelt,
Chief Information Security Officer**

Im Bereich Cyber Security werden bereits heute viele Expertinnen und Experten gesucht und auch in Zukunft wird dieser Job immer wichtiger werden! Aber was macht ein Chief Security Information Officer und welche Kompetenzen sind in diesem Beruf gefragt? Was bedeutet Corporate IT? Und wie schützt man sich gegen Hacker Angriffe?

Über all das sprechen wir mit Gerald Beuchelt, Chief Information Security Officer bei Sprinklr. Darüber hinaus erfahrt ihr in diesem Gespräch praktische und wichtige Tipps für eure eigene Sicherheit im Internet.

https://fb.tipp.fm/4131_Gerald_Beuchelt.htm

IT FITNESS

Das Cyber Security-Spiel DAS GEHACKTE LABOR wurde im Rahmen der Future Skills Initiative entwickelt.

Die Future Skills Initiative ist eine Kooperation von:
// SCHULEWIRTSCHAFT Deutschland,
// Netzwerk Berufswahl-SIEGEL und
// dem Förderverein für Jugend und Sozialarbeit e. V.

Die Initiative wird von Microsoft im Rahmen des weltweiten Skills for Employability Programms im Kontext der Initiative IT-FITNESS gefördert.

www.it-fitness.de