Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Schweizer Armee

Modul 1: Fühle ich mich sicher?

«Sicherheit gibt es mit Sicherheit nicht.»

Erwin Koch (*1932), deutscher Aphoristiker

h
e
p

Lernziele

→ Sie können den Begriff «Sicherheit» definieren.
→ Sie können Arten von Bedrohungen und Gefahren erläutern.
→ Sie können die Sicherheitspolitik der Schweiz an konkreten Beispielen erklären.
→ Sie können Cyber-Szenarien beschreiben und Tipps geben, wie man Gefahren begegnen kann.

Inhaltsverzeichnis

Titelbilder:

Bild links
Militärpolizistin sichert das Gelände.

Bild Mitte
Angehörige der Armee helfen Anwohnern des Berner Mattequartiers bei der Evakuierung (Hochwasser 2005).

Bild rechts
Helikopter EC 635 der Schweizer Luftwaffe übt den Rettungseinsatz mit Seilwinde (Markierung SAR: Search and Rescue).

Modul 1:
Fühle ich mich sicher?

Was bedeutet für Sie Sicherheit? In welchen Bereichen fühlen Sie sich sicher und in welchen bedroht? Was brauchen Sie, um sich sicher zu fühlen? In diesem Modul werden Sie sich mit dem Thema Sicherheit befassen, Cyber-Risiken im eigenen Umfeld erkennen und diese mit verschiedenen Massnahmen selbstständig reduzieren können.

HAUSAUFGABE:
Sicherheit
Bringen Sie einen Gegenstand oder ein Bild mit in den Unterricht, der bzw. das für Sie Sicherheit im Alltag, zu Hause usw. bedeutet.

Digitale Alternative
Erstellen Sie ein Bild mit einer Wortwolke, die Sie mit Begriffen und Assoziationen zum Thema Sicherheit füllen. → www.wordle.net

AUFGABE 1:
Mein Gegenstand/Mein Bild
Erklären Sie in Gruppen, weshalb Ihr Gegenstand bzw. Ihr Bild für Sie Sicherheit bedeutet.

AUFGABE 2:
Fragen zum Thema Sicherheit
Beantworten Sie die folgenden drei Fragen zum Thema Sicherheit. Vergleichen Sie anschliessend Ihre Antworten mit einer Klassenkollegin oder einem Klassenkollegen.

1. Welchen Gefahren/Bedrohungen könnten Sie im Alltag ausgesetzt sein? Nennen Sie vier Beispiele.

   _____

   _____

   _____

   _____

2. Erstellen Sie mit den oben genannten Antworten eine Rangliste: 1. sehr stark usw.

   1. _____
   2. _____
   3. _____
   4. _____

3. Was brauchen Sie, um sich sicher zu fühlen? Begründen Sie Ihre Antwort in 1 – 2 Sätzen.

Ein Verkehrssoldat regelt den Verkehr am Tour-de-Suisse-Radrennen, damit auch junge Fans sicher zuschauen können.

AUFGABE 3:

Umfrage

Führen Sie nun eine Umfrage zum Thema «Was bedeutet für Sie Sicherheit?» durch. Stellen Sie unterschiedlichen (Alter, Geschlecht usw.) Leuten mindestens vier Fragen und werten Sie die Resultate in einer Grafik und einem kurzen Kommentar aus. Stellen Sie unterschiedlichen Leuten mindestens vier Fragen und werten Sie die Resultate in einer Grafik und einem kurzen Kommentar aus. Wählen Sie die Gesprächspartner spezifisch nach verschiedenen Kriterien wie zum Beispiel Alter, Geschlecht oder Beruf aus.

Digitale Alternative

Sie können Ihre Umfrage auch mit dem folgenden Online-Tool durchführen:
→ www.findmind.ch

AUFGABE 4:

Drei Videoclips zum Thema «Bedrohungen und Gefahren»

Schauen Sie sich die drei Videos an:

1.		www.youtube.com/watch?v=3r8Hq6Nvy-o
2.		www.youtube.com/watch?v=UcH6hUdFWUQ
3.		www.srf.ch/news/schweiz/falsche-bombendrohung-loest-ein-satz-der-luftpolizei-aus

AUFGABE 5:

Arten von Bedrohungen und Gefahren

Beschreiben Sie und schätzen Sie ab,

a) um welche Art von Bedrohungen und Gefahren es sich handelt,
b) wie hoch die Wahrscheinlichkeit ist, dass das Risiko eintritt und
c) wie gross die existenziellen Auswirkungen auf die Schweiz dabei sind.

1. Videoclip:
   Art

   Gefahren

   Auswirkung

2. Videoclip:
   Art

   Gefahren

   Auswirkung

3. Videoclip:
   Art

   Gefahren

   Auswirkung

Bedrohungen und Gefahren

Direkt	Indirekt
→ Terrorismus → Natur- und zivilisationsbedingte Katastrophen und Notlagen → Cyber-Angriffe → Verbotener Nachrichtendienst → Gewalttätiger Extremismus → Organisiertes Verbrechen → Gewalt gegen Leib und Leben	→ Weiterverbreitung von Massenvernichtungswaffen → Zerfall staatlicher Strukturen → Migrationsprobleme → Klimawandel → Pandemien

Unterschied: Eine *Bedrohung* setzt einen Willen voraus, die Schweiz oder ihre Interessen zu schädigen oder zumindest eine solche Schädigung in Kauf zu nehmen. Eine *Gefahr* setzt keinen Willen zur Schädigung voraus (z. B. Naturgefahren und technische Gefahren).
(Quelle: Sicherheitspolitischer Bericht 2016)

www.vbs.admin.ch/de/themen/sicherheitspolitik/sicherheitspolitische-berichte/sicherheitspolitischer-bericht-2016.detail.document.html/vbs-internet/de/documents/sicherheitspolitik/sipolb2016/SIPOL-B-2016-de.pdf.html

AUFGABE 6:

Sicherheitspolitik der Schweiz

Sicherheit ist nicht selbstverständlich. Sie muss erarbeitet und gepflegt werden. Seit vielen Jahren geniesst die Schweiz Frieden, Sicherheit und Freiheit: von der Bewegungsfreiheit aller Bürgerinnen und Bürger über die Meinungsäusserungsfreiheit bis zur Wirtschaftsfreiheit. Die Schweiz ist eines der am stärksten vernetzten Länder und entsprechend verletzlich gegenüber Angriffen. Mithilfe der nötigen Mittel und Instrumente ist sie auch in Zukunft bereit, den aktuellen Bedrohungen und Gefahren entgegentreten zu können.
Diese Sicherheit in unserem Land auf lange Sicht zu wahren, ist die Aufgabe der Sicherheitspolitik.

Lesen Sie den folgenden Informationsblock durch und markieren Sie mit einer Farbe wichtige Textstellen.

Sicherheitspolitik
Sicherheitspolitik umfasst die Gesamtheit aller Massnahmen von Bund, Kantonen und Gemeinden zur Vorbeugung, Abwehr und Bewältigung machtpolitisch oder kriminell motivierter Drohungen und Handlungen, die darauf ausgerichtet sind, die Schweiz und ihre Bevölkerung in ihrer Selbstbestimmung einzuschränken oder ihnen Schaden zuzufügen. Dazu kommt die Bewältigung natur- und zivilisationsbedingter Katastrophen und Notlagen.

Ziel der Sicherheitspolitik der Schweiz
Die schweizerische Sicherheitspolitik hat zum Ziel, die Handlungsfähigkeit, Selbstbestimmung und Integrität[1] der Schweiz und ihrer Bevölkerung sowie ihre Lebensgrundlagen gegen direkte und indirekte Bedrohungen und Gefahren zu schützen sowie einen Beitrag zu Stabilität und Frieden jenseits unserer Grenzen zu leisten.

[1] Unverletzlichkeit

Mittel und Instrumente der Schweizer Sicherheitspolitik
Zu den Instrumenten zur Umsetzung der Schweizer Sicherheitspolitik gehören die Aussenpolitik, die Armee, der Bevölkerungsschutz, der Nachrichtendienst, die Polizei, die Wirtschaftspolitik, die Zollverwaltung und der Zivildienst. Sie alle leisten Beiträge zur Prävention[2], Abwehr und Bewältigung von Bedrohungen und Gefahren für die Schweiz.

Quelle: https://www.vbs.admin.ch/de/themen/sicherheitspolitik.html

Bedrohungen und Gefahren nach Relevanz für die Sicherheitspolitik:
www.newsd.admin.ch/newsd/message/attachments/12764.pdf

AUFGABE 7:

Zusammenfassung
Fassen Sie den Informationsblock in drei bis fünf Sätzen zusammen. Formulieren Sie die Zusammenfassung in eigenen Worten.

AUFGABE 8:

Auftrag der Schweizer Armee
Gemäss Bundesverfassung trägt die Schweizer Armee die Verantwortung für die Sicherheit der Schweiz.

Auftrag der Armee: Bundesverfassung

Art. 58 Armee

1 Die Schweiz hat eine Armee. Diese ist grundsätzlich nach dem Milizprinzip[3] organisiert.

2 Die Armee dient der Kriegsverhinderung und trägt bei zur Erhaltung des Friedens; sie verteidigt das Land und seine Bevölkerung. Sie unterstützt die zivilen Behörden bei der Abwehr schwerwiegender Bedrohungen der inneren Sicherheit und bei der Bewältigung anderer ausserordentlicher Lagen. Das Gesetz kann weitere Aufgaben vorsehen.

3 Der Einsatz der Armee ist Sache des Bundes.[14]

[2] Vorsorge

[3] Milizprinzip: Aufgabe wird nebenberuflich ausgeübt.

Schauen Sie sich den Videoclip an und beantworten Sie die folgenden Fragen.

VBS/DDPS: Sicherheit – Vertrauen – Zuverlässigkeit (5:30)
https://www.youtube.com/watch?v=iWrT1phLq1o&list=PL14DDE-207F0A759+E8&index=72

1. Welche Gefahren bedrohen aktuell die Schweiz? Nennen Sie drei konkrete Beispiele.

2. In welchen Bereichen und wie fördert die Armee die Sicherheit? Nennen Sie drei konkrete Beispiele.

3. Welche Gefahren könnten uns in Zukunft bedrohen? Nennen Sie zwei Beispiele.

Sicherheit braucht es auch bei der Stromversorgung sowie für die Infrastruktur, also Kraftwerke und Stromleitungen.

AUFGABE 9:

Cyber-Szenarien

Die meisten von uns bewegen sich täglich im Internet – beruflich und privat. Wir verwalten online unser Bankkonto, kaufen in Webshops ein, schreiben E-Mails, chatten und tauschen vertrauliche Informationen aus. Computer, Smartphones und Tablets sind dabei zu unverzichtbaren Werkzeugen geworden, und dank neuen Technologien sind die Möglichkeiten heute fast grenzenlos.

Doch im Internet bewegen sich auch Menschen mit kriminellen Absichten. Sie hacken Computer, stehlen persönliche Daten und erpressen Geld. Dabei gehen sie immer professioneller vor.

Bilden Sie drei Gruppen, lesen Sie das Ihnen zugeteilte Cyber-Szenario durch und bearbeiten Sie die Aufträge. Sie werden am Schluss Ihr Szenario und die Lösungen mithilfe einer Präsentation der Klasse vorstellen.

GRUPPE 1

Flirt-App / Romance Scam (Love Scam)

a) Lesen Sie die folgende Situation durch und besprechen Sie gemeinsam Unklarheiten.

Situation
Sie surfen auf Facebook und erhalten auf einmal eine Freundschaftsanfrage einer jungen, gutaussehenden Frau oder eines jungen, gutaussehenden Mannes. Sie sind nicht sicher, ob Sie die Person kennen, nehmen die Anfrage aber an. Die Person fängt an zu chatten und wirkt sehr sympathisch. Sie entdecken, dass Sie viele gemeinsame Interessen haben. Die Person scheint einige Ihrer Freunde zu kennen. Nach vielem Hin und Her, auch spätabends, eröffnet Ihnen die Person, sich in Sie verliebt zu haben. Sie tauschen viele Messages aus. Eines Tages teilt Ihnen die Person mit, etwas Schlimmes sei passiert und sie benötige unbedingt Geld. Es geht um mehrere Tausend Franken.

b) Wie würden Sie in dieser Situation vorgehen/handeln. Erstellen Sie eine Liste.

c) Lesen Sie die folgenden Hintergrundinformationen. Fassen Sie den Inhalt in zwei bis vier vollständigen Sätzen zusammen.

Hintergrund
Mit Profilen auf Online-Dating-Seiten oder sozialen Netzwerken kontaktieren Betrüger Personen und geben vor, sich spontan verliebt zu haben. Hat ein potenzielles Opfer angebissen, kommt es zu langwierigen E-Mail-Korrespondenzen, Telefonaten und Liebesbriefen. In der dritten Phase wird meist ein Besuch versprochen.
Später wird unter verschiedenen Vorwänden um einen Geldtransfer via Western Union gebeten, um sich aus einer angeblichen misslichen Situation freikaufen zu können. Heute verfügen Romance Scammer allerdings weltweit über Bankkonten, um den Geldtransfer weniger verdächtig zu machen.

Nicht immer geht es beim Romance Scam ausschliesslich um Geld, manche Scammer versuchen auch, ihre Opfer anderweitig auszunutzen. Beispielsweise wird das Opfer unter einem Vorwand gebeten, eine Kopie seiner Ausweisdokumente zu schicken. Die auf diese Weise ermittelten Daten werden dann für betrügerische Machenschaften verwendet. Eine andere Variante betrifft einen angeblichen Freund oder Verwandten des Scammers, der in Europa lebt und Hilfe benötigt. Das Opfer soll dann beispielsweise für ihn Pakete entgegennehmen oder aufbewahren, ungewollt wird es dadurch zum Komplizen beim Drogenschmuggel.

d) Schauen Sie sich den folgenden Clip an und halten Sie den Inhalt in einer Skizze fest (z. B. Icon).

Beispiel
«Öffentliche Hotspots werden oft für Virenverbreitung und Datenklau missbraucht. Ein Angreifer kann ein manipuliertes Drahtlosnetzwerk verwenden, um Ihre Daten zu stehlen. Ein solcher Angriff ist sehr einfach und erfordert nur wenig Material.»

Öffentliche Hotspots können schädlich sein.
Ein Hotspot Ihres eigenen Handys ist sicher.

Äusserungen in Social Media sind immer als öffentlich anzusehen.
https://www.youtube.com/watch?v=1djyAM5UliU&feature=youtu.be

e) Erstellen Sie eine Präsentation (PowerPoint, Prezi) oder ein Flipchart-Poster mit den folgenden Inhalten:
- Titel der bearbeiteten Situation (Folie 1)
- Aussagekräftiges Bild/Foto der Situation (Folie 2)
- Liste mit Vorschlägen, wie man bei der Situation vorgehen soll (Folie 3)
- Tipp als Skizze: Wie man eine solche Situation verhindern kann (Folie 4)

Sicherheit im Cyber-Bereich braucht viel Knowhow über IT-Software: Programme können Schaden anrichten, aber auch schützen.

GRUPPE 2

USB-Stick liegt auf einem Pult

a) Lesen Sie die folgende Situation durch und besprechen Sie gemeinsam Unklarheiten.

Situation
Sie finden einen neu aussehenden 16 GB USB-Stick auf einem Pult. Erst kürzlich dachten Sie, dass Sie einen neuen Stick brauchen könnten. Dieser kommt gerade gelegen! Sie stecken ihn in Ihren persönlichen Laptop. Nach ein paar Tagen kommt Ihnen etwas merkwürdig vor. Ihr Laptop funktioniert nicht mehr einwandfrei.

b) Wie würden Sie in dieser Situation vorgehen/handeln. Erstellen Sie eine Liste.

c) Lesen Sie die folgenden Hintergrundinformationen. Fassen Sie den Inhalt in zwei bis vier vollständigen Sätzen zusammen.

Hintergrund
Kaum ist der USB-Stick drin, schon kann der Computer gekapert werden. So einfach soll der Cyber-Angriff sein, den deutsche Sicherheitsforscher laut «Zeit Online» entwickelt haben. Die Mitarbeiter des Berliner Security Research Labs (SRLabs) warnen: Fast alle Geräte mit USB-Anschluss, also zum Beispiel auch Tastaturen oder Webcams, haben eine Schwachstelle, die eine ganze Reihe von neuartigen Attacken möglich macht. All diesen Geräten dürfe man nicht mehr trauen.
Dabei geht es nicht um Viren oder Trojaner, die auf einem USB-Stick gespeichert sind, sondern um den sogenannten Controller-Chip des Geräts. Der sorgt für die richtige Kommunikation mit dem Rechner und hat eine eigene Software. Diese schrieben die Berliner für ihren Test um, sodass der Stick zum Beispiel so tun konnte, als sei er eine Tastatur. Also ein vertrauenswürdiges Gerät, von dem der Computer nichts zu befürchten hat. Im Vordergrund konnte das Opfer, ein eingeweihter WDR-Journalist in Köln, den USB-Stick ganz normal zum Speichern von Daten verwenden. Im Hintergrund konnte das Gerät jedoch Befehle in die Windows-Eingabemaske tippen – wie eine Tastatur eben.

d) Schauen Sie sich den folgenden Clip an und halten Sie den Inhalt in einer Skizze fest (z. B. Icon).

Beispiel
«Öffentliche Hotspots werden oft für Virenverbreitung und Datenklau missbraucht. Ein Angreifer kann ein manipuliertes Drahtlosnetzwerk verwenden, um Ihre Daten zu stehlen. Ein solcher Angriff ist sehr einfach und erfordert nur wenig Material.»

Öffentliche Hotspots können schädlich sein.
Ein Hotspot Ihres eigenen Handys ist sicher.

Niemals fremde USB-Geräte an Ihren privaten PC oder Ihre Geräte am Arbeitsplatz anschliessen.
www.youtube.com/watch?v=YYpniVf6nz0&feature=youtu.be

d) Erstellen Sie eine Präsentation (PowerPoint, Prezi) oder ein Flipchart-Poster mit den folgenden Inhalten:
- Titel der bearbeiteten Situation (Folie 1)
- Aussagekräftiges Bild/Foto der Situation (Folie 2)
- Liste mit Vorschlägen, wie man bei der Situation vorgehen soll (Folie 3)
- Tipp als Skizze: Wie man eine solche Situation verhindern kann (Folie 4)

GRUPPE 3

Erpressungstrojaner

a) Lesen Sie die folgende Situation durch und besprechen Sie gemeinsam Unklarheiten.

Situation
Sie erhalten eine E-Mail. Darin befindet sich ein Link, den Sie angeblich anklicken sollen, um für Sie interessante Informationen zu erhalten. Nachdem Sie geklickt haben, passieren seltsame Dinge auf Ihrem PC/Smartphone.
Oder:
Sie erhalten eine E-Mail Ihrer Bank. Darin werden Sie gebeten, Ihre Kontoinformationen zu aktualisieren. Das Logo stimmt, ebenfalls klingt der Text plausibel. Sie sollen auf einen Link klicken. Danach werden Ihre Daten abgefragt: Kontonummer, Username und auch Passwort. Ihnen kommt dies seltsam vor, aber schliesslich fragt Ihre Bank danach.

b) Wie würden Sie in dieser Situation vorgehen/handeln. Erstellen Sie eine Liste.

c) Lesen Sie die folgenden Hintergrundinformationen. Fassen Sie den Inhalt in zwei bis vier vollständigen Sätzen zusammen.

Hintergrund
Zu oft werden die Gefahren, die im Netz lauern, unterschätzt. Mittlerweile kennen Internetnutzerinnen und Internetnutzer das Phänomen ungewollter E-Mails, sogenannter Spam-Mails. Noch nicht genügend bekannt ist aber, dass E-Mails als ganz gewöhnliche Nachrichten von Mitarbeiterinnen und Mitarbeiter oder gar Vorgesetzten daherkommen, jedoch von anderen Absendern stammen können. Es geht um sogenanntes Social Engineering, also Sozialtechniken: Personen benutzen eine falsche Identität, um das Vertrauen der Internet- und E-Mail-Nutzer zu gewinnen. Eigentlich ist das der Enkeltrick im Cyber-Raum. Personen werden dazu gebracht, Links anzuklicken oder Anhänge (Attachments) zu öffnen, und schon hat ein Hacker Zugriff. Beim Spear Fishing werden E-Mail-Empfängerinnen und -Empfänger etwa mit attraktiven Angeboten geködert. Oder bestimmte Gruppen klauen Daten und Fotos von Rechnern und verkaufen sie an die Eigentümer zurück. Falls Letztere nicht bezahlen, wird alles unwiderruflich gelöscht, und Sie verlieren Ihre Daten, wenn Sie kein Backup haben. Es handelt sich dabei um Kriminalität als Geschäftsmodell: im Jargon «Crime as a Business» genannt.

c) Schauen Sie sich den folgenden Clip an und halten Sie den Inhalt in einer Skizze fest (z. B. Icon).

Beispiel
«Öffentliche Hotspots werden oft für Virenverbreitung und Datenklau missbraucht. Ein Angreifer kann ein manipuliertes Drahtlosnetzwerk verwenden, um Ihre Daten zu stehlen. Ein solcher Angriff ist sehr einfach und erfordert nur wenig Material.»

Öffentliche Hotspots können schädlich sein.
Ein Hotspot Ihres eigenen Handys ist sicher.

Keine Mitteilungen/Anhänge/Links unerwarteter Herkunft öffnen. Kontaktieren Sie bei Verdacht den Absender direkt (z. B. anrufen).
www.youtube.com/watch?v=NpMp5pqK6kk&feature=youtu.be

d) Erstellen Sie eine Präsentation (PowerPoint, Prezi) oder ein Flipchart-Poster mit den folgenden Inhalten:
- Titel der bearbeiteten Situation (Folie 1)
- Aussagekräftiges Bild/Foto der Situation (Folie 2)
- Liste mit Vorschlägen, wie man bei der Situation vorgehen soll (Folie 3)
- Tipp als Skizze: Wie man eine solche Situation verhindern kann (Folie 4)

AUFGABE 10:

Eingangszitat

Auf der Titelseite dieses Moduls haben Sie folgendes Zitat von Erwin Koch gelesen:

«Sicherheit gibt es mit Sicherheit nicht.»
Erwin Koch (*1932), deutscher Aphoristiker

a) Formulieren Sie in eigenen Worten, was Erwin Koch mit seinem Zitat aussagen will.

b) Sind Sie mit Erwin Koch einverstanden? Begründen Sie Ihre Meinung.

ZUSATZAUFGABE 1:

Cyber-Attacken

Eine Cyber-Attacke gegen die Schweizer Armee ist gravierend. Deshalb: Sicherheit ist heute ein sehr viel komplexeres Thema als früher.

Cyber-Bedrohungen

Die Formen der Cyber-Bedrohungen lassen sich in folgende Kategorien einordnen:
– Vandalismus
– Aktivismus
– Kriminalität
– Terrorismus
– Konflikt

Dabei ist es in der Regel nicht möglich, zwischen diesen Kategorien eine scharfe Trennung vorzunehmen.

Rolle der Armee

Von der Armee wird erwartet, dass sie bei einer schweren Krise, auch bei einer Cyber-Krise, ihren Unterstützungsbeitrag leistet, mit dem das Land die Auswirkungen auf kritische Infrastrukturen, Versorgung und Sicherheit meistern kann.

Akteure

Die Bedrohungsakteure werden grob in fünf Stufen (Bedrohungen B1 bis B5) eingeteilt. Die Komplexität der Angriffe und das dafür nötige Knowhow nehmen von unten nach oben zu. Die Wahrscheinlichkeit, davon betroffen zu sein und einen Schaden zu erleiden, nimmt hingegen ab.

Lesen Sie zu diesem Thema das Interview mit Bundesrat Guy Parmelin «Wir haben fast täglich Cyber-Angriffe».
www.vbs.admin.ch/de/verteidigung/schutz-vor-cyber-angriffen.detail.news.html/vbs-internet/interviews/2017/171023.html.html

Fragestellung zum Thema

Diskutieren Sie die folgende Fragestellung in der Klasse: Sollte die Armee mehr in die Cyber-Abwehr investieren?

ZUSATZAUFGABE 2:

Videoclip «Sicherheit»

Erstellen Sie einen Videoclip, der den Begriff «Sicherheit» zum Thema hat. Überlegen Sie sich zuerst mögliche Gestaltungsvarianten. Gehen Sie anschliessend in folgenden Schritten vor:

a) Entwickeln Sie eine Idee, wie das Thema «Sicherheit» dargestellt werden könnte.
b) Schreiben Sie ein kurzes Storyboard mit maximal vier Szenen.
c) Sprechen Sie die Szenen durch.
d) Zeichnen Sie den Videoclip auf.
e) Sprechen Sie mit der Lehrperson ab, wo die fertigen Videoclips gespeichert werden sollen.

WEITERFÜHRENDE MATERIALIEN/LINKS

«Blackout» von Marc Elsberg
Wikipedia: Siehe Handlung in Einzelübersicht
https://de.wikipedia.org/wiki/Blackout_%E2%80%93_Morgen_ist_es_zu_sp%C3%A4t

Kurzinterview Marc Elsberg
www.blackout-das-buch.de/autor.php

Buchtrailer zu «Blackout» von Marc Elsberg
www.youtube.com/watch?v=M3_wpgF8Z7c

Surfen Sie mit Verstand!
www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/cybercrime.html

Cyber-Defence
Checkliste
www.vtg.admin.ch/de/aktuell/themen/cyberdefence.html

HP-Schulungsfilm zu Cyber-Crime
«The Wolf: Die Jagd geht weiter» (mit Christian Slater) 7:10 min
www.youtube.com/watch?v=Rr_y0ST1Llk

Romance Scam
Das üble Spiel der Romantik-Betrüger
www.srf.ch/news/panorama/das-ueble-spiel-der-romantik-betrueger

Neuartige Cyber-Attacke
Die Gefahr steckt im USB-Stick
www.stern.de/digital/computer/neuartige-cyber-attacke-die-gefahr-steckt-im-usb-stick-3956212.html

Nutzer stecken USB-Sticks einfach so in ihre Geräte
www.20min.ch/finance/news/story/Nutzer-stecken-USB-Sticks-einfach-so-in-ihre-Geraete-10807493

Erpressung macht sich breit
Ransomware mit neuen Tricks und Techniken
www.heise.de/select/ct/2018/2/1515455905443518

Lagebericht 2018 «Sicherheit Schweiz»
Nachrichtendienst des Bundes
www.vbs.admin.ch/content/vbs-internet/de/die-aktuellsten-informationen-des-vbs/die-neusten-medienmitteilungen-des-vbs.detail.nsb.html/70611.html

www.newsd.admin.ch/newsd/message/attachments/52215.pdf

14-38_010_dfi_Pocketcard_Cyber_Security_2017
PDF-Datei
https://www.vtg.admin.ch/de/aktuell/themen/cyberdefence.html

11-zeitschrift27_2017de_BABS_Cyber-Risiken
PDF-Datei
https://www.babs.admin.ch/de/publikservice/information/zeitschriftbabs.detail.publication.html/babs-internet/de/publications/publikationenservice/zeitschriftbevoelkerungsschutz/zeitschrift29_2017de.pdf.html

Sicherheitspolitischer Bericht 2016
PDF-Datei
www.vbs.admin.ch/de/themen/sicherheitspolitik/sicherheitspolitische-berichte/sicherheitspolitischer-bericht-2016.detail.document.html/vbs-internet/de/documents/sicherheitspolitik/sipolb2016/SIPOL-B-2016-de.pdf.html

«Cyber-Landsgemeinde» des Sicherheitsverbunds Schweiz
www.vbs.admin.ch/content/vbs-internet/de/die-aktuellsten-informationen-des-vbs/die-neusten-medienmitteilungen-des-vbs.detail.nsb.html/70580.html

Cyber-Risiken
Zeitschrift Bundesamt für Bevölkerungsschutz Nr. 27, März 2017. Chancen und Risiken neuer Technologien: S. 7 – 9; Internetbetrüger: S. 10 – 12. Cyber-Risiken im Bevölkerungsschutz S. 16 – 18
www.babs.admin.ch/de/publikservice/information/zeitschriftbabs.detail.publication.html/babs-internet/de/publications/publikationenservice/zeitschriftbevoelkerungsschutz/zeitschrift27_2017de.pdf.html

Das Kryptologen-Detachement der Armee:
Mit angewandter Mathematik zu mehr Sicherheit. Artikel ASMZ 04/17.
PDF-Datei

BILDNACHWEIS

Euronews: S. 4 (Mitte)
iStock: S. 8 (beide), S. 10
Robby80: S. 4 (oben)
SRF: S. 4 (unten)
VBS: S. 1 (alle), S. 4
YouTube: S. 4 (unten)