Lerneinheit

[Cyberkriminalität]

Projekt: B-SAFE
Nummer: 2018-1CZ01-KA204-048148

Funded by the
Erasmus+ Programme
of the European Union

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein."

Co-funded by the
Erasmus+ Programme
of the European Union

Cyber-Kriminalität

Einführung

Sicherlich haben Sie bereits auch mal eine E-Mail erhalten, in der die Änderung Ihrer Passwörter für Ihre Bankkonten oder die Forderung von Zahlungsrückständen oder Schulden verlangt wird. Diese E-Mails sehen im Allgemeinen nicht glaubwürdig aus, es gibt keine klare Identifizierung der Person, der Institution und die sprachliche Formulierung ist meist weniger seriös. Aber viele Menschen wollen der Forderung nachkommen, sie fürchten oft, dass sie etwas vernachlässigen. Was für eine nächste Überraschung sorgt, nämlich dass ihr Bankkonto überzogen wird und die Schuld ungültig war. Das letzte Beispiel für Cyberkriminalität ist die Software-Piraterie, d.h. die Verwendung von illegalen Kopien der Software unter Missachtung der Urheberrechte und ihres Preises. Das sind Beispiele der Cyberkriminalität, welche jede Person die online ist treffen können.

Cyberkriminalität ist ein seit langem etabliertes Phänomen, das untrennbar mit der globalen Konnektivität verbunden ist. Jede kriminelle Aktivität, bei der ein Computer entweder als Instrument, Ziel oder Mittel zur Verübung weiterer Straftaten eingesetzt wird, fällt in den Bereich der Cyberkriminalität. Eine verallgemeinerte Definition von Cyberkriminalität ist "ungesetzliche Handlungen, bei denen der Computer entweder ein Instrument oder ein Ziel oder beides ist" (IT-Gesetz 2000).

Cyberkriminalität wurde zur Beschreibung eines breiten Spektrums von Straftaten verwendet, darunter Straftaten gegen Computerdaten und -systeme, computerbezogene Fälschung und Betrug, Inhaltsdelikte und Urheberrechtsverletzungen. Unsere zunehmende Abhängigkeit von Computern und digitalen Netzwerken macht die Technologie selbst zu einem verlockenden Ziel; entweder zur Gewinnung von Informationen oder als Mittel zur Verursachung von Störungen und Schäden.

Praktische Relevanz - Hierfür benötigen Sie das Wissen und die Fähigkeiten

Nachdem Sie sich durch diese Inhaltseinheit gearbeitet haben, kennen Sie die Definitionen der wichtigsten Begriffe im Zusammenhang mit Kriminalität im Cyberspace, Sie können verschiedene Arten und Methoden der Cyberkriminalität erkennen und sich vor Verbrechen aus dem virtuellen Raum schützen. Sie werden auch mit den gefährlichen Aspekten nicht nur für Erwachsene, sondern auch für Ihre Kinder vertraut sein.

Co-funded by the
Erasmus+ Programme
of the European Union

1.Die Rolle der Cyberkriminalität im Internet

Cyberkriminalität ist die Kehrseite der Cybersicherheit - ein riesiges Spektrum schädlicher und illegaler Aktivitäten, die mit Hilfe von Computern und dem Internet durchgeführt werden. Diese Einheit wird Ihnen helfen, die Cyberkriminalität zu verstehen und wie Sie sich persönlich, Ihre Kinder und Ihre Organisation dagegen verteidigen können.

Die meisten, aber nicht alle Cyberkriminalitäten werden von Cyberkriminellen oder HackerInnen begangen, die Geld verdienen wollen. Cyberkriminalität wird von Einzelpersonen oder Organisationen begangen. Einige Cyberkriminelle sind organisiert, verwenden fortschrittliche Techniken und sind technisch hoch qualifiziert. Andere sind unerfahrene HackerInnen. Selten zielt die Cyberkriminalität darauf ab, Computer aus anderen Gründen als aus Profitstreben zu beschädigen. Dies können politische oder persönliche Gründe sein.

Was versteht man unter Cyberkriminalität? Cyberkriminalität ist definiert als ein Verbrechen, bei dem ein Computer Gegenstand der Straftat ist (Hacking, Phishing, Spamming) oder als Werkzeug zur Begehung einer Straftat verwendet wird (Kinderpornographie, Hassverbrechen).

Hier sind einige konkrete Beispiele für die verschiedenen Arten von Cyberkriminalität:

- E-Mail- und Internet-Betrug.
- Identitätsbetrug (bei dem persönliche Informationen gestohlen und verwendet werden).
- Diebstahl von Finanz- oder Kartenzahlungsdaten.
- Diebstahl und Verkauf von Unternehmensdaten.
- Cybererpressung (Geldforderung, um einen drohenden Angriff zu verhindern).
- Ransomware-Angriffe (eine Art von Cybererpressung).
- Cryptojacking (bei dem Hacker mit Hilfe von Ressourcen, die sie nicht besitzen, Kryptogeld abbauen).
- Cyberspionage (bei der Hacker auf Regierungs- oder Firmendaten zugreifen).

Wenn wir in Anlehnung an die oben genannten Beispiele über Cyberkriminalität sprechen, sprechen wir gewöhnlich von zwei Hauptkategorien von Straftaten:

1. Ein an ein Netz angeschlossener Computer ist das Ziel der Straftat - dies ist der Fall bei Angriffen auf die Vertraulichkeit, Integrität oder Verfügbarkeit von Netzen.
2. eine Straftat, die mit Hilfe von Computern begangen wird, die an ein Netzwerk angeschlossen sind, und der damit verbundenen Informations- und Kommunikationstechnologie - dies ist der Fall bei Angriffen wie Diebstahl, Betrug und Fälschung.

Der folgende Text konzentriert sich auf Straftaten, die mit Hilfe von Computern begangen wurden.

Die Cyberkriminellen bestehen aus verschiedenen Gruppen und Kategorien. Die Arten der Cyberkriminalität werden zur Beschreibung von Straftaten (wie Phishing usw.) verwendet und sind in den folgenden Kategorien enthalten.
Diese Typologie konzentriert sich auf den Gegenstand des Rechtsschutzes: "Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und -systemen"; inhaltsbezogene Straftaten; und urheberrechtsbezogene Straftaten. Die vierte Kategorie der "computerbezogenen Straftaten" konzentriert sich nicht auf den Gegenstand des Rechtsschutzes, sondern auf die Methode, mit der die Straftat begangen wurde. Sie kann zu gewissen Überschneidungen zwischen den Kategorien führen.

Cyberkriminalität Kategorien

Betrachten wir nun jede einzelne dieser Kategorien:

Verstöße gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und -systemen
Alle Straftaten in dieser Kategorie richten sich gegen eines der drei Rechtsprinzipien der Vertraulichkeit, Integrität und Verfügbarkeit.

- Illegaler Zugang (Hacking, Cracking)
- Illegales Abhören (das Abhören ohne Recht)
- Dateninterferenz (Eingabe von bösartigen Codes, z.B. Viren)
- Systemstörungen (Eingeben, Übertragen, Beschädigen, Löschen, Verschlechtern, Verändern oder Unterdrücken von Computerdaten, z.B. Viren, die Computersysteme stoppen oder verlangsamen)

Beispiel
Im Jahr 2017 löste der angeblich von Nordkorea verübte WannaCry-Angriff eine Art von Lösegeldforderung aus, die nicht nur Inhalte auf Benutzergeräten blockiert, sondern sich auch rasch selbst verbreitet. WannaCry infizierte 300.000 Computer auf der ganzen Welt, und die Nutzer wurden aufgefordert, Hunderte von Dollar für die Entschlüsselung und Wiederherstellung ihrer Daten zu zahlen.

Computerbezogene Straftaten
In diese Kategorie fallen viele Straftaten, für deren Begehung ein Computersystem erforderlich ist. Im Gegensatz zu früheren Kategorien sind diese weit gefassten Straftaten oft nicht so streng, was den Schutz der Rechtsgrundsätze betrifft.

- Computerbezogener Betrug
- computerbezogene Fälschung
- Phishing
- Identitätsdiebstahl
- Missbrauch von Geräten

Beispiel
In den Jahren 2013-2016 kam es bei Yahoo zu einem Datenbruch, der zum Diebstahl von 3 Milliarden Benutzerkonten führte. Bei einigen dieser Konten kamen die AngreiferInnen in den Besitz privater Informationen und Passwörter, die für den Zugriff auf Benutzerkonten in anderen Online-Diensten

verwendet werden konnten. Viele dieser Daten sind heute entweder kostenlos oder gegen einen Preis im Dark Web verfügbar.

Inhaltsbezogene Verstöße
Diese Kategorie umfasst:

- Erotisches oder pornographisches Material
- Kinderpornographie
- fremdenfeindliches Material - Rassismus, Hassreden, Gewaltverherrlichung
- Beleidigungen im Zusammenhang mit religiösen Symbolen
- Illegale Glücksspiele und Online-Spiele
- Verleumdung und falsche Informationen
- Spam und verwandte Bedrohungen

Die Entwicklung von Rechtsinstrumenten, die sich mit dieser Kategorie befassen, wird viel stärker von nationalen Ansätzen beeinflusst, die grundlegende kulturelle und rechtliche Prinzipien berücksichtigen können. Bei illegalen Inhalten unterscheiden sich die Werte- und Rechtssysteme der einzelnen Gesellschaften erheblich.

Beispiel
Der berüchtigte Pädophile Matthew Falder (d.h. eine Person, die durch ein Kind sexuell erregt wird), ein britischer Akademiker mit einem Doktortitel der Universität Cambridge, wurde 2017 wegen über 137 Straftaten angeklagt, die gegen 46 Personen begangen wurden, darunter die vorsätzliche Förderung von Vergewaltigung und sexueller Aktivität mit einem Familienmitglied eines Kindes, die Anstiftung zur sexuellen Ausbeutung eines Kindes sowie der Besitz und die Verbreitung von Kinderpornografie, neben anderen Straftaten (Dennison, 2018; Vernalls und McMenemy, 2018). Er erpresste seine Opfer zu demütigenden, abscheulichen, erniedrigenden und missbräuchlichen Handlungen gegen sich selbst (z.B. sich selbst verletzen und eine verschmutzte Toilettenbürste ablecken) und gegen andere und hielt diese Handlungen auf Bildern und Videos fest (Davies, 2018; Dennison, 2018). Anschließend stellte er die Bilder und Videos auf verletzte Kernseiten (wie Hurt 2 the Core, heute nicht mehr vorhanden) zur Verfügung, die auf Vergewaltigung, Mord, Sadismus, Folter und pädophile Inhalte spezialisiert sind (McMenemy, 2018).

Urheberrechtsbezogene Verstöße
Die Digitalisierung hat die Tür für neue Urheberrechtsverletzungen geöffnet. Zu den häufigsten Urheberrechtsverletzungen gehören der Austausch von urheberrechtlich geschützten Liedern, Dateien und Software in Filesharing-Systemen oder über Share-Hosting-Dienste und die Umgehung von Digital-Rights-Management-Systemen (DRM). Dies ist der häufigste Teil der Cyberkriminalität, der im Allgemeinen von der gesamten Gesellschaft toleriert wird, aber wir sollten davon ausgehen, dass es sich dabei um die illegale Handlung mit der möglichen Folge eines falschen Verhaltens handelt.

Beispiel
Die häufigsten Beispiele für Urheberrechtsverletzungen sind das illegale Kopieren von Software auf Ihrem Heimcomputer oder das Herunterladen von Musik oder Filmen aus öffentlichen Online-Shops (z.B. ShareRapid, MegaRapid).

1.Wissen anwenden

Übung WAHR/FALSCH

Situation: Wenn die Musik oder der Film im Internet veröffentlicht ist, kann ich sie legal herunterladen.
Aufgabe: Wählen Sie die richtigen Optionen nach dem Richtig/Falsch-Prinzip aus:

- wahr
- falsch

Übung MULTIPLE CHOICE

Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus: Mehr Antworten könnten wahr sein.

Markieren Sie die richtigen Kategorien von Cyberkriminalität

- Computerbezogene Straftaten
- Physischer Diebstahl eines Computers, Tablets oder Telefons
- Inhaltsbezogene Straftaten
- Urheberrechtsbezogene Verstöße

Übung ANTWORTEN ZUORDNEN

Aufgabe: Aufgabe: Wählen Sie die richtigen Optionen aus der untenstehenden Auswahl aus.

_____ deckt viele Straftaten ab, für deren Begehung ein Computersystem erforderlich ist. Im Gegensatz zu früheren Kategorien sind diese allgemeinen Straftatbestände oft nicht so streng, was den Schutz der Rechtsgrundsätze betrifft.
_____ umfasst Verstöße gegen Rechtsinstrumente, die stärker von nationalen Ansätzen beeinflusst sind, die grundlegende kulturelle und rechtliche Prinzipien berücksichtigen können. Die Werte- und Rechtssysteme unterscheiden sich zwischen den Gesellschaften erheblich.
_____ umfasst den Austausch urheberrechtlich geschützter Lieder, Dateien und Software in Filesharing-Systemen oder durch Share-Hosting-Dienste und die Umgehung von DRM-Systemen (Digital Rights Management)

Urheberrechtsbezogene Straftaten, Computerbezogene Straftaten, Inhaltsbezogene Straftaten

2. Die Methoden und Beispiele der Cyberkriminalität

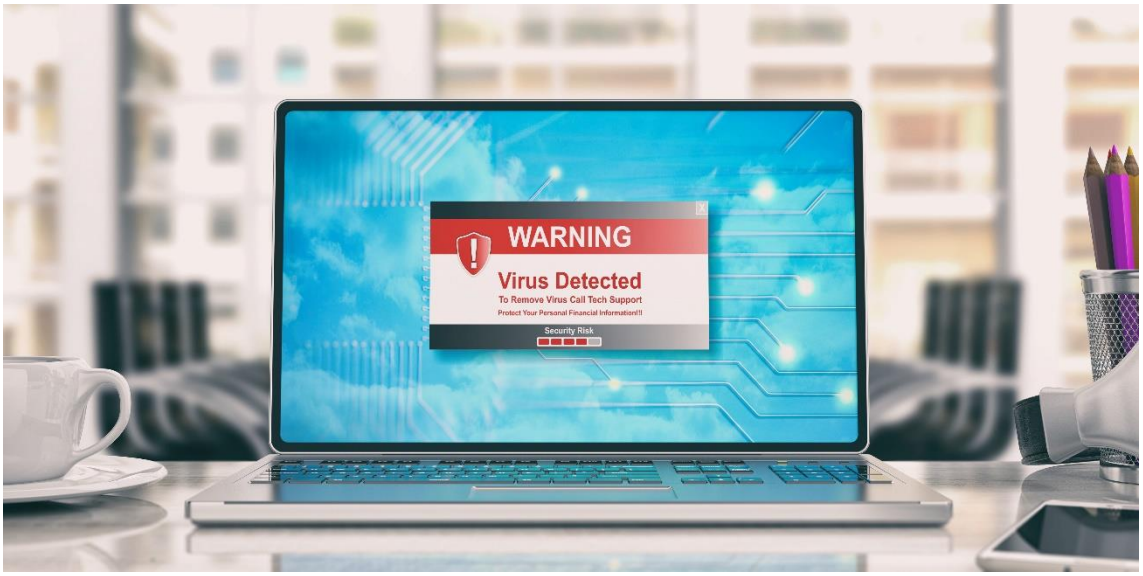
Es handelte sich dabei um vier Kategorien, die bei der Cyberkriminalität unterschieden werden. Nun wollen wir uns näher mit **der Rolle von Computern bei der Cyberkriminalität und den Angriffsmethoden im Cyberspace befassen:**

Computer spielen bei Verbrechen vier Rollen - sie dienen als **Objekte, Subjekte, Werkzeuge und Symbole**. Computer sind Objekte von Verbrechen, wenn sie sabotiert oder gestohlen werden. Computer spielen die Rolle von Subjekten, wenn sie das Umfeld sind, in dem Technologien Verbrechen begehen. Angriffe durch Computerviren fallen in diese Kategorie. Wenn automatisierte Verbrechen stattfinden, sind Computer die Subjekte von Angriffen. Die dritte Rolle von Computern in der Kriminalität ist die eines Werkzeugs, das es Kriminellen ermöglicht, falsche Informationen zu produzieren oder Verbrechen zu planen und zu kontrollieren. Schließlich werden Computer auch als Symbole benutzt, um Opfer zu täuschen.
Die häufigste ist die Cyberkriminalität, die als Subjekt dient. Die wichtigsten Methoden, einen Computer als kriminelles Subjekt zu benutzen, sind

- Malware
- Hacken von
- Spam

- Phishing
- Verteilte DoS-Angriffe (DDoS)

Die wichtigsten Angriffsmethoden



Definition
Malware ist eine allgemeine Bezeichnung für bösartige Software, die sich zwischen Computern ausbreitet und den Betrieb von Computern stört. Malware kann zerstörerisch sein, indem sie beispielsweise Dateien löscht oder Systemabstürze verursacht, kann aber auch zum Diebstahl persönlicher Daten verwendet werden.

Es gibt viele **Formen von Malware**. Einige davon sind die folgenden:

- **Viren** können leichte Computerfunktionsstörungen verursachen, können aber auch schwerwiegendere Auswirkungen haben, indem sie Hardware, Software oder Dateien beschädigen oder löschen.
- **Würmer** sind selbstreplizierende Programme, aber sie können sich autonom, innerhalb und zwischen Computern verbreiten, ohne dass ein Host oder menschliches Handeln erforderlich ist. Die Auswirkungen von Würmern können daher schwerwiegender sein als Viren und ganze Netzwerke zerstören.
- **Trojaner** sind eine Form von Malware, die als legitime Programme erscheinen, aber den illegalen Zugriff auf einen Computer erleichtern. Sie können Funktionen, wie z.B. Datendiebstahl, ohne das Wissen des Benutzers ausführen und können Benutzer austricksen, indem sie eine Routineaufgabe ausführen und dabei versteckte, nicht autorisierte Aktionen ausführen.
- **Spyware** ist Software, die in die Privatsphäre der Benutzer eindringt, indem sie sensible oder persönliche Daten von infizierten Systemen sammelt und die besuchten Websites überwacht.

Definition
Hacking ist ein gängiger Prozess, der zur Verletzung der Privatsphäre und vertraulicher Informationen führt. Die Schwachstellen eines Systems oder Lücken in einem Netzwerk werden identifiziert und es wird auf private Details zugegriffen. Daher wird Hacking auch als unbefugtes Eindringen bezeichnet.

Hacking wird jedoch nicht immer als Diebstahl wahrgenommen und für produktive Zwecke eingesetzt. Diese Art von Hacking, bei der gute Absichten im Spiel sind, wird als ethisches Hacking bezeichnet. Diese Art von Hacking wird zur Sicherung des Betriebssystems durchgeführt.

Hacker können je nach der Absicht, ein System zu hacken, in verschiedene Kategorien eingeteilt werden, z. B. in Weißer Hut, Schwarzer Hut und Grauer Hut.

White-Hat-Hacker - Ethische Hacker
Sie hatten nie die Absicht, ein System zu schädigen, sondern versuchen vielmehr, im Rahmen von Penetrationstests und Schwachstellenbewertungen Schwachstellen in einem Computer oder einem Netzwerksystem herauszufinden. Ethisches Hacking ist nicht illegal und gehört zu den anspruchsvollen Tätigkeiten in der IT-Branche. Zahlreiche Unternehmen stellen Ethik-Hacker für Penetrationstests und Schwachstellenbewertungen ein.

Hacker mit grauem Hut
Sie sind eine Mischung aus Schwarzhut- und Weißhut-Hackern. Sie handeln ohne böswillige Absicht, nutzen aber zu ihrem Vergnügen eine Sicherheitsschwäche in einem Computersystem oder -netzwerk aus, ohne die Erlaubnis oder das Wissen des Besitzers bzw. der Besitzerin. Sie beabsichtigen, die EigentümerIn auf die Schwachstelle aufmerksam zu machen und von ihnen Anerkennung oder eine kleine Belohnung zu erhalten.

Schwarzhut-Hacker - Cracker
Sie hacken, um sich unbefugten Zugang zu einem System zu verschaffen und dessen Betrieb zu schädigen oder sensible Informationen zu stehlen. Black-Hat-Hacking ist aufgrund seiner bösen Absichten, zu denen der Diebstahl von Unternehmensdaten, die Verletzung der Privatsphäre, die Beschädigung des Betriebssystems, die Blockierung der Netzwerkkommunikation usw. gehören, immer illegal.

Definition
Bei **Spam** handelt es sich um unerwünschte oder Junk-E-Mails, die in der Regel in großen Mengen an unzählige EmpfängerInnen in der ganzen Welt verschickt werden und häufig mit pharmazeutischen Produkten oder Pornographie in Verbindung stehen. Spam-E-Mails werden auch zum Versenden von Phishing-E-Mails oder Malware verwendet und können dazu beitragen, den potenziellen Nutzen für Kriminelle zu maximieren).

Die Kriminalität entfernt sich von den traditionellen Methoden wie Gewalt, Drogen oder Einbruch, und die Internet-Kriminalität nimmt an Bedeutung zu. Dies geht einher mit dem Trend, der sich aus der Zunahme von Online-Geschäften und -Kommunikation ergibt. Die Opfer von Verbrechen können alles verlieren, was einen Wert hat - Sicherheit, Frieden, Geld oder Eigentum.

Exkurs
Die erste Studie, die die emotionalen Auswirkungen der Cyberkriminalität untersucht hat, zeigt, dass die stärksten Reaktionen der Opfer wütend (58 %), verärgert (51 %) und betrogen (40 %) sind, und in vielen Fällen geben sie selbst dafür, dass sie angegriffen wurden. Nur 3 % glauben nicht, dass ihnen das passieren wird, und fast 80 % erwarten nicht, dass Cyberkriminelle vor Gericht gestellt werden - was eine ironische Abneigung gegen Maßnahmen und ein Gefühl der Hilflosigkeit zur Folge hat.

Definition
Phishing - Eine Phishing-Kampagne liegt vor, wenn Spam-E-Mails oder andere Kommunikationsformen massenhaft verschickt werden, mit der Absicht, die Empfänger zu etwas zu verleiten, das ihre Sicherheit oder die Sicherheit der Organisation, für die sie arbeiten, untergräbt.

Die Nachrichten einer Phishing-Kampagne können infizierte Anhänge oder Links zu bösartigen Websites enthalten. Oder sie können den Empfänger bzw. der Empfängerin auffordern, mit vertraulichen Informationen zu antworten.
Beispiel
Ein berühmtes Beispiel für einen Phishing-Betrug aus dem Jahr 2018 war einer, der während der Weltmeisterschaft stattfand. Berichten von Inc. zufolge betraf der Phishing-Betrug im Zusammenhang mit der Weltmeisterschaft E-Mails, die an Fußballfans gesendet wurden. Diese Spam-E-Mails versuchten, die Fans mit gefälschten Gratisreisen nach Moskau, dem Austragungsort der Weltmeisterschaft, zu locken. Personen, die die in diesen E-Mails enthaltenen Links öffneten und darauf klickten, wurden ihre persönlichen Daten gestohlen.

Definition
Verteilte DoS-Angriffe (Distributed DoS-Angriffe) sind eine Art von Cyberkriminalität, die von Cyberkriminellen benutzt wird, um ein System oder Netzwerk zum Einsturz zu bringen. Manchmal werden verbundene IoT-Geräte (Internet der Dinge) verwendet, um DDoS-Angriffe zu starten. Ein DDoS-Angriff überwältigt ein System, indem er eines der Standardkommunikationsprotokolle verwendet, mit denen das System mit Verbindungsanfragen gespammt wird.

Beispiel
Ein berühmtes Beispiel für diese Art von Angriff ist der DDoS-Angriff 2017 auf die Website der UK National Lottery. Dadurch wurden die Website und die mobile App der Lotterie offline geschaltet und die BürgerInnen des Vereinigten Königreichs am Spielen gehindert.

Zu den am häufigsten begangenen Cyberkriminalität gehören:

Online-Imitation
Dieses Verbrechen ist eine der am häufigsten begangenen Cyberkriminalität, die es gibt. Für diese kriminelle Handlung ist es typisch, den Namen, die Domänenadresse, die Telefonnummer oder andere identifizierende Informationen einer anderen Person ohne Zustimmung zu verwenden, um Schaden anzurichten oder Betrug zu begehen, was ein Verbrechen ist.

Beispiel
Claire begann, von Fremden belästigt zu werden, nachdem jemand im Internet einen Posting gemacht hatte, in dem sexuelle Dienstleistungen in ihrem Namen angeboten wurden. Der Beitrag enthielt private Informationen, darunter ihre Telefonnummer und ihre Wohnadresse.

Cyberstalking
Physisches Stalking kann in Form von persönlichem Verfolgen, heimlichem Beobachten, hartnäckigem Anrufen und Schreiben von SMS zur Manipulation und verschiedenen anderen Mitteln zur unerwarteten Annäherung an das Opfer erfolgen. Der Unterschied des Cyberstalking besteht darin, dass es über Online-Technologien wie E-Mail, soziale Netzwerke, Instant Messaging, online verfügbare persönliche Daten begangen wird - alles im Internet kann von Cyberstalkern genutzt werden, um unangemessenen Kontakt mit ihren Opfern aufzunehmen

Co-funded by the
Erasmus+ Programme
of the European Union

Beispiel
Nachdem John und seine Freundin sich getrennt hatten, begann er sie zu verfolgen, indem er ein GPS-fähiges Prepaid-Handy unter ihrem Auto platzierte. John verfolgte die Bewegungen seiner Ex-Freundin und folgte ihr, indem er sich online in das Handy-Konto einloggte. Außerdem rief John seine Ex-Freundin über 200 Mal am Tag an.

Cybermobbing

Wir können dieses Verbrechen beim Namen nennen, wenn Menschen soziale Medien oder das Internet nutzen, um andere einzuschüchtern, zu belästigen, zu bedrohen oder herabzusetzen. Im Allgemeinen kann dieses Verhalten ein Verbrechen darstellen, wenn eine Person das Internet oder eine andere Form der elektronischen Kommunikation benutzt, um eine andere Person einzuschüchtern, zu belästigen oder zu erschrecken.

Beispiele
Während er mit einer Juniorenmannschaft unterwegs ist, macht einer der Spieler ein peinliches Foto von einem Mädchen, das er auf der Eisbahn getroffen hat. Er veröffentlicht das Foto dann auf Facebook und schickt es an alle anderen Spieler der Mannschaft. Das Foto wird dann verteilt. Drei von Pauls Mannschaftskameraden schicken ihm Texte, in denen sie ihn für die Niederlage der Mannschaft verantwortlich machen und ihm sagen, dass er nicht weiß, wie man das Spiel spielt. Paul hat Angst, es seinem Trainer bzw. seiner Trainerin zu sagen, und seine Eltern tolerieren das Mobbing während der gesamten Hockeysaison. Er kehrt in der nächsten Saison nicht zum Hockey zurück.

Was ist der Unterschied zwischen Cybermobbing und Cyberstalking?

Cybermobbing	Cyberstalking
Cybermobbing ist ständiger Kontakt mit der Person; man sagt der Person verletzende Dinge oder erzählt anderen unwahren Informationen über die Person. Der Täter richtet zum Beispiel die Facebook-Gruppe "Ich hasse..." ein und lädt alle Freunde ein, ihr beizutreten.	Cyberstalking ist eine Obsession, so viel wie möglich über die Person herauszufinden (ohne sie tatsächlich zu fragen). Zum Beispiel findet der Täter bzw. die Täterin heraus, wo die Person geboren wurde, ob die Person verheiratet ist usw.

Identitätsdiebstahl und Datendiebstahl

Unter Identitätsdiebstahl versteht man den Diebstahl persönlicher Identifikationsdaten, um illegale Handlungen zu begehen, wie z.B.: die Eröffnung eines Kreditrahmens, die Anmietung eines Hauses, den Kauf von Waren oder Dienstleistungen, Auktions- und Lohnbetrug oder Erpressung.

Datendiebstahl ist die Handlung des illegalen Besitzes sensibler Daten, zu denen unverschlüsselte Kreditkarteninformationen, die in Unternehmen gespeichert sind, Geschäftsgeheimnisse, geistiges Eigentum, Quellcode, Kundeninformationen und Mitarbeiterdaten gehören.

Beispiel
Das Marriott wurde im Jahr 2018 gehackt, wo 383 Millionen Gastdatensätze und über 5 Millionen Reisepassnummern gestohlen wurden, Datenverletzungen haben an Häufigkeit und Schwere zugenommen. Diese Daten könnten auf dem Schwarzmarkt verkauft werden, und jeder kann sie missbrauchen und die andere Identität verwenden.

Finanzkriminalität

Diese Vielfalt umfasst Aktivitäten, die auf unehrliche Weise Reichtum für diejenigen erzeugen, die an dem fraglichen Verhalten beteiligt sind. Sie besteht in der Ausnutzung von Insider-Informationen oder dem Erwerb von Eigentum einer anderen Person durch Täuschung zur Erlangung eines materiellen Vorteils. Unter Finanzkriminalität versteht man gemeinhin die folgenden Delikte: Betrug, Geldwäsche, Bestechung, Bestechlichkeit und Korruption und viele andere.

Beispiel
Zu den bekanntesten Finanzverbrechen der letzten Zeit gehören der Enron-Skandal, bei dem der Energiekonzern weit verbreiteten Betrug und Korruption beging, und der Investitionsskandal von Bernie Madoff, bei dem Madoff vorgab, eine erfolgreiche Investmentfirma zu haben, in Wirklichkeit aber nur Geld von neuen Kunden stahl und es älteren Kunden gab (dies wird als Ponzi-Schema bezeichnet, und Madoff führte das größte in der Geschichte). Madoff wurde wegen zahlreicher Straftaten verurteilt, darunter Geldwäsche und viele verschiedene Arten von Betrug.

Cyberkriminalität wird oft von jemandem in Ihrer Nähe begangen - zum Beispiel in Ihrem Unternehmen. Diese Art der Cyberkriminalität wird als interner Betrug bezeichnet und bezieht sich auf eine Art von Betrug, der von einer Einzelperson gegen eine Organisation begangen wird. Bei dieser Art von Betrug beteiligt sich ein Betrüger an Aktivitäten, die darauf abzielen, zu betrügen, Eigentum zu veruntreuen oder die Vorschriften, Gesetze oder Richtlinien eines Unternehmens zu umgehen. Zum Beispiel umfasst interner Betrug Aktivitäten wie die absichtliche Nichtmeldung von Transaktionen, die Durchführung nicht autorisierter Transaktionen und die absichtliche Fehlbesetzung von Positionen.
Interner Betrug kann in zwei große Kategorien eingeteilt werden: Veruntreuung und Identitätsdiebstahl. Im Falle der Veruntreuung wird das Geld direkt von den Organisationen abgezogen, und im Falle des Identitätsdiebstahls werden die persönlichen Daten eines Kunden bzw. einer Kundin vom Mitarbeitenden zur Erzielung eines Gewinns veruntreut. Beispiele für internen Betrug sind

- Der Diebstahl des Geldes eines Kunden bzw. einer Kundin
- Kreditmissbrauch eines Kunden bzw. einer Kundin
- Geldwäscherei
- Beschaffungsbetrug
- Datendiebstahl

Auf der anderen Seite werden die betrügerischen Aktivitäten von unternehmensfremden Personen als externer Betrug bezeichnet. Es handelt sich um den Diebstahl von Geld oder Aktien durch Personen außerhalb des Unternehmens. Beispiele für externen Betrug sind

- Identitätsdiebstahl - Übernahme der Kontrolle über eine virtuelle Identität der Person
- Fälschung von Rechnungsangaben (Änderung der Kontonummer des Zahlungsempfängers)
- Fälschung von Auftragsdetails, so dass Waren an den falschen Bestimmungsort geliefert werden

- Die Stimme einer Person imitieren oder ihre Unterschrift fälschen
- Fälschung von E-Mails

Es gibt verschiedene Zwecke von Cyber-Angriffen im Cyberspace, von moderaten bis hin zu gnadenlosen, die 4 typischsten Ziele sind:

- Vandalismus (häufige Angriffe auf Regierungs-Websites)
- Propaganda (Verbreitung von politischen Nachrichten hauptsächlich über das Internet)
- Zugangsverweigerung (Angriffe gegen z.B. Streitkräfte, die Computer und Satelliten zur Kommunikation nutzen)
- Netzangriffe auf die Infrastruktur (Angriffe auf Übertragungssysteme der Unternehmen der Energie-, Gas-, Heizungs-, Erdölindustrie und Kommunikationsinfrastruktur, die für Cyber-Angriffe empfindlich sind, usw.)

2.Wissen anwenden

Übung SINGLE CHOICE

Situation: Was sind verteilte DoS-Angriffe (DDoS)?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist wahr.

- wenn Spam-E-Mails oder andere Kommunikationsformen massenhaft verschickt werden
- eine Art von Cyberkriminalität, die von Cyberkriminellen benutzt wird, um ein System oder Netzwerk zum Einsturz zu bringen
- Unerwünschte oder Junk-E-Mails, die typischerweise in Massen an unzählige EmpfängerInnen in der ganzen Welt verschickt werden
- die unbefugte Benutzung von oder der unbefugte Zugang zu Computern oder Netzwerkressourcen, die identifizierte Sicherheitslücken in Netzwerken ausnutzen

Übung SINGLE CHOICE

Situation: Welche Aktivitäten kennzeichnet folgende Person: "Hacker mit grauem Hut"?
Aufgabe: Wählen Sie die richtige Option nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist wahr.

a) Es ist eine Person, die unwahre Informationen über eine andere Person verbreitet.
b) Es ist eine Person, die versucht, persönliche Identifikationsinformationen zu stehlen.
c) Es ist eine Person, die sich unerlaubt Zugang zu einem System von jemandem verschafft, nur zum Spaß.
d) Es ist eine Person, die für viele Finanzdelikte über das Internet verantwortlich ist.

Übung SINGLE CHOICE

Situation: Was bedeutet interner Betrug?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist wahr.

a) Interner Betrug wird von Lieferanten begangen, wenn sie die ausgehandelte Dienstleistung oder Ware nicht zum vereinbarten Zeitpunkt liefern.
b) Interner Betrug umfasst Aktivitäten wie Grooming oder Cyberbullying.
c) Interner Betrug wird von Angestellten begangen, wenn sie nicht autorisierte finanzielle Transaktionen durchführen.
d) Interner Betrug wird von Kunden des Unternehmens begangen, indem sie eine ungerechtfertigte Beschwerde einreichen.

Co-funded by the
Erasmus+ Programme
of the European Union

3.Auswirkungen der Cyberkriminalität

Computer können auch für Angriffe verwendet werden, um Verbrechen in der realen Welt (Verletzungen von Rechten des geistigen Eigentums, Kreditkartenbetrug, EFT-Betrug, Pornografie usw.) und sogar Terrorismus zu begehen. Terroristen nutzen oft Informationstechnologie, um ihre kriminellen Aktivitäten zu planen und auszuführen. Dies wird dann mit dem Begriff Cyberterrorismus bezeichnet. Die Zunahme der internationalen Interaktion und der weit verbreitete Einsatz von IT hat die Zunahme von Kriminalität und Terrorismus begünstigt. Aufgrund der fortgeschrittenen Kommunikationstechnologie müssen die Menschen nicht in einem Land sein, um ein solches Verbrechen zu organisieren. Daher können Terroristen und Kriminelle Sicherheitslücken im System finden und von ungewöhnlichen Orten aus operieren, anstatt von ihrem Wohnsitzland aus.

Die Mehrheit der künftigen internationalen Zwischenfälle, ob militärisch oder als Spionage, wird eine Cyberdimension haben. Daher ist es an der Zeit, über die Bewertung dieser Angriffe nachzudenken. Gegenwärtig gibt es Debatten über die Möglichkeit der Eskalation von Vorfällen zu einem nicht tragfähigen Kriegskonflikt, bei dem es zu Tod, Zerstörung, Personen- oder Sachschäden kommen kann. Das Problem besteht darin, dass es fast unmöglich ist, Handlungen einem bestimmten Staat zuzuordnen. Es ist schwierig, einen bestimmten Angreifenden ohne die präzise Zusammenarbeit des Staates zu erkennen, auf dessen Territorium sich der Angreifende befindet.

Die Auswirkungen der Cyberkriminalität

Die Auswirkungen der Cyberkriminalität können aufgrund des hohen Risikos von Datenverlust und finanziellen Auswirkungen verheerend sein.

Für Einzelpersonen

Datenverletzungen, Identitätsdiebstahl, Probleme mit Geräten: Cyberkriminalität kann große Auswirkungen auf den Einzelnen haben. Sie könnten es mit verdächtigen Belastungen Ihrer Kreditkarte infolge von Identitätsdiebstahl zu tun haben, mit einer Lösegeld-Attacke, bei der Hunderte oder Tausende erpresst werden, um Ihre Dateien freizugeben, oder mit teuren Gebühren für Daten oder

Strom aus Cryptojacking oder Botnets. Die Kosten können schlimmer als monetäre Kosten sein, wenn Sie von Cyberbullying, einschließlich sexueller Belästigung, geplagt werden.

Für Unternehmen und Regierungen
Sowohl Unternehmen als auch Organisationen des Gesundheitswesens und Regierungen können ebenfalls unter dem Verlust sensibler Daten, enormen finanziellen Belastungen und Markenschäden leiden. Der durchschnittliche Lösegeld-Angriff auf kleine und mittlere Unternehmen im Jahr 2019 verlangte 5.900 Dollar, um ihre Dateien oder Systeme freizugeben. Weitaus schlimmer ist, dass die Ausfallzeiten während dieser Angriffe die betroffenen Unternehmen durchschnittlich $141.000 kosteten. Ganz zu schweigen von den Lösegeld-Angriffen auf Regierungen, wie derjenige, der Jackson County, Georgia, dazu veranlasste, 400.000 Dollar für die Wiederherstellung ihrer IT-Systeme und Infrastruktur zu zahlen.

Ein anderer in diesem Zusammenhang verwendeter Begriff ist Cyberwar. Lassen Sie uns diese beiden Begriffe im Detail betrachten:

Was ist Cyberterrorismus?	**Was ist Cyberwar?**
Das Konzept der Cyberkriminalität wird oft mit Cyberterrorismus verwechselt. Cyberterrorismus ist immer gravierender als andere Verhaltensweisen, die im oder durch den Cyberspace ausgeführt werden. Die NATO definiert Cyberterrorismus als "Cyberangriff, bei dem Computer- oder Kommunikationsnetze genutzt oder ausgenutzt werden, um eine ausreichende Zerstörung oder Störung zu verursachen, um Angst zu erzeugen oder eine Gesellschaft zu einem ideologischen Ziel einzuschüchtern".	Beim Cyberwar geht es um den Einsatz und die Ausrichtung von Computern und Netzwerken im Krieg. Er umfasst offensive und defensive Operationen gegen die Bedrohung durch Cyberattacken, Spionage und Sabotage. Cyberwar wurde definiert als "Handlungen eines Nationalstaates, die darauf abzielen, in die Computer oder Netzwerke einer anderen Nation einzudringen, um Schaden oder Störungen zu verursache

Beispiel
Cyberware, einschließlich Netzwerkangriffe, hat seit dem 11. September zusätzlich an Bedeutung gewonnen. Diese Situation nach den Anschlägen vom 11. September brachte eine intensive Diskussion über die Nutzung von Informations- und Kommunikationstechnologien durch Terroristen mit sich. Diese Diskussion wurde durch Berichte erleichtert, dass die TäterInnen das Internet zur Vorbereitung des Anschlags nutzten. Obwohl es sich bei den Angriffen nicht um Cyber-Angriffe handelte, spielte das Internet bei der Vorbereitung des Angriffs eine Rolle. In diesem Zusammenhang wurden verschiedene Arten entdeckt, in denen terroristische Organisationen das Internet nutzen.

3.Wissen anwenden

Übung SINGLE CHOICE

Situation: Was ist der schlimmste Cyber-Angriff, um Verbrechen in der realen Welt zu begehen?
Die Aufgabe: Wählen Sie die richtigen Optionen nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist wahr.

- Kreditkartenbetrug

- Pornographie
- Cyber-Terrorismus
- Identitätsdiebstahl

Übung MULTIPLE CHOICE

Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus: Mehr Antworten könnten wahr sein.

Welche Auswirkungen kann die Cyberkriminalität für den Einzelnen haben?

- Identitätsdiebstahl
- Verlust des Arbeitsplatzes
- gesunde Probleme
- Datenverletzungen

Übung LÜCKENTEXT

Aufgabe: Aufgabe: Wählen Sie die richtige Option aus der untenstehenden Auswahl aus.

_____ können auch unter dem Verlust sensibler Daten, enormen finanziellen Belastungen und Markenschäden leiden.

Unternehmen, Angestellte, Hacker

4.Möglichkeiten der Prävention und des Schutzes

Alles, von gestohlenem Geld, Diebstahl persönlicher und finanzieller Daten, Produktivitätsverlust bis hin zur Beschädigung und Zerstörung kritischer Unternehmens- oder Individualdaten, wird als Cyberkriminalität eingestuft. Leider werden die Hacker und diejenigen, die Cyberkriminalität begehen, immer raffinierter.

Was sind die besten Möglichkeiten, Ihren Computer und Ihre persönlichen Daten zu schützen?

Der beste Weg, sich vor Cyberkriminalität zu schützen, ist Prävention. Für die Online-Sicherheit sind fünf Kernpunkte gut im Gedächtnis zu behalten: **Vorbeugung, Prävention, Schutz, Bewahrung und Ausdauer.**

Diese Punkte sind in den folgenden Schritten enthalten:

1. Vermeiden Sie die Offenlegung persönlicher Informationen im Internet und per E-Mail
2. Erwägen Sie sorgfältig, jedes Foto online zu schicken, - jeder kann es jederzeit in einem anderen Kontext verwenden
3. Verwenden Sie sichere Passwörter
4. Verwendung und Aktualisierung von Antiviren-Software
5. Vermeiden Sie es, Kreditkartennummern und Passwörter per E-Mail zu versenden.
6. Überwachen Sie die Websites, auf die Ihre Kinder zugreifen
7. Sichern Sie Ihre Daten, um den Verlust von Informationen aufgrund eines Virenangriffs zu verhindern.
8. Verwenden Sie ein Sicherheitsprogramm, das die Kontrolle über die Cookies
9. Software und Betriebssystem auf dem neuesten Stand halten
10. Öffnen Sie niemals Anhänge in Spam-E-Mails
11. Klicken Sie nicht auf Links in Spam-E-Mails oder auf nicht vertrauenswürdige Websites.
12. Direkte Kontaktaufnahme mit Unternehmen bei verdächtigen Anfragen
13. Behalten Sie Ihre Kontoauszüge im Auge
14. Achten Sie darauf, welche Websites Sie besuchen

Wie kann ich die sicheren Websites erkennen?

Die folgenden 3 Tipps zur Website-Sicherheit räumen die Unsicherheit aus dem Weg und zeigen Ihnen, wie Sie erkennen können, ob eine Website vertrauenswürdig ist oder nicht. Zuerst lernen Sie ein paar einfache visuelle Kontrollen, die Ihnen nützliche Informationen auf einen Blick liefern. Dann erklären wir Ihnen, welche Sicherheitswerkzeuge Sie für die Website haben sollten, um Sie zu informieren und anzuleiten. Schließlich sagen wir Ihnen, wie Sie etwas tiefer recherchieren können, falls noch Fragen offen bleiben. Lassen Sie uns jetzt schlau werden und wieder Spaß am Surfen im Internet haben.

1 - Visuelle Sicherheitsüberprüfungen der Website

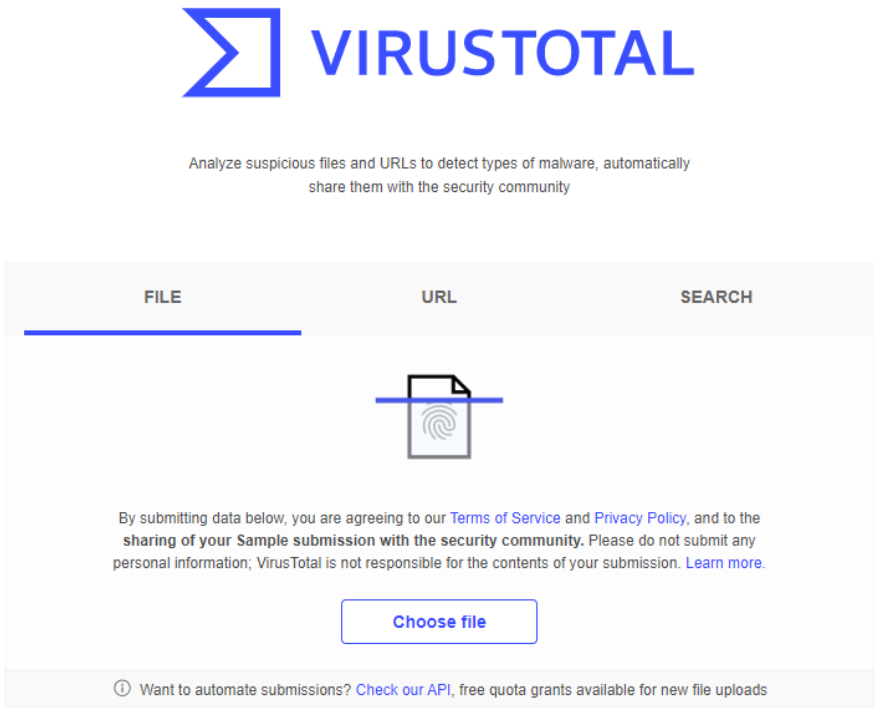
- Überprüfen Sie diese URLs doppelt - Beginnen wir mit dem einfachsten Tipp. Es ist wirklich nicht schwieriger, als sicherzustellen, dass die URL echt aussieht. Bevor Sie auf einen Link klicken, bewegen Sie den Mauszeiger über den Link und sehen Sie sich die linke untere Ecke Ihres Bildschirms an, wo die URL angezeigt wird. Der erste Trick beim Phishing besteht darin, so authentisch wie möglich auszusehen. Auf den ersten Blick mag die URL wie der echte McCoy aussehen, aber bei genauerem Hinsehen kann eine 1 anstelle eines l oder .net anstelle von .com erscheinen. Üben Sie sich darin, jede einzelne URL zu überprüfen, bevor Sie darauf klicken oder bevor Sie persönliche Daten wie Benutzername und Passwort eingeben.
- Prüfen Sie auf https - Die Buchstaben, die Sie am Anfang jeder URL sehen, stehen für Hypertext Transfer Protocol (http). Es ist die Grundlage dafür, wie Daten im Web kommuniziert werden. Und obwohl es äußerst nützlich ist, ist es auch leicht zu hacken. Der Zusatz eines "S" wie in "https" (und das Schloss-Symbol) zeigt jedoch an, dass die Site sicher ist. Websites mit einem Vorhängeschloss-Symbol in der Adressleiste und einem https-Präfix sind verschlüsselt und verfügen über ein vertrauenswürdiges SSL-Zertifikat, das im Grunde genommen eine sichere Verbindung zwischen Website und Browser garantiert. Wenn Sie nicht überprüfen können, ob eine Website oder ein Link mit https sicher ist, seien Sie auf der Hut und geben Sie keine persönlichen Daten ein.

Und beachten Sie bitte: Cyberkriminelle tun alles in ihrer Macht Stehende, um sich als legitim zu präsentieren. Während also https: Websites sicherer sind, könnten Sie einer Website auf der Spur sein, die von einem Gauner bzw. einer Gaunerin betrieben wird. Wenn Sie also einer https:-Website immer noch misstrauisch gegenüberstehen, überprüfen Sie mit den anderen unten aufgeführten Sicherheitstools, ob eine Website sicher ist.

2 - Website-Sicherheitswerkzeuge

- Verwenden Sie Ihre integrierten Browser-Werkzeuge - Die ersten Werkzeuge, mit denen Sie sich vertraut machen sollten, sind die Sicherheitsmaßnahmen, die bereits in Ihrem Browser vorhanden sind. Sehen Sie sich Ihre Datenschutz- und Sicherheitseinstellungen an. Wahrscheinlich werden Sie feststellen, dass die Standardeinstellungen lockerer sind, als Ihnen lieb ist. Passen Sie die Regeln und Einstellungen manuell so an, wie es für Sie bequem ist. Blockieren Sie Popups, verhindern Sie automatische Downloads, erlauben Sie keine Nachverfolgung. Ihre Optionen variieren je nach dem von Ihnen gewählten Browser.

- Führen Sie eine Sicherheitsüberprüfung der Online-Website durch - Es gibt mehrere, aus denen Sie wählen können, aber wir empfehlen VirusTotal wegen seiner unvoreingenommenen Position. Diese Online-Tools verwenden Antiviren-Scanner und andere Sicherheitslösungen, um eine Website auf mögliche Bedrohungen zu überprüfen. Geben Sie einfach die URL, die gescannt werden soll, in die Suchleiste der Website ein, und Sie erhalten sofort Ergebnisse. Geben Sie eine URL ein, und VirusTotal teilt Ihnen mit, ob die Website verdächtig ist.



- Installieren Sie Web-Sicherheitstools - Schützen Sie sich mit erstklassigen Cybersicherheits-Suites (z. B. Avast Free Antivirus, McAfee, AVG, Windows Defender), um die Sicherheit Ihrer Website zu gewährleisten. Wenn Sie ein virtuelles privates Netzwerk verwenden, können Sie die Sicherheit Ihrer Website auch um den Vorteil der Privatsphäre erweitern.

3 - Website-Sicherheit schnelle Recherche

- Prüfen Sie die Kontaktdaten für die Website - Wenn Sie alle oben genannten Punkte erledigt haben und sich immer noch nicht ganz sicher sind, dann marschieren Sie zur Haustür und klopfen Sie an. Das heißt, suchen Sie die "Kontakt"-Information auf der Website und rufen Sie sie an. Je nachdem, wie (und ob) sie antworten, werden Sie erfahren, ob es sich um eine legitime Operation handelt oder nicht.
- Prüfen Sie, ob Ihr Antivirenprogramm über ein Anti-Phishing-Zertifikat verfügt - nicht alle tun dies. Suchen Sie nach Labors von DrittanbieterInnen, die auf Anti-Phishing testen, z. B. AV-Comparatives. Sie testen Antivirus-Produkte gegen Phishing-URLs (die versuchen, an Ihre persönlichen Daten zu gelangen), und sie prüfen auf falsch-positive Ergebnisse, wenn es um legitime Bank-Websites geht, um sicherzustellen, dass das Sicherheitsprodukt den Unterschied kennt.
- Prüfen Sie, ob die URL über eine Datenschutzrichtlinie verfügt - dies ist ein Kinderspiel. Wenn eine Website keine Datenschutzrichtlinie hat, ist das eine rote Flagge dafür, ob die Firma legitim ist oder nicht.
- Suchen Sie mit WHOIS nach dem Domänenbesitzenden der Website - Sie können auch recherchieren, wer eine bestimmte Domäne besitzt, indem Sie die über eine WHOIS-Suche verfügbaren öffentlichen Aufzeichnungen überprüfen. Erfahren Sie alles über die Domäne, einschließlich wer sie wann registriert hat.

Eine geschäftliche Antwort auf Cyber-Kriminalität

Als Unternehmen ist Ihre beste Wette gegen Cyberkriminalität die Erstellung eines soliden Reaktionsplans auf Vorfälle. Oft reicht die Planung nicht aus - Sie sollten über das Sicherheitspersonal und die Werkzeuge verfügen, um ihn auszuführen. Ein Plan zur Reaktion auf einen Vorfall umfasst gemäß dem SANS-Rahmenwerk

- Vorbereitung - Sie modifizieren Ihre Sicherheitspolitik, identifizieren die Arten kritischer Sicherheitsvorfälle, erstellen einen Kommunikationsplan und dokumentieren Rollen, Verantwortlichkeiten und Prozesse für jeden einzelnen. Rekrutieren Sie Mitglieder für Ihr Computer Security Incident Response Team (CSIRT) und schulen Sie diese.
- Identifizierung - Verwenden Sie Sicherheitstools, um anomales Verhalten im Netzwerkverkehr, an Endpunkten, Anwendungen oder Benutzerkonten genau zu erkennen und schnell Beweise zu sammeln, um zu entscheiden, was mit dem Vorfall zu tun ist.
- Eindämmungs-Isola
- Die betroffenen Systeme, bereinigen sie und bringen sie nach und nach wieder ans Netz.
- Ausmerzung - Ermitteln Sie die Ursache des Vorfalls und unternehmen Sie alles, um sicherzustellen, dass sich das Problem nicht wiederholt. Beheben Sie defekte Sicherheitsmaßnahmen, die die Angreifenden hereinlassen, flicken Sie Schwachstellen und stellen Sie sicher, dass Sie Malware von allen Endpunkten bereinigen.
- Wiederherstellung - Stellen Sie die Produktionssysteme wieder her und sorgen Sie dafür, dass ein weiterer ähnlicher Angriff verhindert wird. Führen Sie Tests durch, um sicherzustellen, dass die Systeme gesichert sind und wie gewohnt funktionieren.
- Lektionen, die Sie bis zu zwei Wochen nach dem Vorfall gelernt haben, besprechen Sie sie mit dem Team, um zu verstehen, was gut gelaufen ist und was nicht, und verbessern Sie Ihren Plan zur Reaktion auf den Vorfall.

Die EU versucht, die Cyberkriminalität mit einem breiten Spektrum von Mitteln zu bekämpfen. Im Jahr 2005 verabschiedete der Rat die EU-Terrorismusbekämpfungsstrategie, um den Terrorismus zu bekämpfen und Europa sicherer zu machen. Die Strategie umfasst vier Säulen: Prävention, Schutz, Verfolgung und Reaktion.

Um Cyberkriminalität auf verschiedenen Ebenen zu bekämpfen und zu verfolgen, hat die EU die folgenden gesetzgeberischen Maßnahmen umgesetzt:

- 2001 - Rahmenbeschluss zur Bekämpfung von Betrug und Fälschung, der die betrügerischen Verhaltensweisen definiert, die die EU-Staaten als strafbare Straftaten betrachten müssen.
- 2002 - Datenschutzrichtlinie für elektronische Kommunikation (ePrivacy Directive), die Regelungen für die elektronische Kommunikation innerhalb der EU festlegt, um den Schutz der Privatsphäre von Einzelpersonen und Organisationen zu verbessern.
- 2011 - Eine Richtlinie zur Bekämpfung der sexuellen Ausbeutung von Kindern im Internet und der Kinderpornographie, die sich mit neuen Entwicklungen im Online-Umfeld befasst, wie z.B. Grooming (Täter, die sich als Kinder ausgeben, um Minderjährige für sexuellen Missbrauch zu ködern)
- 2013 - Eine Richtlinie über Angriffe auf Informationssysteme, mit der groß angelegte Cyber-Angriffe bekämpft werden sollen, um die nationalen Gesetze zur Cyber-Kriminalität zu stärken und härtere strafrechtliche Sanktionen einzuführen

International tätige Organisationen versuchen, einen Beitrag zur Bekämpfung der Cyberkriminalität zu leisten. Es gibt zwei große Organisationen, die in der EU tätig sind:

Europäisches Zentrum für Cyberkriminalität - EC3 unterstützt die Mitgliedsstaaten bei ihren Bemühungen, Cyberkriminalitätsnetze zu zerschlagen und zu stören, sowie bei der Entwicklung von Werkzeugen und der Bereitstellung von Schulungen.

Die Agentur der Europäischen Union für Computer- und Netzsicherheit (ENISA) arbeitet daran, Beratung und Lösungen anzubieten und die Fähigkeiten im Bereich der Computer- und Netzsicherheit zu verbessern. Ein Kompetenzzentrum für Mitgliedstaaten und EU-Institutionen, die Rat in Fragen der Netz- und Informationssicherheit suchen.

4.Wissen anwenden

Übung SINGLE CHOICE

Aufgabe: Wählen Sie die richtigen Optionen nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist wahr.

Was ist ein Anti-Phishing-Zertifikat?

- Prüfen Sie auf falsch-positive Ergebnisse, wenn es sich um legitime Bank-Websites handelt, um sicherzustellen, dass das Sicherheitsprodukt den Unterschied kennt
- prüfen, ob eine Website keine Datenschutzrichtlinie hat
- zu überprüfen, ob eine Website oder ein Link mit https sicher ist
- den tatsächlichen Eigentümer der Website überprüfen

Übung WAHR/FALSCH

Aufgabe: Wählen Sie die richtigen Optionen nach dem Wahr/Falsch-Prinzip aus: Nur eine Antwort ist richtig.

Das Hinzufügen eines "S" wie in "https" (und des Schloss-Symbols) ist eine sicherere Website.

- Wahr
- Falsch

Übung SINGLE CHOICE

Aufgabe: Wählen Sie die richtigen Optionen nach dem Single-Choice-Prinzip aus: Eine Antwort ist richtig.

Was ist VirusTotal?

- Antivirenprogramm mit Installation auf Ihrem Computer
- Web-Browser
- Werkzeug zur Online-Prüfung der Web-Sicherheit
- Hypertext-Übertragungsprotokoll

5. Die Auswirkungen der Cyberkriminalität auf das Leben

Das Internet kann **für Kinder und auch für Erwachsene eine gefährliche Umgebung sein**. Besonders in dieser digitalen Zeit, in der soziale Medien wie Facebook, Instagram oder das Internet im Allgemeinen eine untrennbare Rolle spielen. Gerade der Schutz von Kindern im Internet erfordert ein hohes Risikobewusstsein und fortgeschrittene IT-Kenntnisse - als Eltern müssen Sie wissen, welche Gefahren lauern und wie Sie sich davor schützen können.

Hier sind die sechs größten Risiken, denen Kinder online ausgesetzt sind:

- Cybermobbing
- Versehentliches Herunterladen von Malware
- Pflege
- Phishing
- Veröffentlichen privater Informationen
- Chat-Raum "Freunde

Doch nicht nur Kinder sind mit virtuellen Bedrohungen konfrontiert. Die Landschaft der Cyberkriminalität ist riesig, und es gibt eine Vielzahl von Möglichkeiten, auf denen Cyberkriminelle direkt zu Ihnen aufschließen können. Cyberkriminelle greifen menschliche Unwissenheit und Bequemlichkeit an, was zu einem Verlust von Identität und Finanzen führen kann. Worüber sollten sich die Menschen im Klaren sein? Kriminelle entwerfen ihre Fallen bewusst, indem sie menschliche Schwächen oder menschliches Verhalten ausnutzen, wie z.B:

- die Bereitschaft des Einzelnen, anderen zu vertrauen
- vorgeschlagene Dringlichkeit oder Wichtigkeit einer Botschaft
- Zeichen der Legitimität oder Autorität in einer Botschaft oder einem Individuum (Branding identisch mit dem offiziellen Branding eines Individuums oder einer Organisation, um Vertrauen zu kultivieren)
- Angst vor Situationen, die hohen Stress bedeuten oder in denen der Einzelne sehr ängstlich sein kann
- Bequemlichkeit (die leichtere Entscheidung ist möglicherweise nicht die sicherste)
- die Neigung von Einzelpersonen, persönliche Identitätsangaben online (insbesondere über Formen sozialer Medien, einschließlich Facebook, Twitter, LinkedIn) übermäßig zu verbreiten
- Geringe Vertrautheit mit neuen Formen der Technologie, die den Einzelnen für Risiken öffnen
- Unterschätzung der Situation durch den Einzelnen

Wenn eine Person das oben gezeigte Verhalten beibehält, ist sie einem höheren Risiko ausgesetzt, Opfer eines Cyberdiebstahls zu werden. Cyberdiebstahl ist eine Art von Verbrechen, wenn finanzielle oder persönliche Informationen durch die Benutzung von Computern gestohlen werden. Cyber-Diebe sind raffiniert und können Daten aus Sicherheitsmaßnahmen verletzen.
In der ersten Phase muss sich der Täter bzw. die Täterin zunächst eine fremde Computer-Identität aneignen. Dies geschieht meist durch Diebstahl elektronischer Daten (Passwörter, Zugangsdaten usw.), meist durch unbefugtes Kopieren (Skimming), betrügerisches Phishing oder Hacking. Dies wird als Identitätsdiebstahl bezeichnet. In der zweiten Phase missbraucht der Täter bzw. die Täterin die Identität. Das Ziel ist in der Regel ein Eigentumsvorteil. In einigen Fällen kann das Ziel einfach darin bestehen, dem Opfer zu schaden, z.B. indem er unter seinem Namen in sozialen Netzwerken wie Facebook handelt.

Die Verteidigung ist nicht kompliziert - es ist wichtig, ein paar einfache Regeln zu befolgen:

1. das Konto überwachen
2. auf sicheren Websites kaufen - wenn vor dem "https" ein grünes Vorhängeschloss-Symbol steht, wissen Sie sofort, dass Sie sich auf einer sicheren Website befinden
3. seien Sie vorsichtig beim Öffnen vertrauensunwürdiger E-Mails

Cyber-Diebstahl liegt vor, wenn Ihre finanziellen oder persönlichen Daten durch den Einsatz von Computern gestohlen werden. Cyber-Diebe können Banken, Unternehmen und Einzelpersonen ins Visier nehmen.
In der ersten Phase muss sich der Täter bzw. die Täterin zunächst eine fremde Computer-Identität aneignen. Dies geschieht meist durch Diebstahl elektronischer Daten (Passwörter, Zugangsdaten

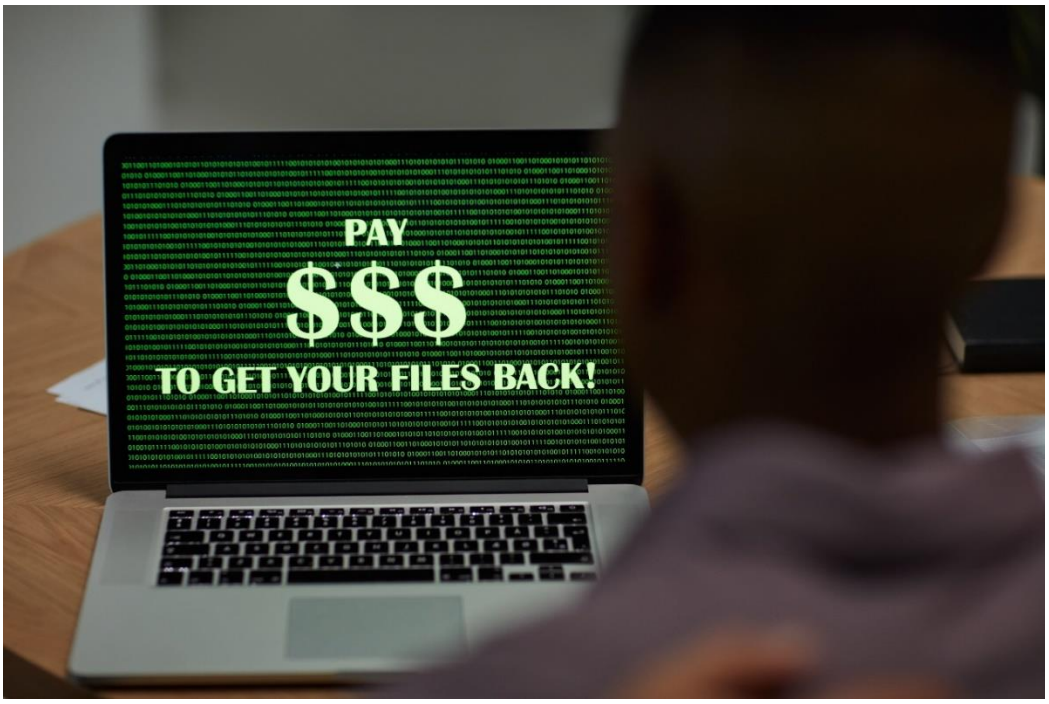
usw.), meist durch unbefugtes Kopieren (Skimming), betrügerisches Phishing oder Hacking. Dies wird als Identitätsdiebstahl bezeichnet.

In der zweiten Phase missbraucht der Täter bzw. die Täterin die Identität. Das Ziel ist in der Regel ein Eigentumsvorteil. In einigen Fällen kann das Ziel einfach darin bestehen, dem Opfer zu schaden, z.B. indem er unter seinem Namen in sozialen Netzwerken wie Facebook handelt.

Auswirkungen auf Individuen, Unternehmen und Gesellschaft

Cyberkriminalität hat einen direkten und bedeutenden **Einfluss auf Arbeitsplätze, Innovation, Wirtschaftswachstum und Investitionen**. Darüber hinaus macht der Diebstahl von geistigem Eigentum mindestens 25% der Kosten der Cyberkriminalität aus und stellt eine besonders hohe Bedrohung für die Militärtechnologie dar. Zwei Bereiche der Cyberkriminalität, die schwer zu messen sind, sind der Diebstahl von IP (IP-Adressen) und der Verlust von Chancen.

Einzelpersonen und Unternehmen können aufgrund von Cyberkriminalität erhebliche **finanzielle Verluste** erleiden, wobei die offensichtlichste Auswirkung der Diebstahl ist. Geschäftsverluste können auch im Falle eines Denial-of-Service-Angriffs für große Unternehmen erheblich sein.



Es mag das Leben leichter machen, aber es macht uns auch anfällig für Risiken**. Aus diesem Grund hat die Cybersicherheit höchste Priorität und beeinflusst unser Alltags-/Arbeitsleben stark**. Verstöße gegen die Cybersicherheit können für Organisationen und ihre MitarbeiterInnen oder KundInnen katastrophale Folgen haben.

Schäden durch Cyberattacken und Cyberdiebstahl können vom ursprünglichen Ziel auf wirtschaftlich verbundene Unternehmen übergreifen und dadurch den Schaden für die Wirtschaft vergrößern. Die Unternehmen haben gemeinsame Cyber-Schwachstellen, so dass Cyber-Bedrohungen firmenübergreifend korreliert sind.

Kriminalität betrifft jeden und in Zukunft wird die Cyberkriminalität (und die Cybersicherheit) immer mehr Menschen betreffen. Niemand ist sicher - sie betrifft die Reichen und die Armen:

- Jeder, der ein Mobiltelefon in der Tasche hat.

- Jeder, der ein Bankkonto hat.
- Jeder, der wichtige Dateien auf seinem Computer speichert.
- Jeder, dessen Name in einer Direktmarketing-Datenbank steht.

Cyberkriminalität ist keine futuristische Möglichkeit. Sie wird derzeit jeden Tag begangen. Diebe begehen Cyberkriminalität, um das Geld der Menschen und ihre Identität zu stehlen. Mit Ihrer Identität kann der Dieb Kredite aufnehmen, Kredite aufnehmen, Schulden anhäufen und dann spurlos fliehen. Es kann Jahre dauern, bis Ihre Identität wiederhergestellt ist. Ein Virus kann die Dateien von jemandem zerstören, und eine verlorene Datenbank kann dazu führen, dass er unerwünschte Verkaufsgespräche erhält.

Cybersicherheit ist wichtig für die nationale Sicherheit - zur Sicherung unseres schönen Landes.

- Es gibt einige Staatsgeheimnisse, die geheim bleiben müssen.
- Die persönliche Sicherheit unserer Führungskräfte ist sehr wichtig.
- Die Fingerabdruck-Datenbank und die Datenbank für innere Angelegenheiten müssen sicher sein.
- Terroristen dürfen nicht in der Lage sein, den Handel mit sensiblen Daten in der wichtigen nationalen und weltweiten Datenbank zu unterbinden.

Aber **die nationale Sicherheit kann unsere persönliche Freiheit**, für die wir so hart gekämpft haben, **nicht außer Kraft setzen**:

- Unsere Redefreiheit ist entscheidend.
- Eine freie Presse hält die Menschen zur Rechenschaft.
- Die persönliche Privatsphäre sichert die Demokratie.
- Die Freiheit, Dinge online ohne Überwachung zu tun.

5.Wissen anwenden

Übung SINGLE CHOICE

Aufgabe: Wählen Sie die richtigen Optionen nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist wahr.

Wer kann von Cyberkriminalität betroffen sein?

- Jeder, der mit Mobil-, Online- oder Bankkonten zu tun hat.
- Nur Kinder.
- nur Unternehmen
- nur öffentliche Einrichtungen.

Übung SINGLE CHOICE

Aufgabe: Wählen Sie die richtigen Optionen nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist wahr.

Was ist Cyber-Diebstahl?

- Besessenheit davon, so viel wie möglich über die Person herauszufinden
- Computer- oder Kommunikationsnetze zu benutzen oder auszunutzen, um eine ausreichende Zerstörung oder Störung zu verursachen, um Angst zu erzeugen oder eine Gesellschaft zu einem ideologischen Goa einzuschüchtern.
- verletzende Dinge zu der Person zu sagen oder anderen unwahren Informationen über die Person zu erzählen

- wenn Ihre finanziellen oder persönlichen Daten durch die Verwendung von Computern gestohlen werden

Übung WAHR/FALSCH

Aufgabe: Wählen Sie die richtigen Optionen nach dem Wahr/Falsch-Prinzip aus: Nur eine Antwort ist richtig.

Cybersicherheit ist für die nationale Sicherheit nicht wichtig.

- Wahr
- Falsch

Co-funded by the
Erasmus+ Programme
of the European Union

Quellen

Source: http://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf
Source: https://study.com/academy/lesson/finance-crime-definition-comparisons-examples.html
Source: https://www.avast.com/c-cybercrime
Source: NATO science for peace and security series, 2008
Source: CLARKE, Richard A. Cyber War, HarperCollins (2010) ISBN 9780061962233
Source: CNN, News, 04.08.2004, available at: www.cnn.com/2004/US/08/03/terror.threat/index.html. For an overview, see: Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; Gercke, Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007
Source: EU counter-terrorism strategy
Source: https://www.avast.com/c-website-safety-check-guide
Source: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
Source: https://www.enisa.europa.eu/
Source: https://arxiv.org/pdf/1811.06624.pdf

Co-funded by the
Erasmus+ Programme
of the European Union

Wissen sichern

Zusammenfassung

Der Einsatz von Computertechnologie, Informationssystemen und Informationstechnologie und deren Integration in fast alle Bereiche menschlicher Tätigkeit ist ein Phänomen der heutigen Zeit. Es gibt fast keinen Bereich menschlicher Tätigkeit, in dem die Informations- oder Kommunikationstechnologie nicht eingesetzt wird.

Leider nimmt mit dem technischen Fortschritt die Möglichkeit der Kriminalität zu. Verbrechen können auf viele Arten begangen werden, zu den häufigsten gehören die Cyberkriminalität:

- **Malware** - allgemeine Bezeichnung für bösartige Software, die sich zwischen Computern ausbreitet und den Computerbetrieb stört
- **Hacking** - gemeinsamer Prozess, der zur Verletzung der eigenen Privatsphäre und vertraulicher Informationen führt
- **Spam** - Unerwünschte oder Junk-E-Mails, die in der Regel in großen Mengen an unzählige EmpfängerInnen in der ganzen Welt verschickt werden
- **Phishing** - Spam-E-Mails oder andere Formen der Kommunikation werden massenhaft verschickt, mit der Absicht, die EmpfängerInnen zu etwas zu verleiten, das ihre Sicherheit oder die Sicherheit der Organisation, für die sie arbeiten, untergräbt.
- **Verteilte DoS-Angriffe (Distributed DoS Attacks, DDoS)** - Angriff überwältigt ein System, indem eines der Standardkommunikationsprotokolle verwendet wird, um das System mit Verbindungsanfragen zu spammen

Hacking wird jedoch nicht immer als Diebstahl wahrgenommen und für produktive Zwecke eingesetzt. Diese Art von Hacking, bei der gute Absichten im Spiel sind, wird als **ethisches Hacking** bezeichnet. Diese Art von Hacking wird zur Sicherung des Betriebssystems durchgeführt.

Zu den am häufigsten begangenen Cyberkriminalität gehören:

- **Online-Imitation** - Verwendung des Namens, der Domänenadresse, der Telefonnummer oder anderer Identifizierungsinformationen einer anderen Person ohne deren Zustimmung
- **Cyberstalking** - Besessenheit davon, so viel wie möglich über die Person herauszufinden
- Cybermobbing - verletzende Dinge zu einer Person zu sagen oder anderen unwahren Informationen über die Person zu erzählen
- **Identitätsdiebstahl** - Diebstahl persönlicher Identifikationsdaten zur Begehung illegaler Handlungen
- **Datendiebstahl** - illegaler Besitz von sensiblen Daten, darunter unverschlüsselte Kreditkarteninformationen, die in Unternehmen gespeichert sind
- **Finanzkriminalität** - darunter Betrug, Geldwäsche, Bestechung, Bestechlichkeit

Die Auswirkungen der Cyberkriminalität können aufgrund der Rufschädigung, des hohen Risikos von Datenverlusten und der finanziellen Auswirkungen für die Betroffenen verheerend sein:

- Kinder
- Erwachsene
- Unternehmen
- Staaten/Regierungen

Die Cyberkriminalität kann nicht nur finanzielle, sondern auch unredliche Auswirkungen auf Einzelpersonen oder Unternehmen haben. Sowohl Unternehmen als auch Organisationen des

Gesundheitswesens und Regierungen können ebenfalls unter dem Verlust sensibler Daten, enormen finanziellen Belastungen und Markenschäden leiden.
Die riesigen geplanten Aktionen der Cyberkriminalität sollten als **Cyberterrorismus** oder sogar als Cyberwar bezeichnet werden. Cyberterrorismus ist immer schwerwiegender als andere Verhaltensweisen, die im oder durch den Cyberspace ausgeführt werden. Cyberangriff, bei dem Computer- oder Kommunikationsnetzwerke genutzt oder ausgenutzt werden, um genügend Zerstörung oder Störungen zu verursachen, um Angst zu erzeugen oder eine Gesellschaft zu einem ideologischen Ziel einzuschüchtern.
Cyberwar beinhaltet den Einsatz und die gezielte Ausrichtung von Computern und Netzwerken im Krieg. Er umfasst offensive und defensive Operationen gegen die Bedrohung durch Cyberattacken, Spionage und Sabotage.

Ein wichtiges Instrument im Kampf gegen Cyberkriminalität ist die Prävention und Aufklärung. Schließlich sind Computerkenntnisse als wesentliches Element zur Verhinderung der Nutzung von Informations- und Kommunikationstechnologien wichtig. Wir sollten nicht nur Kinder, sondern auch Erwachsene und Unternehmen auf die Gefahren des Cyberspace vorbereiten und versuchen, ihnen das nötige Wissen zur sicheren Nutzung der Informationstechnologien zu vermitteln.

Für die Online-Sicherheit sind fünf Schlüsselpunkte gut im Gedächtnis zu behalten: **Vorsorge, Vorbeugung, Schutz, Bewahrung und Ausdauer.**

Diese Punkte sind in den folgenden Schritten enthalten:

1. Vermeiden Sie die Offenlegung persönlicher Informationen im Internet und per E-Mail
2. Erwägen Sie sorgfältig, jedes Foto online zu schicken, - jeder kann es jederzeit in einem anderen Kontext verwenden
3. Verwenden Sie sichere Passwörter
4. Verwendung und Aktualisierung von Antiviren-Software
5. Vermeiden Sie es, Kreditkartennummern und Passwörter per E-Mail zu versenden.
6. Überwachen Sie die Websites, auf die Ihre Kinder zugreifen, und nutzen Sie die Tools zur elterlichen Kontrolle
7. Sichern Sie Ihre Daten, um den Verlust von Informationen aufgrund eines Virenangriffs zu verhindern.
8. Verwenden Sie ein Sicherheitsprogramm, das die Kontrolle über die Cookies
9. Software und Betriebssystem auf dem neuesten Stand halten
10. Öffnen Sie niemals Anhänge in Spam-E-Mails
11. Klicken Sie nicht auf Links in Spam-E-Mails oder auf nicht vertrauenswürdige Websites.
12. Direkte Kontaktaufnahme mit Unternehmen bei verdächtigen Anfragen
13. Behalten Sie Ihre Kontoauszüge im Auge
14. Achten Sie darauf, welche Websites Sie besuchen

<u>Wie kann ich die sicheren Websites erkennen?</u>
1 - Visuelle Kontrollen der Website-Sicherheit
2 - Website-Sicherheitswerkzeuge
3 - Website-Sicherheit schnelle Recherche

Im Internet wimmelt es von Phishing-Betrügereien. Keine Marke ist vor Fälschungen sicher, und kein Benutzer bzw. keine Benutzerin ist vor der Zielscheibe sicher. Mehr als je zuvor müssen wir die Verantwortung für unsere eigene Online-Sicherheit übernehmen. Befolgen Sie die obigen Tipps und bleiben Sie clever. Sie haben alle Informationen erhalten, die Sie benötigen, aber **Ihr größter Verteidiger sind Sie**.

Co-funded by the
Erasmus+ Programme
of the European Union

Lösungsschlüssel
(die korrekten Antworten sind fett markiert)

1.Wissen anwenden

Situation: Wenn die Musik oder der Film im Internet veröffentlicht ist, kann ich sie legal herunterladen.
Aufgabe: Wählen Sie die richtigen Optionen nach dem Wahr/Falsch-Prinzip aus:

- wahr
- **falsch**

Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus: Mehr Antworten könnten wahr sein.
Markieren Sie die richtigen Kategorien von Cyberkriminalität

- **Computerbezogene Straftaten**
- Physischer Diebstahl eines Computers, Tablets oder Telefons
- **Inhaltsbezogene Straftaten**
- **Urheberrechtsbezogene Verstöße**

Aufgabe: Wählen Sie die richtigen Optionen aus der untenstehenden Auswahl aus.

_____ deckt viele Straftaten ab, für deren Begehung ein Computersystem erforderlich ist. Im Gegensatz zu früheren Kategorien sind diese allgemeinen Straftatbestände oft nicht so streng, was den Schutz der Rechtsgrundsätze betrifft.
_____ umfasst Verstöße gegen Rechtsinstrumente, die stärker von nationalen Ansätzen beeinflusst sind, die grundlegende kulturelle und rechtliche Prinzipien berücksichtigen können. Die Werte- und Rechtssysteme unterscheiden sich zwischen den Gesellschaften erheblich.
_____ umfasst den Austausch urheberrechtlich geschützter Lieder, Dateien und Software in Filesharing-Systemen oder durch Share-Hosting-Dienste und die Umgehung von DRM-Systemen (Digital Rights Management)

Computerbezogene Straftaten, Inhaltsbezogene Straftaten, Urheberrechtsbezogene Straftaten

2.Wissen anwenden

Situation: Was sind verteilte DoS-Angriffe (DDoS)?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist wahr.

- wenn Spam-E-Mails oder andere Kommunikationsformen massenhaft verschickt werden
- **eine Art von Cyberkriminalität, die von Cyberkriminellen benutzt wird, um ein System oder Netzwerk zum Einsturz zu bringen**
- Unerwünschte oder Junk-E-Mails, die typischerweise in Massen an unzählige EmpfängerInnen in der ganzen Welt verschickt werden
- die unbefugte Benutzung von oder der unbefugte Zugang zu Computern oder Netzwerkressourcen, die identifizierte Sicherheitslücken in Netzwerken ausnutzen

Situation: Welche Aktivitäten kennzeichnet folgende Person: "Hacker mit grauem Hut"?

Aufgabe: Wählen Sie die richtige Option nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist wahr.

- Es ist eine Person, die unwahre Informationen über eine andere Person verbreitet.
- Es ist eine Person, die versucht, persönliche Identifikationsinformationen zu stehlen.
- **Es ist eine Person, die sich unerlaubt Zugang zu einem System von jemandem verschafft, nur zum Spaß.**
- Es ist eine Person, die für viele Finanzdelikte über das Internet verantwortlich ist.

Situation: Was bedeutet interner Betrug?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist wahr.

- Interner Betrug wird von Lieferanten begangen, wenn sie die ausgehandelte Dienstleistung oder Ware nicht zum vereinbarten Zeitpunkt liefern.
- Interner Betrug umfasst Aktivitäten wie Grooming oder Cyberbullying.
- **Interner Betrug wird von Angestellten begangen, wenn sie nicht autorisierte finanzielle Transaktionen durchführen.**
- Interner Betrug wird von Kunden des Unternehmens begangen, indem sie eine ungerechtfertigte Beschwerde einreichen.

3.Wissen anwenden

Situation: Was ist der schlimmste Cyber-Angriff, um Verbrechen in der realen Welt zu begehen?
Die Aufgabe: Wählen Sie die richtigen Optionen nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist wahr.

- Kreditkartenbetrug
- Pornographie
- **Cyber-Terrorismus**
- Identitätsdiebstahl

Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus: Mehr Antworten könnten wahr sein.
Welche Auswirkungen kann die Cyberkriminalität für den Einzelnen haben?

- **Identitätsdiebstahl**
- Verlust des Arbeitsplatzes
- gesunde Probleme
- **Datenverletzungen**

Aufgabe: Wählen Sie die richtigen Optionen aus der untenstehenden Auswahl aus.

_____ können auch unter dem Verlust sensibler Daten, enormen finanziellen Belastungen und Markenschäden leiden.

Unternehmen, Angestellte, Hacker

4.Wissen anwenden

Aufgabe: Wählen Sie die richtigen Optionen nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist wahr.
Was ist ein Anti-Phishing-Zertifikat?

- **Prüfen Sie auf falsch-positive Ergebnisse, wenn es sich um legitime Bank-Websites handelt, um sicherzustellen, dass das Sicherheitsprodukt den Unterschied kennt**
- prüfen, ob eine Website keine Datenschutzrichtlinie hat
- zu überprüfen, ob eine Website oder ein Link mit https sicher ist
- den tatsächlichen Eigentümer der Website überprüfen

Aufgabe: Wählen Sie die richtigen Optionen nach dem Wahr/Falsch-Prinzip aus: Nur eine Antwort ist richtig.
Das Hinzufügen eines "S" wie in "https" (und des Schloss-Symbols) ist eine sicherere Website.

- **Wahr**
- Falsch

Aufgabe: Wählen Sie die richtigen Optionen nach dem Single-Choice-Prinzip aus: Eine Antwort ist richtig.
Was ist VirusTotal?

- Antivirenprogramm mit Installation auf Ihrem Computer
- Web-Browser
- **Werkzeug zur Online-Prüfung der Web-Sicherheit**
- Hypertext-Übertragungsprotokoll

5.Wissen anwenden

Aufgabe: Wählen Sie die richtigen Optionen nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist wahr.
Wer kann von Cyberkriminalität betroffen sein?

- **Jeder, der mit Mobil-, Online- oder Bankkonten zu tun hat.**
- Nur Kinder.
- nur Unternehmen
- nur öffentliche Einrichtungen.

Aufgabe: Wählen Sie die richtigen Optionen nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist wahr.
Was ist Cyber-Diebstahl?

a. Besessenheit davon, so viel wie möglich über die Person herauszufinden
b. Computer- oder Kommunikationsnetze zu benutzen oder auszunutzen, um eine ausreichende Zerstörung oder Störung zu verursachen, um Angst zu erzeugen oder eine Gesellschaft zu einem ideologischen Goa einzuschüchtern.
c. verletzende Dinge zu der Person zu sagen oder anderen unwahren Informationen über die Person zu erzählen
d. wenn Ihre finanziellen oder persönlichen Daten durch die Verwendung von Computern gestohlen werden

Aufgabe: Wählen Sie die richtigen Optionen nach dem Wahr/Falsch-Prinzip aus: Nur eine Antwort ist richtig.
Cybersicherheit ist für die nationale Sicherheit nicht wichtig.

- Wahr
- **Falsch**