Wissensfabrik
Unternehmen für Deutschland

IT2School

Gemeinsam IT entdecken

Modul E5 – Cyberkriminalität und -Sicherheit

Was ist das und wie kann ich mich schützen?

In Kooperation mit

Accenture-Stiftung

Mit Unterstützung von

Wissensfabrik
Unternehmen für Deutschland

Inhalt

1 Cyberkriminalität und -Sicherheit

Mit Cyberkriminalität bezeichnet man Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten oder im weiteren Sinne auch Straftaten, die mittles dieser Informationstechnik begangen werden, z.B. Datendiebstahl. **In diesem Modul wird vermittelt, was Cyberkriminalität bedeutet und welche Auswirkungen kriminelle Aktivitäten haben, die mit Hilfe von digitalen Technologien durchgeführt werden.**

Zusätzlich werden **Maßnahmen** vorgestellt, wie man gegen Cyberkriminelle vorgehen kann und wie man sich schützt. Die so genannte "Cyber-Sicherheit" befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Hierbei wird auch die persönliche Sphäre eingegangen aber auch auf den unternehmerischen Kontext.

Lernfeld/Cluster:	IT selber machen	
Zielgruppe/Klassenstufe:	**X**	4. bis 5. Klasse - Anfänger
	X	6. bis 7. Klasse - Anfänger
	X	8. bis 10. Klasse - Fortgeschritten
	X	11. bis 12. Klasse - Fortgeschritten
Geschätzter Zeitaufwand:	2x45 Minuten	
Lernziele:	• Wissen, was Cyberkriminalität bedeutet. • Verstehen, welche Folgen Cyberkriminalität haben kann. • Erkennen, wie man sich vor Angriffen schützen kann.	
Vorkenntnisse der Schülerinnen und Schüler:	• Unterschiedliche Vorkenntnisse berücksichtigt	
Vorkenntnisse der/des Lehrenden:	• Wir empfehlen zur Vorbereitung der Unterrichtsstunde das Booklet „Digitalität und Kriminalität“ (hier kostenlos)	
Vorkenntnisse der Unternehmensvertreterin/des Unternehmensvertreters		
Sonstige Voraussetzungen:	Voraussetzung • Laptops/PCs für die Online Trainings	

2 Warum gibt es das Modul?

Mit zunehmender Mediennutzung und Integration von digitalen Endgeräten in den Alltag, z.B. beim Online-Banking, haben auch Kriminelle Technologien als ihr Machtinstrument gefunden. Im Vergleich zum Jahre 2000 sind die polizeilich erfassten Fälle von Cyberkriminalität in Deutschland von 10.117 auf 45.793 in 2015 gestiegen.

Durchschnittlich benutzt die Gesamtbevölkerung das Internet an verschiedenen Geräten insgesamt 128 Minuten am Tag, wobei 14-29jährige sogar 245 Minuten täglich im Internet verbringen. Damit ein verantwortungsvoller und sichereres Surfen im WWW gegeben ist, sollten Schülerinnen und Schüler schon früh über Gefahren aufgeklärt werden und Handlungsoptionen im Falle eines Cyberangriffs sowie präventive Maßnahmen aufgezeigt bekommen.

3 Ziele des Moduls

1. *Wissen, was Cyberkriminalität bedeutet.*
2. *Verstehen, welche Folgen Cyberkriminalität haben kann.*
3. *Erkennen, wie man sich vor Angriffen schützen kann.*

4 Inhalte des Moduls

Diese Unterrichtseinheit sensibilisiert zum Einen Ihre Schüler/innen für das Thema Cyberkriminalität. Sie lernen grundlegende Begriffe kennen und erfahren, welche Konsequenzen ein Angriff für Betroffene haben kann. Abschließend setzen Sie sich damit auseinander, welches Verhalten sie vor Cyberkriminalität schützen kann.

Zum Anderen vertieft diese Unterrichtseinheit das Thema . Sie lernen, was sich hinter dem Begriff verbirgt, welche Akteure es gibt und welche Maßnahmen vor der Cyberattacke ergriffen sein sollten. Abschließend setzen Sie sich damit auseinander, wie im Falle einer Cyberattacke zu agieren ist.

5 Unterrichtliche Umsetzung

5.1 Für Anfänger

Beginnen Sie das Modul mit der Frage, wer bereits persönlich oder im Bekanntenkreis **Erfahrungen mit Internetkriminalität** gemacht hat. Dazu zählen z.B. folgende Bereiche:

- Phishing E-Mail bekommen
- Virus auf dem Computer
- Chat mit einer Person, welche vorgibt jemand anderes zu sein
- Datendiebstahl

Sollte es niemanden in Ihrer Klasse getroffen haben, können Sie auf ein lebensnahes Beispiel „Ein Beispiel“ in der Kopiervorlage des Booklets „Digitalität und Kriminalität“ (**hier**) zurückgreifen, um Ihre Schüler/innen eingangs für das Thema zu sensibilisieren.

Um sich tiefergehend mit dem Thema Kriminalität im Netz auseinanderzusetzen, ist es zunächst wichtig, grundlegende Schlagwörter kennenzulernen. Führen Sie dazu das folgende **Online Training** durch, welches einen umfassenden Einstieg in das Thema bietet. Zunächst werden einleitende Informationen zu Methoden und Gründen von Cyberkriminalität vermittelt. Anschließend wird erklärt, was unter Cyberkriminalität und Cybersecurity zu verstehen ist.

Nachdem Ihre Schüler/innen nun gelernt haben, wie präsent Cyberkriminalität im Alltag ist und welche wichtigen Begriffe damit in Verbindung stehen, geht es nun darum zu verstehen, wie wichtig der Schutz der eigenen Daten ist. Zeigen Sie dazu dieses Video, in dem erklärt wird, wie Hacker an Nutzerdaten und Passwörter gelangen und welche Konsequenzen dadurch für die Betroffenen entstehen können.

Doch wie erkennt man eine Cyberattacke? Welchen weiteren Angriffspunkten müssen Ihre Schüler/innen im Alltag entgehen? Nutzen Sie das Arbeitsblatt „Was tust du?“ im Booklet, um Ihre Schüler/innen in Einzel- oder Gruppenarbeit für verschiedene Formen von Angriffen zu sensibilisieren. Die Aufgabe besteht darin, in unterschiedlichen alltagsnahen Situationen einzuschätzen, welches Verhalten geeignet ist, um einem Angriff durch Viren oder Phishing-Mails zu entgehen.

Lassen Sie die Schüler/innen dieses **Online Training** durchführen, um tiefergehende Informationen zu den dargestellten Schutzmaßnahmen zu erlangen. Weiterhin erfahren sie, wie sie sich im Falle einer Cyberattacke am besten verhalten.

Diskutieren und reflektieren Sie anhand der folgenden Anregungen:

Welche Konsequenzen kann Cyberkriminalität für Betroffene haben
- ➔ Finanzielle Konsequenzen
- ➔ Datendiebstahl
- ➔ Rufschädigung
- ➔ Juristische Konsequenzen

Wie kann man sich vor Cyberattacken schützen?
- ➔ Vorsichtiger Umgang mit Daten
- ➔ Software immer auf dem aktuellen Stand halten
- ➔ Komplexe Passwörter anlegen und geheim halten
- ➔ Keine vertraulichen Informationen im Netz teilen
- ➔ Skeptischer Umgang mit E-Mail Anhängen und neuen Bekannten im Netz

Unterrichtsszenarien	Kurze Zusammenfassung
Einstieg	Einführung ins Thema mit Sammlung von Erfahrungsberichten
Einstieg	Einführung zu Cybersecurity und Cyberkriminalität mittels Online Training
Vertiefung	Folgen von Cyberkriminalität mittels Videos
Vertiefung	Einzelaufgabe zur Abwehr von Cyberattacken
Vertiefung	Quiz – Security im Alltag
Abschluss	Abschluss mit Rückbezug auf eingangs geschilderte Erfahrungsberichte

5.2 Für Fortgeschrittene

Fragen Sie Ihre Schüler/innen, wer bereits persönlich oder im Bekanntenkreis Erfahrungen mit Internetkriminalität gemacht hat. Dazu zählen z.B. folgende Bereiche:

- *Phishing E-Mail bekommen*
- *Virus auf dem Computer*
- *Chat mit einer Person, welche vorgibt jemand anderes zu sein (Fake-Profil)*
- *Datendiebstahl*
- *Gehackte Social-Media-Accounts, z.B. Facebook- oder Instagramkonten*

Nachdem Ihre Schüler/innen wissen, was unter Cyberkriminalität zu verstehen ist, soll es nun um die **verschiedenen Akteure** gehen. Diese haben unterschiedliche „Zielgruppen“ bzw. Opfer, gehen anders vor und werden von diversen Motiven angetrieben. In der folgenden Tabelle wird ein Überblick über die populärsten Akteure und deren Motive geboten.

	HACKTIVISTEN	**CYBERTERRORISMUS/ STAATLICHE SPIONAGE**	**ORGANISIERTE KRIMINALITÄT**
OPFER	Firmen, größere Systeme, Medien und Politik	Einzelpersonen, Firmen und Institutionen	Privatpersonen und Firmen
METHODE	Überwindung von Sicherheitssystemen, Protest und Propaganda	Erpressung und Ausspionieren von Daten und Informationen	Datenklau durch die bewusste Täuschung von anderen Personen
MOTIV	Politische/ ideologische Ziele oder Anerkennung in Hackerkreisen	Politische bzw. wirtschaftliche Ziele, wie z.B. der Gefährdung der öffentlichen Sicherheit	Geld

Aber nicht nur die Akteure variieren, sondern auch die Art der Cyberattacke kann sehr unterschiedlich ausfallen. Um das Wissen Ihrer Schüler/innen zu überprüfen, bearbeiten Sie das Arbeitsbaltt „Arten von Cyberattacken“ in der Kopiervorlage des Booklets „Digitalität und Kriminalität“ (hier).

Was sollte vor einer Cyberattacke geklärt sein? Inhaltliche Grundlage für ein Unterrichtsgespräch:

- **BUSINESS CONTINUITY:** Welchen Einfluss hat der Ausfall von bestimmten Systemen auf das Tagesgeschäft? Um bei einem Angriff weiterhin dem Kundengeschäft nachgehen zu können, sollten Unternehmen für sehr wichtige Systeme über den ganzen Globus verteilte Datencenter mit den exakt gleichen Daten haben. So stehen diese Daten im Notfall weiterhin zur Verfügung.
- **INCIDENT RESPONSE:** Welchen Plan verfolgen wir, wenn eine Cyberattacke stattfindet? Dafür sollte man z.B. erfahrene und vertrauenswürdige Experten einbinden, die das Unternehmen dabei unterstützen, die richtigen Maßnahmen zu finden. Damit die Experten schlimmeres verhindern und unverzüglich mit der Arbeit beginnen können, müssen ihnen die technischen und finanziellen Ressourcen unverzüglich zur Verfügung gestellt werden.

Gerade für Unternehmen stellen Cyberattacken eine Gefahr dar. Dabei sind kleine und mittelständische Unternehmen genauso betroffen, wie die großen. Es ist also unabhängig von der Unternehmensgröße wichtig, Vorsorgemaßnahmen zu ergreifen, um sich vor potentiellen Cyberattacken zu schützen. In diesem kurzen online Quiz können Ihre Schüler/innen herausfinden, ob sie wissen, welche Schutzmaßen ein Unternehmen ergreifen sollte.

Wenn alle Schutzmaßnahmen versagt haben und es im Unternehmen doch zu einer Cyberattacke gekommen ist, gibt es einige Dinge zu beachten. Genaueres wird Peter Stinner, Cyber Defense Spezialst, im folgenden Video erklären.

Diskutieren Sie zum Abschluss mit Ihren Schüler/innen, wie verantwortungsbewusstes Verhalten im Netz aussieht, z.B.

- ➔ Sichere Passwörter (Diskussionsanregungen, zur Passworterstellung finden Sie **hier**)
- ➔ Keine persönlichen Daten preisgeben
- ➔ Freundschaftsanfragen in sozialen Netzwerken nur von Personen annehmen, die man auch im realen Leben kennt
- ➔ Keine E-Mail-Anhänge von unbekannten Absendern öffnen oder runterladen

Unterrichtsszenarien	Kurze Zusammenfassung
Einstieg	Einführung ins Thema mit Sammlung von Erfahrungsberichten
Einstieg	Einführung zu Motiven hinter Cyberattacken
Vertiefung	Arbeitsblatt Arten Cyberattacke
Vertiefung	Video zu Maßnahmen im Angriffsfall
Vertiefung	Diskussion: Was sollte vor einer Cyberattacke geklärt werden?
Vertiefung	Online Training zu Schutzmaßnahmen von Unternehmen
Abschluss	Diskussion: Wie sieht verantwortungsbewusstes Verhalten aus?

6 Literatur und Links

Digitale Lernwerktatt:

https://digitale-lernwerkstatt.com/ Weitere Lernmodule und Unterrichtsmaterialien kostenfrei zu vielen digitalen Themen

Videos:

- https://www.youtube.com/watch?v=i2TVQdjw7lc Sophos Security Software – Wie WannaCry Ransomware funktioniert, englisch
- https://www.youtube.com/watch?v=v_goLwpQliw heise online → sehr detaillierte Beschreibung der Funktionalität von WannaCry

Weitere Links:

- https://krebsonsecurity.com/2017/05/global-wana-ransomware-outbreak-earned-perpetrators-26000-so-far/
- https://krebsonsecurity.com/2017/05/microsoft-issues-wanacrypt-patch-for-windows-8-xp/
- https://www.bsi.bund.de