

LEHRERMAPPE

LESESKRIPT & UNTERRICHTSMATERIAL



GRUNDEINSTELLUNGEN – FÜR EINEN SICHEREN ARBEITSPLATZ

LERNEINHEIT 1





LERNEINHEIT 1: GRUNDEINSTELLUNGEN FÜR EINEN SICHEREN ARBEITSPLATZ

Ein sicherer Arbeitsplatz muss die Grundlagen der Datensicherheit berücksichtigen. Ein **sicheres Passwort**, ein **aktuelles Antiviren-Programm** und die **Firewall** gehören zu der Grundausstattung im Betrieb. Aber auch die **Software** muss ständig aktuell gehalten werden, damit alles reibungslos und sicher funktioniert. Denn gerade im wirtschaftlichen Bereich werden unseriöse Akteure immer kreativer – was für kleinere und mittlere Unternehmen ein hohes Risiko bedeuten kann.



DIE THEMEN:

- | | |
|---|----------|
| 1. IT-Sicherheitsrisiken: Viren, Trojaner und Co. | Seite 3 |
| 2. Abwehr von Schadsoftware: Virenschutz und Firewall | Seite 7 |
| 3. Sicherheitsvorkehrungen bei Browser und Software | Seite 11 |
| 4. Das sichere Passwort im Arbeitsalltag: 123456? | Seite 14 |
| Unterrichtsmaterialien | Seite 17 |

Für welche Ausbildungslehrgänge empfohlen?

Diese Lerneinheit wird allen Ausbildungslehrgängen und vor allem bei **fehlendem Grundlagenwissen** empfohlen.



LERNZIELE

Nach diesen Unterrichtseinheiten wissen die Schüler*:

- ✓ wie man einen Schadprogrammbefall bemerkt,
- ✓ wie eine Firewall vor ungebeten Gästen schützt,
- ✓ wie Softwareaktualisierungen und Plug-ins zur IT-Sicherheit beitragen,
- ✓ welche Sicherheitseinstellungen bei Browser und Software zu beachten sind,
- ✓ wie ein sicheres Passwort aussieht.

*Obwohl aus Gründen der Lesbarkeit im Text die männliche Form gewählt wurde, beziehen sich die Angaben auf Angehörige aller Geschlechter. In den Arbeitsmaterialien für den Unterricht wird dagegen das Gender-Sternchen verwendet.



1. IT-SICHERHEITSRISIKEN: VIREN, TROJANER UND CO.

Malware vom engl. malicious Software = Schadsoftware.

Schadprogramme oder Malware (Abkürzung von engl. malicious Software = Schadsoftware) sind heutzutage ein Oberbegriff für solche Programme, die sich in andere Programme oder Dateien einschleusen, sich selber verbreiten und Schadfunktionen ausführen. So kann Schadsoftware beispielsweise Veränderungen an Hardware, dem Betriebssystem und der Software vornehmen und erheblich die Computersicherheit gefährden. Beispiele für Schadprogramme sind **Trojaner, Viren, und Würmer**.

Computervirus: häufig Synonym für Schadsoftware.

Der Begriff **Computervirus** wird umgangssprachlich häufig für Schadsoftware verwendet. Ein Computervirus ist ein Schadprogramm mit einer Infektionsfunktion, welches sich selbst in ein Wirtsprogramm (bzw. Dokumente, Skripte und Makros, oder sogar dem Bootsektor) einschleust und beim Ausführen dieses Programms (bzw. der Datei etc.) mitaufgerufen wird. Im Anschluss verbreitet sich das Virus weiter oder führt eine Schadfunktion aus bzw. beeinträchtigt das Wirtsprogramm oder das gesamte Wirtssystem. Fehlfunktionen, Datenverlust oder ganze Hard- und Softwareschäden können die Folge sein.



VERBREITUNGSWEGE VON SCHADSOFTWARE



- > **Wechseldatenträger:** USB-Sticks, Wechselfestplatten, aber auch CDs und DVDs.
- > **Netzwerke:** Viren können sich über lokale Netzwerke (LAN) oder globale Netzwerke (WAN) verbreiten; besonders **P2P-Netzwerke** (peer-to-peer: Zusammenschluss gleichberechtigter Arbeitsstationen in einem Netzwerk; kein zentraler Server nötig), wie sie bei Tauschbörsen eingesetzt werden, werden von Angreifern ausgenutzt.
- > **Infizierte Webseiten:** Nutzer laden sich unbemerkt bereits beim Aufsuchen einer Webseite Schadsoftware auf den Rechner (sogeannter **drive-by-download**). Hierbei werden von den Viren Sicherheitslücken in den Browsern ausgenutzt.
- > **E-Mail: Phishing** E-Mails (gefälschte Absender und Betreffe) enthalten oftmals infizierte Dateianhänge oder Links, die auf infizierte Webseiten verlinken.
- > **Downloads:** Neben den erwähnten P2P-Downloads sind heruntergeladene Dateien (z.B. über FTP-Server), vor allem von nicht vertrauenswürdigen Quellen, oftmals mit Schadsoftware verseucht.
- > **Instant Messaging:** Über Messenger wie WhatsApp, Skype oder MSN Messenger werden gezielt Links mit Würmern verbreitet.



ANREGUNGEN FÜR DEN UNTERRICHT

Diskussionsfrage: Welche Schadprogramme kennen die Schüler?
Waren sie selbst bereits schon betroffen?



LINKTIPP

Spiel 3 „Datenträger“ von Sichere Identität Berlin Brandenburg:
<http://www.sichere-identitaet-bb.de/sicheriminternet/>

Schadsoftware wird
häufig durch Anhän-
ge übertragen.

Die schnelle Gefahr: Computer Würme

Ein **Computerwurm** oder einfach auch Wurm genannt, ist eine **eigenständige Programmroutine**, die sich auf dem Rechner oder auch Smartphone verbreitet und dort zum Teil einen erheblichen Schaden anrichtet.

Die **Aktivierung eines Computerwurms** geschieht entweder durch eine manuelle Ausführung des Benutzers, beispielweise über das **Öffnen eines Dateianhangs**. Die Aktivierung kann aber auch automatisch geschehen (anders als beim Computervirus), indem der Computerwurm eine **Sicherheitslücke im Programm** nutzt, sobald er auf dem Zielsystem eingetroffen ist. Diese Variante der Verbreitung ist häufig anzutreffen, da sie effizient ist und so sehr schnell viele Systeme infiziert werden können. Zum Beispiel kann sich ein Computerwurm in einem **Anhang einer E-Mail** verstecken und sich selbstständig an alle Kontakte des Adressbuches verschicken. Ist der Computerwurm im Postfach der Kontakte angelangt, wiederholt er den Vorgang. So können sich Würmer in einer rasenden Geschwindigkeit ausbreiten und ganze Netzwerke infizieren.

Die Auswirkungen eines Wurmbefalls können im Firmennetzwerk großen Schaden anrichten. Die **Folgekosten** im Unternehmen können beachtlich sein, da Zeit, Personal und Software für die Beseitigung des schädlichen Codes und zur Wiederherstellung der Daten und Funktionen zum Einsatz kommen müssen.



ANREGUNGEN FÜR DEN UNTERRICHT

Diskussionsfrage: Wie verbreiten sich Schadprogramme wie Viren?

Getarnte Schädlinge: Trojaner

Bei Trojanischen Pferden - oder nur kurz **Trojanern** - handelt es sich dem Äußeren nach um vermeintlich nutzvolle Software, die **im Hintergrund jedoch für den Nutzer nicht sichtbare Funktionen ausführt**. Sie stellen mit mehr als drei Vierteln die häufigste Art von Schadsoftware dar. Häufig dienen Würmer dazu, Trojanische Pferde auf dem Computer zu verbreiten, da Trojaner nicht in der Lage sind, sich selbsttätig zu vervielfältigen. Insbesondere im **Firmennetzwerk** sind Trojaner eine echte Bedrohung und als sehr gefährlich einzustufen.



Zu den **schädlichen Aktionen**, die Trojaner ausführen können, gehören unter anderem:

- > das Löschen,
- > das Sperren,
- > das Modifizieren,
- > sowie das Kopieren von Daten.
- > Beeinträchtigen der Funktionalität von Computern oder Computernetzwerken.

Trojaner haben ein **breites Spektrum an Schaden**, den sie anrichten können. Entsprechend groß sind die unterschiedlichen Varianten von Trojanern. Sie werden anhand der Aktivität klassifiziert, die sie auf einem Computer ausführen.



VERTIEFUNG: ÜBERSICHT VON UNTERSCHIEDLICHEN TROJANERN

Variante 1 - Backdoor-Trojaner: Ein Backdoor-Trojaner übergibt einem anderen Benutzer die Kontrolle über den infizierten Computer. Der Benutzer, der den Trojaner eingeschleust hat, kann dann beliebige Aktionen ausführen, einschließlich Senden, Empfangen, Starten und Löschen von Dateien, Anzeigen von Daten oder Neustart des Computers. Backdoor-Trojaner werden häufig eingesetzt, um die befallenen Computer zu einem **Botnet** oder Zombie-Netzwerk zusammenzuschließen, das dann zu kriminellen Zwecken verwendet wird (siehe unten „Botnetz-Betrug“).

Variante 2 - Exploits: Exploits sind Programme, die Daten oder Codes enthalten, mit dem sich Schwachstellen innerhalb der auf dem Computer ausgeführten Programmsoftware ausnutzen lassen.

Variante 3 - Rootkit: Mit Rootkits lassen sich bestimmte Objekte oder Vorgänge auf dem System verstecken. Sie dienen meistens dazu, die Entdeckung durch Schadsoftware auf einem System zu verhindern, um damit den Zeitraum zu verlängern, in dem Programme auf einem befallenen Computer ungehindert ausgeführt werden können.

Variante 4 - Trojan-Dropper: Diese Programme werden von Hackern eingesetzt, um Trojaner bzw. Viren zu installieren. Nicht alle Antiviren-Programme sind in der Lage, sämtliche Bestandteile innerhalb dieses Trojaner-Typs zu untersuchen.

Variante 5 - Trojan-Mailfinder: Diese Programme dienen dazu, die auf Ihrem Computer vorhandenen E-Mail-Adressen abzuschöpfen.



ANREGUNGEN FÜR DEN UNTERRICHT

Diskussionsfrage: Wie kann man einen Virenbefall bemerken?



ANZEICHEN EINES BEFALLS

- > der Computer wird immer langsamer,
- > vorher laufende Funktionen werden nicht mehr ausgeführt,
- > Dateien verschwinden,
- > Abstürze werden häufiger,
- > der Browser öffnet unbekannte Webseiten,
- > der Computer verhält sich ungewöhnlich und gibt merkwürdige Meldungen.

(D)DoS-Attacken

stehen für (Distribu-
ted) Denial of Ser-
vice Angriffe: dabei
wird von einer Viel-
zahl von infizierten
Botrechnern z.B.
eine Website gleich-
zeitig aufgerufen, so
dass der Webserver
unter der Last zu-
sammenbricht. Die
Website ist dadurch
dann nicht mehr
aufrufbar für andere
Nutzer.

Botnetz-Betrug

Botnetze sind ein wichtiges Werkzeug für Online-Kriminelle. Ein Botnetz oder Botnet ist eine Gruppe von automatisierten Computerprogrammen. Die Betreiber installieren diese speziellen Schädlinge ohne Wissen der Inhaber auf Computern und nutzen sie für ihre Zwecke. Sie installieren daraufhin oft weitere Programme, z.B. zum **Versenden von Spam-Mails** oder um koordinierte Angriffe auf Web-Server zu starten (z.B. (D)DoS-Attacken).

Botnetze werden oft über zentrale Kommando-Server gesteuert, die auch als Mutterschiffe bezeichnet werden. Die infizierten Rechner, Zombies genannt, halten Kontakt mit einem der Mutterschiffe oder untereinander. Sie geben ausgespähte Daten wie etwa Passwörter für Banken-Webseiten, aber auch gesammelte Mail-Adressen oder Kreditkartendaten an den Angreifer weiter. Mittlerweile ist das Vermieten von Botnetzen für gezielte Angriffe ein lukratives Geschäft für Cyber-Kriminelle geworden.



LINKTIPP

Weitere Informationen zum Thema **Botnetze** und dem Schutz davor finden sich beim Anti-Botnet-Beratungszentrum (einem Projekt des eco – Verband der deutschen Internetwirtschaft e.V.) unter: <https://www.botfrei.de/>



2. ABWEHR VON SCHADSOFTWARE: VIRENSCHUTZ UND FIREWALL

Ein **Antiviren-Programm, Virenschanner oder Virenschutz-Programm** ist eine **Software**, die bekannte **Computerviren** **aufspüren, blockieren** und **beseitigen** soll. Hierbei steht Nutzern eine Vielzahl von Programmen unterschiedlicher Anbieter zur Verfügung. Im privaten Bereich reichen die kostenfreien Angebote der Anbieter oftmals aus. Kostenpflichtige und professionelle Angebote sollten von kleineren Unternehmen in Erwägung gezogen werden.



HINTERGRUNDWISSEN VIRENSCANNER

Echtzeitscanner und manuelle Scanner

Echtzeitscanner (auch Zugriffsscanner genannt) und manuelle Scanner (auch Dateiscanner genannt) werden mit dem Betriebssystem ausgeliefert oder als Programme lokal installiert. Während der Echtzeitscanner permanent im Hintergrund läuft und Dateien, Programme, Arbeitsspeicher und eventuell den Datenverkehr überwacht, wird diese Überprüfung beim manuellen Scanner vom Nutzer ausgelöst (oder per Assistent zu bestimmten Zeiten automatisch ausgelöst), um eine tiefergehende Prüfung des Systems vorzunehmen. Auf jedem System sollten diese Scanner installiert sein und zum Einsatz kommen.

Online-Virenschanner

Diese Scanner sind über Webseiten oder auch Erweiterungen in Browsern verfügbar. Sie bieten sich vor allem für das Scannen einzelner Dateien an und sind stets auf dem neuesten Stand. Die Dateien werden dabei zur Prüfung auf den Webservice hochgeladen. Das Hochladen geschäftskritischer Dateien sollte dabei vermieden werden. Einige Anbieter von Online-Scannern bieten die Möglichkeit an, eine URL mit einer dort hinterlegten Datei, die man sich zum Beispiel herunterladen möchte, zu übertragen, und die Datei vorab zu überprüfen.

Ist der Scanner in der Lage den Virus aus der Datei zu entfernen, erfolgt dies über die Option „**Reinigung**“. Kann der Scanner den Virus nicht aus der Datei entfernen, bieten sich in der Regel zwei Optionen:

- > Der Scanner kann die befallene Datei **löschen**. Hierbei gehen jedoch die **Dateiinhalte verloren**.
- > Der Scanner kann die Datei in **Quarantäne** verschieben. Die Isolierung der Datei sorgt dafür, dass der Virus **kein weiteres Unheil** auf dem PC anrichten kann.

Was die Scanner mit gefundenen Viren tun können: Reinigung, Löschen, Quarantäne.



ANREGUNGEN FÜR DEN UNTERRICHT

Falls es einen PC mit Internetzugang im Klassenraum gibt, zeigen sie den Schülern den installierten Virensch scanner und führen Sie gemeinsam einen Scan durch.

Virensch scanner sind Ergänzung zu allgemeinen Vorsichtsmaßnahmen, entbinden den Nutzer aber nicht vom aufmerksamen Handeln bei der Internetnutzung.

Die Leistung von Virenschutzprogrammen

Virensch scanner erkennen **Schadprogramme** (Viren, Würmer, Trojaner etc.) auf zwei Weisen: Der Anbieter des Virensch scanners analysiert neue Viren, ermittelt deren Signatur und aktualisiert diese in der Datenbank, mit der sich der Virensch scanner in regelmäßigen Abständen – oder manuell ausgelöst – zum Abgleich verbindet. Aus diesem Grund ist es wichtig, dass die Datenbanken von Virensch scanner regelmäßig aktualisiert werden. Es gibt auch Virensch scanner, die u.a. aufgrund von heuristischen Methoden neuartige Schadsoftware auf dem Rechner selber erkennt.




VIRENSCHUTZ – TIPPS AUF EINEN BLICK

- ✓ **Keine E-Mails mit unbekannten Anhängen öffnen!** Dies ist immer noch einer der meist genutzten Verbreitungswege für Viren.
- ✓ **Gastkonto verwenden, um im Internet zu surfen!** Somit kann Schadsoftware keine Administratorrechte ausnutzen, um im Hintergrund Programme zu installieren oder Systemdateien zu verändern.
- ✓ **Regelmäßige Aktualisierung des Virenschutz-Programmes!** Nur bekannte Viren können auch erkannt werden.
- ✓ **Sichere Passwörter nutzen!**
- ✓ **Vorsichtig sein mit fremder Software und Dateien von Kunden oder Geschäftspartnern!** Durch Unwissenheit oder Sabotage können sich hier Viren befinden.

Sicherheitscheck: Status des Virenschutzes bei Windows überprüfen

Der Status des Virenschutzes lässt sich bei **Windows** ganz einfach im Wartungscenter des Computers überprüfen.

1. Wartungscenter öffnen durch das Klicken auf die Schaltfläche **Start** , dann auf **Systemsteuerung** klicken, **System und Sicherheit** auswählen und dann auf **Wartungscenter** klicken.
2. Unter **Sicherheit** wird die Antiviren-Software bei **Virenschutz und/oder Schutz vor Spyware und unerwünschter Software** aufgelistet, sofern Windows diese erkennt.
3. Falls die Software aktualisiert werden muss, auf **Jetzt aktualisieren** klicken.



ANREGUNG FÜR DEN UNTERRICHT

Falls es einen PC mit Microsoft Windows Betriebssystem im Klassenraum gibt, führen Sie gemeinsam mit den Schülern den Sicherheitscheck durch.

Firewall: Beschränkt Netzwerkzugriff und überwacht den Datenverkehr.

Die Firewall: Der Türsteher des Netzwerks

Ein **Virens Scanner** durchsucht ein System **intern** nach Schädlingen. Eine **Firewall** schützt den PC oder das Netzwerk **vor Zugriffen von außen**, indem der durch die Firewall laufende Datenverkehr überwacht wird und Netzwerkzugriffe beschränkt bzw. unterbunden werden.

Um einen bestmöglichen Schutz zu erlangen, sollte man die Computer bzw. Netzwerke mit **beiden Varianten** ausstatten, wenn regelmäßig im Internet gesurft wird.

Grundsätzlich wird unterschieden zwischen einer **Personal Firewall** (Desktop Firewall) und einer **externen Firewall** (Netzwerk- oder Hardware-Firewall). Die Desktop Firewall wird als Anwendung bzw. Programm auf dem Rechner installiert. Die Software einer externen Firewall arbeitet nicht auf dem zu schützenden System selbst, sondern auf Geräten im Netzwerk.



VIRENSCANNER UND FIREWALL: FÜR DEN BESTEN SCHUTZ IMMER BEIDE SCHUTZVORKEHRUNGEN INSTALLIEREN!

Die Firewall kann

- > nur präventiv schützen
- > nicht aktiv in die Virenvernichtung eingreifen
- > nur ein Teilaspekt eines Sicherheitssystems sein



LINKTIPP

Das Onlinespiel zum Thema „Allgemeine IT-Sicherheit“ von Sichere Identität Berlin Brandenburg:



<http://www.sichere-identitaet-bb.de/microsites/sicheriminternet/episode3/>



3. SICHERHEITSVORKEHRUNGEN BEI BROWSER UND SOFTWARE

Beim Besuch einer Internetseite speichert der Browser Bilder, Texte und ggfs. Videos im **Cache** (Puffer, Speicher) des Browsers. Dabei ist es möglich, dass der Browser Programmcodes ausführt und so **automatisch Schadsoftware wie Viren, Würmer und Trojaner auf den Rechner lädt**. Viele Webseiten setzen z.B. **JavaScript** ein, um Funktionalität und die „User Experience“ der Seitenbesucher zu gewährleisten; allerdings werden diese Scripte auch von vielen Webseiten (oft ohne Wissen des Betreibers) zur Verbreitung von Schadsoftware genutzt.

Flash und JavaScript erhöhen die User Experience, aber auch das Sicherheitsrisiko.

Viele der üblichen Browser verfügen über eine gute Sicherheitsausstattung und enthalten z.B. einen **eingebauten Filter, der vor schädlichen Webseiten warnt**. Für ein Höchstmaß an Sicherheit beim Surfen sollte mit den meisten Browsern das **Ausführen von Flash, JavaScript oder Java Applets etc. auf ausgewählte, vertrauenswürdige Seiten beschränkt werden** (siehe auch folgender Absatz). Dies kann in den Browser-Einstellungen oder mit Hilfe von Software-Erweiterungen für den Browser, den sogenannten **Plug-ins** (siehe nächster Abschnitt) erfolgen.



LINKTIPP

Für kleine und mittlere Unternehmen und Webseitenbetreiber bieten sich Webseitenchecks wie <https://www.initiative-s.de> an.

Plug-ins oder Add-ons erhöhen für viele gängige Browser die Sicherheit beim Surfen.

Nützliche Plug-ins und Filter

Mittlerweile sind alle gängigen Browser mit sogenannten **Plug-ins** (auch **Add-ons** bzw. **Erweiterungen**) ausgestattet, die dem Nutzer **mehr Sicherheit** während des Surfens bieten. Vor der Installation von Plug-ins sollte der Nutzer sich anhand der **Bewertungen und weiteren Informationen** (Foren, Artikeln, Website) ein umfassendes Bild über die Vertrauenswürdigkeit des Urhebers des Plug-ins verschaffen. Zum allgemeinen Grundschutz gehören Erweiterungen, die das Ausführen von Scripten unterbinden, um beispielsweise das Ausführen von JavaScript zu verhindern oder vor dem Ausführen zur Bestätigung auffordern. Außerdem gibt es Erweiterungen, die den Browser immer eine sichere, **verschlüsselte Verbindung (SSL)** zum Server aufbauen lassen, sofern der Betreiber dies anbietet (hier ist die Erweiterung „HTTPS EVERYWHERE“ der *Electronic Frontier Foundation* zu empfehlen).

Viele Webseitenbetreiber „tracken“ (verfolgen) das Nutzungsverhalten eines Seitenbesuchers, um so z.B. die Seite für Besucher zu optimieren. Auch hier bieten viele Erweiterungen an, das Tracken zu unterbinden – neben der Möglichkeit, das „do not track“-Häkchen in den Einstellungen der jeweiligen Browser vorzunehmen. Viele dieser Erweiterungen zeigen dem Nutzer im Browser an, wie viele Tracker unterdrückt wurden, und von wem sie stammen.

Zudem können Werbeflocker bzw. „**Ad-Blocker**“ (von engl. „Advertisement“), die das Einblenden von Werbung unterbinden, die Sicherheit beim Surfen erhöhen, da Werbung oftmals von Servern Dritter geladen wird,



und hier Sicherungsvorkehrungen seitens des primären Webseitenbetreibers in der Regel fehlen.

Auch bei diesem Plug-in können selbstverständlich Ausnahmen hinzugefügt werden, um den Betreiber einer Seite die Werbeeinnahmen zu ermöglichen. Mittlerweile sind einige Webseiten mit installierten Werbeblockern gar nicht mehr oder nur eingeschränkt nutzbar. Die Webseitenbetreiber sind auf die Werbeeinnahmen angewiesen und unterbinden ihrerseits das Anzeigen von Inhalten bei Browsern mit diesen Erweiterungen. Bei der Auswahl der Anbieter von Ad-Blockern sollte genauer hingeschaut werden, woher die Erweiterung kommt, und was gegebenenfalls das Geschäftsmodell des Anbieters ist. Oftmals stecken hinter diesen Erweiterungen nicht nur altruistische Beweggründe.

Sicherheitshinweise zu Plug-ins

Auch Plug-ins, die Sicherheit propagieren, sollten niemals blind vertraut werden.

Neben dem Browser selbst sollten auch installierte **Plug-ins regelmäßig aktualisiert** werden, um den erweiterten Schutz bieten zu können. Grundsätzlich sollten auch **Plug-ins niemals blind vertraut** werden, auch wenn sie damit werben, dem Nutzer mehr Sicherheit zu bieten. Plug-ins sind in der Lage, Daten über das Surfverhalten des Nutzers anzulegen, und diese können wiederum an Datenhändler verkauft werden. Nutzer sollten sich aus diesem Grund vor der Installation der Plug-ins über den Ursprung der Erweiterung im Bilde sein, und abwägen, ob der propagierte Gewinn an Sicherheit gegenüber Webseitenbetreibern nicht zulasten der Sicherheit der eigenen Daten geht. Im Zweifel sollten Plug-ins nicht verwendet werden, und nur die oben erwähnten Anwendungsfälle in Betracht gezogen werden.

Sicherheitsrisiko Cookies

Cookies stellen ein erhöhtes Daten-schutzrisiko für Unternehmen dar.

Cookies sind Textdateien und enthalten typischerweise **Daten über besuchte Webseiten**, die vom Webbrowser beim Surfen im Internet gespeichert werden. Sie können den Nutzer beim nächsten Seitenbesuch wiedererkennen. Mit ihnen kann auch das **Surfverhalten nachverfolgt werden**, aufgrund dessen stellen Cookies ein **Datenschutzrisiko** für Unternehmen dar und sollten nach jeder Online-Sitzung **automatisch gelöscht werden**. „**Cookies von Drittanbietern**“ sollten generell **nicht** zugelassen werden (dies lässt sich in den Browser-Einstellungen regeln).

Einige Browser ermöglichen, den Web- und Werbeanbietern mitzuteilen, dass man nicht verfolgt werden möchte („**do not track**“). Dann liegt es allerdings bei den Betreibern der Webseite, diese Einstellung zu respektieren, weshalb sie **kein Ersatz für entsprechende Plug-ins** (s.o.) bildet.

Die sogenannten **Flash-Cookies** (auch LSO-Cookies genannt) sammeln besonders viele Daten im Vergleich zu den normalen Text-Cookies. Diese Cookies speichern Daten unabhängig vom eingesetzten Browser und besitzen eine längere Verweildauer. Somit werden sie auch nicht von den Cookie-Einstellungen im Browser eingeschränkt.



SICHERHEITSTIPP FÜR UNTERNEHMEN

Die Nutzung von interaktiven und multimedialen Inhalten ist mit Sicherheitsrisiken verbunden. Cookies sollten regelmäßig gelöscht und Sicherheitsupdates regelmäßig ausgeführt werden, um Daten des Unternehmens besser zu schützen.



Aktuell und schnell: Die sichere Software für den Arbeitsplatz

Um ein bestimmtes Mindestmaß an Sicherheit auf dem Computer zu gewährleisten, sollten **Softwareaktualisierungen** (Updates), die seitens der Softwareentwickler angeboten werden, immer zeitnah ausgeführt werden. Die verschiedenen Hersteller veröffentlichen ein solches Update, sobald sie eine potenzielle Schwachstelle im Programmcode ihrer Software entdecken. Aktualisierungen gibt es u.a. für:

- > Betriebssysteme,
- > Drucker-Software,
- > Bild- und Textverarbeitungsprogramme,
- > E-Mail-Programme,
- > Programme zur Wiedergabe von Videos.

Was ist bei Aktualisierungen zu beachten?

Softwareaktualisierungen sollten nur **direkt über die Programme** oder **per Download** auf der Webseite des Anbieters initialisiert werden. Hinter Pop-ups auf Webseiten über vermeintliche Updates eines Anbieters ist Vorsicht geboten: hinter den aufblinkenden Softwareaktualisierungen steckt häufig ein **Betrugsversuch**. Dies kann von unwissentlich und kostenpflichtig zu buchenden Abos eines bestimmten Produktes bis hin zum ungewollten Installieren von Schadsoftware reichen.

Ein genauer Blick auf die Aktualisierungsanfrage oder auch die Webseite des Anbieters ist angebracht. Vorsicht ist insbesondere geboten, wenn plötzlich **neue Berechtigungen** wie Zugriff auf die Kontaktdatenbank o.ä. verlangt werden oder auf einmal einen Zugang zum Internet gefordert werden.

Manche Softwareaktualisierungen sind sehr groß und benötigen zwischen wenigen Minuten bis zu mehreren Stunden, so dass in der Zeit der Aktualisierung nicht oder nur eingeschränkt gearbeitet werden kann. Hier bietet sich eine Mittagspause oder ein Meeting an, bei dem man eine gewisse Zeit ohne Computer auskommt. Auch ein Neustart des Gerätes kann nötig sein, so dass weitere Arbeitszeit in Anspruch genommen wird.



SICHERHEITSTIPP BEI AKTUALISIERUNGEN

- ✓ **Direkt** über die Programme oder per Download auf der Webseite des Anbieters herunterladen!
- ✓ Vorsicht bei **Pop-ups** auf Webseiten über vermeintliche Updates: Betrugsversuch! Schadsoftware!
- ✓ Bei unnötigen **Berechtigungsanfragen** misstrauisch werden!



Schwache Passwörter können durch Dictionary-Attacks leicht geknackt werden.

4. DAS SICHERE PASSWORT IM ARBEITSALLTAG: 123456?

Aus Gründen der Bequemlichkeit verwenden viele Nutzer häufig leicht einprägsame Passwörter, wie die Namen von Familienangehörigen oder Haustieren. Derartige Passwörter sind durch vollautomatisierte **Wörterbuchangriffe** (sogenannte „Dictionary-Attacks“) oder auch dem Angreifer bekannte persönliche Informationen über den Nutzer **leicht zu knacken**. In einem Unternehmen hat diese Art von Passwörtern nichts zu verloren, und entspricht in den meisten größeren Unternehmen auch nicht den internen Sicherheitsrichtlinien. Passwörter sollten bestimmte **Qualitätsanforderungen** erfüllen, insbesondere dann, wenn es sensible Daten schützen soll.



DIE WICHTIGSTEN REGELN FÜR EIN SICHERES PASSWORT

- ✓ **Keine einfachen Passwörter:** Simple Passwörter wie „Passwort“, „1234“ sollten vermieden werden.
- ✓ **Keine Namen:** Namen des Haustieres, Straßennamen, Spitznamen und ähnliches sollten nicht verwendet werden.
- ✓ **Buchstaben- und Ziffernkombinationen:** Buchstaben und Ziffern sollen in Kombination verwendet werden sowie Groß- und Kleinbuchstaben und Sonderzeichen.
- ✓ **Länger ist sicherer:** Ein Passwort mittlerer Sicherheit hat sechs bis acht Zeichen, für hohe Sicherheit müssen es zwölf sein.
- ✓ Passwörter **nicht am Rechner notieren**.
- ✓ Passwörter **nicht mehrfach benutzen**.
- ✓ Passwörter sollen **regelmäßig geändert** werden.

Das Erzeugen sicherer Passwörter über Passphrasen.

Mit der **Passphrasen-Methode** kann ein sicheres Passwort generiert werden, das alle Sicherheitsregeln erfüllt und dennoch einfach zu merken ist. Dazu überlegt man sich einen Satz, der aus Wörtern und Zahlen besteht und jeweils die Anfangsbuchstaben zu einem Passwort zusammensetzt.



BEISPIEL PASSPHRASEN

Ein sicheres Passwort steht in keinem Wörterbuch und besteht neben Buchstaben auch aus Sonderzeichen und Zahlen. Speichern soll man es auch nicht, aber wie soll man sich ein solches Zeichenchaos merken? Jens denkt sich einen Satz aus: „Jens möchte am liebsten jeden Tag zwei Mal Sport machen, denn Jens ist eine Sportskanone.“ Er kürzt den Satz, indem er nur die Anfangsbuchstaben der Worte nimmt und 'zwei Mal' in '2*' umwandelt. Sein sicheres, gut zu merkendes Passwort lautet: **JmalJT2*Sm,dJieS**.



TIPP

Mit der **Muster-Passwortkarte von DsiN** lassen sich einfach und effektiv sichere Passwörter kreieren: Von einem beliebigen Startpunkt auf dem Koordinatenfeld nimmt man einen „Weg“ in eine beliebige Richtung vor.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
1	&	\$	P	5	&	Y	V	Y	D	8	\$	t	4	D	3	n	k	@	4	&	q	W	c	@	5	\$	1
2	F	3	\$	Z	8	#	K	1	#	5	6	%	R	6	#	B	6	&	M	8	@	M	3	@	4	8	2
3	W	u	4	R	o	7	A	i	9	S	h	5	4	f	0	D	s	7	I	y	4	I	r	6	G	J	3
4	%	3	0	@	7	M	\$	1	P	#	4	U	#	6	L	\$	3	3	\$	2	C	\$	8	G	@	6	4
5	3	q	E	4	&	O	1	f	6	5	&	Y	3	u	T	6	\$	U	6	y	B	0	%	h	7	5	5
6	\$	#	G	6	#	M	z	b	Q	1	%	b	3	J	9	k	k	\$	4	&	r	A	r	&	7	&	6
7	A	2	@	C	4	&	R	5	@	7	5	@	0	6	#	L	4	#	T	6	\$	W	5	\$	3	6	7
8	T	h	4	U	d	0	P	b	3	E	w	4	2	y	0	X	p	0	L	m	9	I	o	6	W	s	8
9	@	1	5	&	7	N	\$	4	D	@	7	Z	%	6	J	&	0	1	@	7	H	\$	6	K	\$	2	9
10	5	w	N	2	@	R	5	I	3	5	#	I	4	j	T	0	#	A	7	q	H	7	\$	e	8	1	10
11	\$	\$	K	6	#	V	w	k	I	5	@	s	7	Z	6	b	f	#	9	\$	w	E	w	@	6	%	11
12	D	7	@	X	0	@	W	5	#	0	1	\$	s	6	#	M	1	#	K	3	@	H	6	%	1	7	12
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	

Regeln für den Gebrauch

1. **Einstiegspunkt wählen** (z.B. M10) 2. **Passwort bilden**, z.B. 2 Felder nach oben, 5 Felder nach links (H8) 3. **Merken** Einstieg, Verlauf und Ausstiegspunkt

<https://www.sicher-im-netz.de/dsin-muster-passwortkarte>



ANREGUNG FÜR DEN UNTERRICHT

Lassen Sie die Schüler mit Hilfe der vorgestellten Methoden ein sicheres Passwort entwickeln!

Passwort-Verwaltungsprogramme nutzen

Die meisten Menschen können sich trotz Eselsbrücken nur wenige sichere Passwörter merken. Denn Passwörter sollten aus Sicherheitsgründen **nicht mehrfach verwendet**, sondern immer nur für einen Zweck eingesetzt werden. Gelangt das Passwort in unseriöse Hände, sind dann nicht gleich mehrere Dienste und Systeme betroffen. Auch **Passwörter aufschreiben oder im Computer speichern, empfiehlt sich nicht**, da Einbrecher oder Schadsoftware solche Verstecke leicht finden. In dieser Situation können Passwort-Verwaltungsprogramme eine sichere Alternative sein.

Passwort-Verwaltungsprogramme helfen, die eigenen Passwörter sicher zu verwalten. Die Passwörter werden dabei in einer verschlüsselten Datenbank gespeichert, die man mithilfe eines Master-Passwortes absichert. So muss man sich nur ein sicheres Passwort merken.



LINKTIPP

Mehr Informationen zum Thema Passwörter finden sich in der Lehrbuchsammlung von Wikipedia „Wikibooks“:

https://de.wikibooks.org/wiki/Internet:_Sicherheit:_Passwort

Auf der Website des Informationsportals für Verbraucher „Verbraucher Sicher Online“ finden Sie weitere Hintergrundartikel und Erklärungen: <https://www.verbraucher-sicher-online.de/thema/passwoerter>



LINKTIPP

Das Onlinespiel zum Thema „Sichere Passwörter“ von Sichere Identität Berlin Brandenburg.



<http://www.sichere-identitaet-bb.de/microsites/sicheriminternet/episode1/>



LERNEINHEIT 1: GRUNDEINSTELLUNGEN FÜR EINEN SICHEREN ARBEITSPLATZ

UNTERRICHTSVERLAUF

4 Schulstunden á 45 Minuten

1. SCHULSTUNDE (ANMERKUNG: ZUSAMMENHÄNGEND MIT SCHULSTUNDE 2)

Thema	Inhalt und Methode	Arbeitsform	Material	Dauer
Vorbereitung	<ul style="list-style-type: none"> > Aufbau & ggfs. Technik-Check > Evtl. Bildung von Gruppenarbeitsstischen 			
Einstieg & Begrüßung	<ul style="list-style-type: none"> > Start mit SuS: Begrüßung und kurze Vorstellung 	Plenum		5 Min
Diskussion: IT in Unternehmen	<ul style="list-style-type: none"> > Diskussion im Plenum: Wie wird IT heutzutage in KMU genutzt? Welche Risiken gibt es hierbei? > Brainstorming mit Hilfe einer Web-Anwendung. Beispiele: https://answergarden.ch https://www.mentimeter.com > <u>Alternative:</u> Sammlung an Tafel, Whiteboard, Flipchart o.ä. 	Plenum	<ul style="list-style-type: none"> > PC, Beamer oder Smartboard > Smartphones oder Computer mit Internetzugang, Brainstorming-App, Beamer oder Smartboard > Tafel, Whiteboard oder Flipchart 	10 Min
Gruppenarbeit: Grundeinstellungen für einen sicheren Arbeitsplatz	<ul style="list-style-type: none"> > Bildung von vier Kleingruppen > Ausgabe Gruppenarbeitsbögen AB 1 > Lesen des Textes und Beantwortung der Fragen in der Gruppe > Zusammenfassung mit Hilfe einer PowerPoint Präsentation oder in Form eines Wikis Nützliche Wiki-Empfehlungen: http://www.lehrerfortbildung-bw.de/st_digital/medienwerkstatt/internet/cms/wiki/wikiengine.htm > <u>Alternative:</u> Zusammentragen der Ergebnisse auf einem Plakat, Tafel, Whiteboard o. Flipchart 	Kleingruppen	<ul style="list-style-type: none"> > Gruppenarbeitsbögen AB 1 > Computer, Beamer oder Smartboard > Tafel, Whiteboard oder Flipchart, ggfs. Eddings 	30 Min



2. SCHULSTUNDE (ANMERKUNG: ZUSAMMENHÄNGEND MIT SCHULSTUNDE 1)

Thema	Inhalt und Methode	Arbeitsform	Material	Dauer
Gruppenarbeit: Präsentation der Ergebnisse	<ul style="list-style-type: none"> > Ggfs. Finalisieren der Plakate aus Schulstunde 1 > Präsentation und Diskussion der Ergebnisse im Plenum (etwa 8 Minuten pro Gruppe) 	Kleingruppen Plenum	<ul style="list-style-type: none"> > Computer, Beamer oder Smartboard mit Präsentation bzw. Poster (aus Stunde 1) > Eddings 	40 Min
Abschluss	<ul style="list-style-type: none"> > Ggfs. offene Fragen klären > Ausblick für die nächste Stunde > Ergebnissicherung: Die Lehrkraft fotografiert Poster bzw. sichert Präsentationen. <p>Wenn nicht Schulstunde 3 durchgeführt wird: Aushängung Transfermaterialien sowie der ausgedruckten PowerPoint Folien als Handout</p>	Plenum	<ul style="list-style-type: none"> > Ggfs. Transfermaterialien (Poster, Checkliste, Arbeitsauftrag etc.) & Handouts (PowerPoint Folien LE1) 	5 Min

ALTERNATIVE SCHULSTUNDE ZU SCHULSTUNDE 1 UND 2

Thema	Inhalt und Methode	Arbeitsform	Material	Dauer
Vorbereitung	<ul style="list-style-type: none"> > Aufbau & Technik-Check > Ggfs. für QR-Code-Rallye: QR-Codes befestigen vorbereiten 		<ul style="list-style-type: none"> > Ausgedruckte und ausgeschnittene QR-Codes 	
Einstieg & Begrüßung	<ul style="list-style-type: none"> > Start mit SuS: Begrüßung und kurze Vorstellung 	Plenum		5 Min
Input: Grundeinstellungen für einen sicheren Arbeitsplatz	<ul style="list-style-type: none"> > Präsentation der PowerPoint Folien (Kap. 1 – Kap. 4) durch die Lehrkraft > Ggfs. Diskussion im Plenum 	Plenum	<ul style="list-style-type: none"> > Laptop/PC mit Beamer oder Smartboard > Speichermedium mit Präsentationsfolien LE1 	20 Min
Wissens-Check: Quiz	<ul style="list-style-type: none"> > Beantwortung des Quiz Q1 durch SuS auf Papier oder online auf der Bottom-Up Webseite unter www.dsin-berufsschulen.de > Alternativ: Bearbeiten der QR-Code-Rallye QR1 (Hinweis: diese Methode dauert etwa 10 - 15 Minuten länger, ggfs. die Diskussion kürzen) > Vergleich und Diskussion der Lösungen 	Einzel- oder Gruppenarbeit Kleingruppen Plenum	<ul style="list-style-type: none"> > Arbeitsbogen Q1 bzw. Smartphone o. Computer mit Internetzugang > ausgedruckte QR-Codes, Arbeitsbogen QR1 und Smartphones mit QR-Code-Scanner 	15 Min
Abschluss	<ul style="list-style-type: none"> > Wenn nicht Schulstunde 3 durchgeführt wird: Aushängung Transfermaterialien sowie der ausgedruckten PowerPoint Folien als Handout 	Plenum	<ul style="list-style-type: none"> > Ggfs. Transfermaterialien (Poster, Checkliste, Arbeitsauftrag etc.) & Handouts (PowerPoint Folien LE1) 	5 Min



3. SCHULSTUNDE

Thema	Inhalt und Methode	Arbeitsform	Material	Dauer
Vorbereitung	<ul style="list-style-type: none"> > Aufbau & Technik-Check > Evtl. Aufbau einer „Bühne“ für das Planspiel 			
Einstieg & Begrüßung	<ul style="list-style-type: none"> > Start mit SuS: Begrüßung und kurze Vorstellung 	Plenum		5 Min
Einstieg & Begrüßung Wiederholung	<ul style="list-style-type: none"> > Präsentation der PowerPoint Folien (Kap. 4 – Kap. 5) durch die Lehrkraft > Ggfs. Diskussion im Plenum 	Plenum	<ul style="list-style-type: none"> > Laptop oder PC > Beamer & Sound oder Smartboard > Speichermedium mit Präsentationsfolien LE1 	10 Min
Transferübung: Rollenspiel	<ul style="list-style-type: none"> > Rollenspiel Lerneinheit 1: „Passwörter geknackt“ > Umsetzung als Fotostory möglich. Hilfreiche Anleitungen finden Sie hier: http://www.bpb.de/lernen/grafstat/partizipation-vor-ort/157901/fotostory-erstellen https://www.medienpaedagogik-praxis.de/2012/11/25/fotostories-erstellen 	Plenum Gruppenarbeit	<ul style="list-style-type: none"> > Arbeitsbogen R1 > Computer mit Internetzugang oder Smartphones 	25 Min
Alternativ: Lückentext + Online-Spiel	<ul style="list-style-type: none"> > <u>Alternativ</u>: Bearbeiten des Lückentextes L1: „Computervirus in der Firma“ durch SuS auf Papier oder online auf der Bottom-Up Webseite unter www.dsin-berufsschulen.de > <u>sowie</u>: SuS spielen einzeln das Spiel „Episode 1: Soll dein Passwort sicher sein, packe viele Zeichen rein“ von sichere Identitäten Berlin-Brandenburg unter: http://www.sichere-identitaet-bb.de/microsites/sicheriminternet/episode1/ > Diskussion der Ergebnisse im Plenum 	Einzelarbeit Plenum	<ul style="list-style-type: none"> > Arbeitsbogen L1 bzw. Smartphone o. Computer mit Internetzugang > PCs mit Internetzugang 	
Abschluss: Aushändigung des Transfermaterials & Arbeitsauftrags	<ul style="list-style-type: none"> > Ggfs. offene Fragen klären > Aushändigung der ausgedruckten PowerPoint Folien als Handout > Aushändigung und kurze Erläuterung des Transfermaterials: Poster, Checkliste & Arbeitsauftrag 	Plenum	<ul style="list-style-type: none"> > Handouts (PowerPoint Folien LE 1) > Transfermaterialien (Poster, Checkliste, Arbeitsauftrag etc.) 	5 Min



ARBEITSBOGEN GRUPPENARBEIT AB 1

ARBEITSANWEISUNG FÜR DIE LEHRKRAFT

Beschreibung

Die Schüler*innen werden in vier Kleingruppen aufgeteilt. Jede Kleingruppe erhält ein Thema:

- 1. IT-Sicherheitsrisiken: Viren, Trojaner und Co.**
- 2. Abwehr von Schädlingen: Virenschutz und Firewall**
- 3. Aktualisierungen sowie Sicherheitseinstellungen bei Browser und Software**
- 4. Das sichere Passwort im Arbeitsalltag**

Nun erhält jedes Gruppenmitglied einen eigenen Arbeitsbogen (siehe folgende Seiten) entsprechend seines Themas. Die Schüler*innen beantworten in der Kleingruppe die Leitfragen mit Hilfe des Leittextes und wenn möglich/nötig des Internets. Die Fragen können auch innerhalb der Gruppe aufgeteilt, in Einzelarbeit beantwortet und anschließend in der Kleingruppe diskutiert werden.

Die Ergebnisse fasst jede Kleingruppe auf einem Plakat zusammen. Abschließend präsentieren die Gruppen in der nächsten Schulstunde ihre Ergebnisse vor der Klasse.



ARBEITSBOGEN AB1: GRUPPE 1

IT-SICHERHEITSRISIKEN: VIREN, TROJANER UND CO.



Arbeitsauftrag

1. Lesen Sie zunächst den **Leittext**.
2. Beantworten Sie die **Leitfragen** in der Gruppe. Sie können die Fragen auch innerhalb der Gruppe aufteilen. Für die Beantwortung können Sie auch weitere Quellen wie das Internet verwenden.
3. Fassen Sie die Ergebnisse übersichtlich zusammen und erstellen Sie ein aussagekräftiges und übersichtliches **Plakat**.
4. **Präsentieren** Sie Ihre Ergebnisse in der nächsten Schulstunde vor der Klasse

Leitfragen

- > Was sind Schadprogramme?
- > Wie verbreiten sich Schadprogramme?
- > Welchen Schaden können Viren, Trojaner und Co. für Unternehmen anrichten?
- > Wie kann man einen Befall durch Schadsoftware bemerken?

Leittext

Schadprogramme oder Malware (Abkürzung von engl. malicious software = Schadsoftware) sind heutzutage ein Oberbegriff für solche Programme, die sich in andere Programme oder Dateien **einschleusen**, sich selber **verbreiten** und **Schadfunktionen** ausführen. So kann Schadsoftware beispielsweise Veränderungen an Hardware, dem Betriebssystem und der Software vornehmen und erheblich die Computersicherheit gefährden. Beispiele für Schadprogramme sind Trojaner, Viren, und Würmer.

Der Begriff **Computervirus** wird umgangssprachlich häufig für Schadsoftware verwendet. Ein Computervirus ist ein Schadprogramm mit einer Infektionsfunktion, welches sich selbst in ein Wirtsprogramm (bzw. Dokumente, Skripte und Makros, oder sogar dem Bootsektor) einschleust und beim Ausführen dieses Programms (bzw. der Datei etc.) mitaufgerufen wird. Im Anschluss verbreitet sich das Virus weiter oder führt eine Schadfunktion aus bzw. beeinträchtigt das Wirtsprogramm oder das gesamte Wirtssystem. Fehlfunktionen, Datenverlust oder ganze Hard- und Softwareschäden können die Folge sein.

Ein **Computerwurm** oder einfach auch Wurm genannt, ist eine eigenständige Programmroutine, die sich auf dem Rechner oder auch Smartphone verbreitet und dort zum Teil einen erheblichen Schaden anrichtet.



Die **Aktivierung** eines Computerwurms geschieht entweder durch eine **manuelle** Ausführung des Benutzers, beispielweise über das Öffnen eines Dateianhangs. Die Aktivierung kann aber auch **automatisch** geschehen (anders als beim Computervirus), indem der Computerwurm eine Sicherheitslücke im Programm nutzt, sobald er auf dem Zielsystem eingetroffen ist. Diese Variante der Verbreitung ist häufig anzutreffen, da sie effizient ist und so sehr schnell viele Systeme infiziert werden können. Zum Beispiel kann sich ein Computerwurm in einem Anhang einer E-Mail verstecken und sich selbstständig an alle Kontakte des Adressbuches verschicken. Ist der Computerwurm im Postfach der Kontakte angelangt, wiederholt er den Vorgang. So können sich Würmer in einer rasenden Geschwindigkeit ausbreiten und ganze Netzwerke infizieren.

Die **Auswirkungen** eines Wurmbefalls können im Firmennetzwerk großen Schaden anrichten. Die Folgekosten im Unternehmen können beachtlich sein, da Zeit, Personal und Software für die Beseitigung des schädlichen Codes und zur Wiederherstellung der Daten und Funktionen zum Einsatz kommen müssen.

Bei **Trojanischen Pferden** - oder nur kurz Trojanern - handelt es sich dem Äußeren nach um vermeintlich nützvolle Software, die im Hintergrund jedoch für den Nutzer nicht sichtbare Funktionen ausführt. Sie stellen mit mehr als drei Vierteln die häufigste Art von Schadsoftware dar. Häufig dienen Würmer dazu, Trojanische Pferde auf dem Computer zu verbreiten, da Trojaner nicht in der Lage sind, sich selbsttätig zu vervielfältigen. Insbesondere im Firmennetzwerk sind Trojaner eine echte Bedrohung und als sehr gefährlich einzustufen.

Zu den **schädlichen Aktionen**, die Trojaner ausführen können, gehören unter anderem:

- > das Löschen,
- > das Sperren,
- > das Modifizieren,
- > sowie das Kopieren von Daten.
- > Beeinträchtigen der Funktionalität von Computern oder Computernetzwerken.

Trojaner haben ein breites Spektrum an Schaden, den sie anrichten können. Entsprechend groß sind die unterschiedlichen Varianten von Trojanern. Sie werden anhand der Aktivität klassifiziert, die sie auf einem Computer ausführen.

Misstrauisch sollte man werden, wenn der Computer immer langsamer wird, sich ungewöhnlich verhält und merkwürdige Meldungen gibt. Auch dass der Browser unbekannte Webseiten öffnet, Dateien einfach verschwinden, vorher laufende Funktionen nicht mehr ausgeführt werden und Abstürze häufiger werden, können Indizien für eine Trojaner-Infektion sein.



ARBEITSBOGEN AB1: GRUPPE 2

ABWEHR VON SCHADSOFTWARE: VIRENSCHUTZ UND FIREWALL



Arbeitsauftrag

1. Lesen Sie zunächst den **Leittext**.
2. Beantworten Sie die **Leitfragen** in der Gruppe. Sie können die Fragen auch innerhalb der Gruppe aufteilen. Für die Beantwortung können Sie auch weitere Quellen wie das Internet verwenden.
3. Fassen Sie die Ergebnisse übersichtlich zusammen und erstellen Sie ein aussagekräftiges und übersichtliches **Plakat**.
4. **Präsentieren** Sie Ihre Ergebnisse in der nächsten Schulstunde vor der Klasse

Leitfragen

- > Welche Arten von Virenschutzprogrammen gibt es?
- > Was ist der Unterschied zwischen einer Firewall und einem Virens Scanner?
- > Warum sind Virens Scanner und eine Firewall so wichtig?
- > Wie kann man sich noch vor Computerviren schützen?

Leittext

Ein **Antiviren-Programm**, **Virens Scanner** oder **Virenschutz-Programm** ist eine Software, die bekannte Computerviren **aufspüren**, **blockieren** und **beseitigen** soll. Hierbei steht Nutzern eine Vielzahl von Programmen unterschiedlicher Anbieter zur Verfügung. Im privaten Bereich reichen die kostenfreien Angebote der Anbieter oftmals aus. Kostenpflichtige und professionelle Angebote sollten von kleineren Unternehmen in Erwägung gezogen werden.

Es gibt **verschiedene Arten** von Virens Scannern: Echtzeitscanner (auch Zugriffsscanner genannt) und manuelle Scanner (auch Dateiscanner genannt) werden mit dem Betriebssystem ausgeliefert oder als Programme lokal installiert. Während der Echtzeitscanner permanent im Hintergrund läuft und Dateien, Programme, Arbeitsspeicher und eventuell den Datenverkehr überwacht, wird diese Überprüfung beim manuellen Scanner vom Nutzer ausgelöst (oder per Assistent zu bestimmten Zeiten ausgelöst), um eine tiefergehende Prüfung des Systems vorzunehmen.

Finden diese Scanner etwas Verdächtiges, fragen sie in der Regel den Benutzer nach dem weiteren Vorgehen. Ist der Scanner in der Lage, den Virus aus der Datei zu **entfernen** und einen Reparaturversuch vorzunehmen, erfolgt dies über die Option „Reinigung“.



Kann der Scanner den Virus nicht aus der Datei entfernen, bieten sich in der Regel zwei Optionen: Der Scanner kann die befallene Datei **löschen**, hierbei gehen jedoch die Dateiinhalte verloren. Eine Alternative bietet das **Verschieben in die Quarantäne**. Die Isolierung der Datei sorgt dafür, dass der Virus kein weiteres Unheil auf dem PC anrichten kann.

Als **Online-Virens Scanner** werden Antiviren-Programme bezeichnet, die über Webseiten oder auch Erweiterungen in Browsern verfügbar sind. Sie bieten sich vor allem für das Scannen einzelner Dateien an und sind stets auf dem neuesten Stand. Die Dateien werden dabei zur Prüfung auf den Webservice hochgeladen. Das Hochladen geschäftskritischer Dateien bietet sich in diesem Fall weniger an. Einige Anbieter von Online-Scannern bieten die Möglichkeit, an den Webservice eine URL mit der dort hinterlegte Datei, die man vor dem Herunterladen testen möchte, zu übertragen.

Virens Scanner erkennen Schadprogramme (Viren, Würmer, Trojaner etc.) auf **zwei Weisen**: Der Anbieter des Virens Scanners analysiert neue Viren, ermittelt deren Signatur und aktualisiert diese in der Datenbank, mit der sich der Virens Scanner in regelmäßigen Abständen – oder manuell ausgelöst – zum Abgleich verbindet. Aus diesem Grund ist es wichtig, dass die Datenbanken von Virens Scanner regelmäßig aktualisiert werden. Es gibt auch Virens Scanner, die u.a. aufgrund von heuristischen Methoden neuartige Schadsoftware auf dem Rechner selber erkennt.

Ein Virens Scanner durchsucht ein System intern nach Schädlingen. Eine **Firewall** schützt den PC oder das Netzwerk vor Zugriffen **von außen**, indem der durch die Firewall laufende Datenverkehr überwacht wird und Netzwerkzugriffe beschränkt bzw. unterbunden werden. Um einen bestmöglichen Schutz zu erlangen, sollte man die Computer bzw. Netzwerke mit **beiden Varianten** ausstatten, wenn regelmäßig im Internet gesurft wird. Grundsätzlich wird unterschieden zwischen einer Personal Firewall (Desktop Firewall) und einer externen Firewall (Netzwerk- oder Hardware-Firewall). Die Desktop Firewall wird als Anwendung bzw. Programm auf dem Rechner installiert. Die Software einer externen Firewall arbeitet nicht auf dem zu schützenden System selbst, sondern auf Geräten im Netzwerk.

Neben Virens Scannern und Firewall gibt es noch grundlegende **Verhaltensweisen**, mit denen man einem Schadprogrammbefall vorbeugen kann. Hierzu zählt, keine E-Mails mit **unbekannten Anhängen** zu öffnen - Dies ist immer noch einer der meist genutzten Verbreitungswege für Viren. Man sollte also auch vorsichtig sein mit **fremder Software und Dateien** von Kunden oder Geschäftspartnern! Durch Unwissenheit oder Sabotage können sich hier Viren befinden. Auch lohnt es sich, ein **Gastkonto** zu verwenden, um im Internet zu surfen. Somit kann Schadsoftware keine Administratorrechte ausnutzen, um im Hintergrund Programme zu installieren oder Systemdateien zu verändern. Auch die Nutzung sicherer **Passwörter** sollte erwähnt sein.



ARBEITSBOGEN AB1: GRUPPE 3

AKTUALISIERUNGEN SOWIE SICHERHEITSEINSTELLUNGEN BEI BROWSER UND SOFTWARE



Arbeitsauftrag

1. Lesen Sie zunächst den **Leittext**.
2. Beantworten Sie die **Leitfragen** in der Gruppe. Sie können die Fragen auch innerhalb der Gruppe aufteilen. Für die Beantwortung können Sie auch weitere Quellen wie das Internet verwenden.
3. Fassen Sie die Ergebnisse übersichtlich zusammen und erstellen Sie ein aussagekräftiges und übersichtliches **Plakat**.
4. **Präsentieren** Sie Ihre Ergebnisse in der nächsten Schulstunde vor der Klasse

Leitfragen

- > Was sind Plug-ins und welche nützlichen Plug-ins gibt es?
- > Was sind Cookies und was ist daran bedenklich?
- > Warum sind Softwareaktualisierungen wichtig?

Leittext

Mittlerweile haben alle üblichen Browser eine gute Sicherheitsausstattung und enthalten z.B. einen eingebauten Filter, der vor schädlichen Webseiten warnt. Für ein Höchstmaß an Sicherheit beim Surfen sollte mit den meisten Browsern das Ausführen von Flash, JavaScript oder Java Applets etc. auf ausgewählte, vertrauenswürdige Seiten beschränkt werden. Dies kann in den **Browser-Einstellungen** oder mit Hilfe von Software-Erweiterungen für den Browser, den sogenannten **Plug-ins** erfolgen.

Beim Besuch einer Internetseite speichert der Browser Bilder, Texte und ggfs. Videos im Cache des Browsers. Dabei ist es möglich, dass der Browser Programmcodes ausführt und so automatisch Schadsoftware wie Viren, Würmer und Trojaner auf den Rechner lädt. Viele Webseiten setzen z.B. JavaScript ein, um Funktionalität und die „User Experience“ der Seitenbesucher zu gewährleisten; allerdings werden diese Scripte auch von vielen Webseiten zur Verbreitung von Schadsoftware genutzt.

Mittlerweile sind alle gängigen Browser mit sogenannten Plug-ins ausgestattet, die dem Nutzer mehr Sicherheit während des Surfens bieten. Vor der Installation von Plug-ins sollte der Nutzer sich anhand der Bewertungen und weiteren Informationen ein Bild über die **Vertrauenswürdigkeit** des Urhebers des Plug-ins verschaffen. Zum allgemeinen Grundschutz gehören Erweiterungen wie „NoScript“ (bzw. „ScriptSafe“ etc.), mit der das Ausführen von JavaScript unterbunden wird bzw. vor dem Ausführen bestätigt werden muss. Außerdem gibt es Erweiterungen, die den Browser immer eine sichere, verschlüsselte Verbindung (SSL) zum Server aufbauen lassen, sofern der Betreiber dies anbietet.



Viele Webseitenbetreiber **„tracken“** (verfolgen) das Nutzungsverhalten eines Seitenbesuchers, um so z.B. die Seite für Besucher zu optimieren. Die Erweiterung „Ghostery“ für Firefox zeigt dem Nutzer an, wie viele „Tracker“ auf einer Webseite aktiv sind und ermöglicht dem Nutzer anzugeben, welche Tracker zugelassen werden dürfen. Zudem können **„Ad-Blocker“**, die das Einblenden von Werbung unterbinden, die Sicherheit beim Surfen erhöhen, da Werbung oftmals von Servern Dritter geladen wird, und hier oftmals Sicherungsvorkehrungen seitens des Webseitenbetreibers fehlen. Auch bei diesem Plug-in können selbstverständlich Ausnahmen hinzugefügt werden, um den Betreiber einer Seite die Werbeeinnahmen zu ermöglichen. Neben dem Browser selbst sollten auch installierte Plug-ins regelmäßig aktualisiert werden, um den erweiterten Schutz bieten zu können.

Cookies sind Textdateien und enthalten typischerweise **Daten über besuchte Webseiten**, die vom Webbrowser beim Surfen im Internet gespeichert werden. Sie können den Nutzer beim nächsten Seitenbesuch **wiedererkennen**. Mit ihnen kann auch das Surfverhalten nachverfolgt werden, aufgrund dessen stellen Cookies ein **Datenschutzrisiko** für Unternehmen dar und sollten nach jeder Online-Sitzung automatisch gelöscht werden. „Cookies von Drittanbietern“ sollten generell nicht zugelassen werden (dies lässt sich in den Browser-Einstellungen regeln). Einige Browser ermöglichen, den Web- und Werbeanbietern mitzuteilen, dass man nicht verfolgt werden möchte („do not track“). Dann liegt es allerdings bei den Betreibern der Webseite, diese Einstellung zu respektieren, weshalb sie kein Ersatz für entsprechende Plug-ins (s.o.) bildet. Die sogenannten Flash-Cookies (auch LSO-Cookies genannt) sammeln besonders viele Daten im Vergleich zu den normalen Text-Cookies. Diese Cookies speichern Daten unabhängig vom eingesetzten Browser und besitzen eine längere Verweildauer. Somit werden sie auch nicht von den Cookie-Einstellungen im Browser eingeschränkt.

Um ein bestimmtes Mindestmaß an Sicherheit auf dem Computer zu gewährleisten, sollten **Softwareaktualisierungen** (Updates), die seitens der Softwareentwickler angeboten werden, immer zeitnah ausgeführt werden. Die verschiedenen Hersteller veröffentlichen ein solches Update, sobald sie eine potenzielle Schwachstelle im Programmcode ihrer Software entdecken. Softwareaktualisierungen sollten nur direkt über die Programme oder per Download auf der Webseite des Anbieters initialisiert werden. Hinter **Pop-ups** auf Webseiten über vermeintliche Updates eines Anbieters ist Vorsicht geboten: hinter den aufblinkenden Softwareaktualisierungen steckt häufig ein Betrugsversuch. Dies kann von unwissentlich und kostenpflichtig zu buchenden Abos eines bestimmten Produktes bis hin zum ungewollten Installieren von Schadsoftware reichen.

Ein genauer Blick auf die Aktualisierungsanfrage oder auch die Webseite des Anbieters ist angebracht. **Vorsicht** ist insbesondere geboten, wenn plötzlich neue Berechtigungen wie Zugriff auf die Kontaktdatenbank o.ä. verlangt werden oder auf einmal einen Zugang zum Internet gefordert werden.



ARBEITSBOGEN AB1: GRUPPE 4

DAS SICHERE PASSWORT IM ARBEITSALLTAG: 123456?



Arbeitsauftrag

1. Lesen Sie zunächst den **Leittext**.
2. Beantworten Sie die **Leitfragen** in der Gruppe. Sie können die Fragen auch innerhalb der Gruppe aufteilen. Für die Beantwortung können Sie auch weitere Quellen wie das Internet verwenden.
3. Fassen Sie die Ergebnisse übersichtlich zusammen und erstellen Sie ein aussagekräftiges und übersichtliches **Plakat**.
4. **Präsentieren** Sie Ihre Ergebnisse in der nächsten Schulstunde vor der Klasse

Leitfragen

- > Ist es sinnvoll, durch den Internetbrowser Passwörter zu speichern?
- > Erstellen Sie eine Liste an Merkmalen für sichere Passwörter.
- > Beschreiben Sie ein Verfahren, mit welchem jeder ein sicheres Passwort erstellen kann, welches man sich gut merken kann.

Leittext

Aus Gründen der Bequemlichkeit verwenden viele Nutzer häufig **leicht einprägsame Passwörter**, wie die Namen von Familienangehörigen oder Haustieren. Derartige Passwörter sind durch vollautomatisierte Wörterbuchangriffe (sog. „Dictionary-Attacks“) oder auch dem Angreifer bekannte persönliche Informationen über den Nutzer leicht zu knacken. In einem Unternehmen hat diese Art von Passwörtern nichts zu verloren, und entspricht in den meisten größeren Unternehmen auch nicht den **internen Sicherheitsrichtlinien**. Passwörter sollten bestimmte **Qualitätsanforderungen** erfüllen, insbesondere dann, wenn es sensible Daten schützen soll.

- > **Keine einfachen Passwörter:** „Passwort“, „1234“ sollten vermieden werden.
- > **Keine Namen:** Namen des Haustieres, Straßennamen, Spitznamen und ähnliches sollten nicht verwendet werden.
- > **Buchstaben- und Ziffernkombinationen:** Buchstaben und Ziffern sollen in Kombination verwendet werden sowie Groß- und Kleinbuchstaben und Sonderzeichen
- > **Länger ist sicherer:** Ein Passwort mittlerer Sicherheit hat sechs bis acht Zeichen, für hohe Sicherheit müssen es zwölf sein.
- > Passwörter **nicht am Rechner notieren**.
- > Passwörter **nicht mehrfach benutzen**.
- > Passwörter sollen **regelmäßig geändert** werden.



Mit der **Passphrasen-Methode** kann ein sicheres Passwort generiert werden, das alle Sicherheitsregeln erfüllt und dennoch einfach zu merken ist. Dazu überlegt man sich einen Satz, der aus Wörtern und Zahlen besteht und jeweils die Anfangsbuchstaben zu einem Passwort zusammensetzt. Ein Beispiel: „Janine möchte am liebsten jeden Tag zwei Mal Sport machen, denn Janine ist eine Sportskanone.“ Man kürzt den Satz, indem man nur die Anfangsbuchstaben der Worte nimmt und 'zwei Mal' in '2*' umwandelt. Das sichere Passwort lautet: JmaljT2*Sm,dJieS.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
1	&	\$	P	5	&	Y	v	y	D	8	\$	t	4	D	3	n	k	@	4	&	q	W	c	@	5	\$	1
2	F	3	\$	Z	8	#	K	1	#	5	6	%	R	6	#	B	6	&	M	8	@	M	3	@	4	8	2
3	W	u	4	R	o	7	A	l	9	S	h	5	4	f	0	D	s	7	I	y	4	l	r	6	G	j	3
4	%	3	0	@	7	M	\$	1	P	#	4	U	#	6	L	\$	3	3	\$	2	C	\$	8	G	@	6	4
5	3	q	E	4	&	O	1	f	6	5	&	Y	3	u	T	6	\$	U	6	y	B	0	%	h	7	5	5
6	\$	#	G	6	#	M	z	b	Q	1	%	b	3	J	9	k	k	\$	4	&	r	A	r	&	7	&	6
7	A	2	@	C	4	&	R	5	@	7	5	@	0	6	#	L	4	#	T	6	\$	W	5	\$	3	6	7
8	T	h	4	U	d	0	P	b	3	E	w	4	2	y	0	X	p	0	L	m	9	I	o	6	W	s	8
9	@	1	5	&	7	N	\$	4	D	@	7	Z	%	6	J	&	0	1	@	7	H	\$	6	K	\$	2	9
10	5	w	N	2	@	R	5	l	3	5	#	I	4	j	T	0	#	A	7	q	H	7	\$	e	8	1	10
11	\$	\$	K	6	#	V	w	k	l	5	@	s	7	Z	6	b	f	#	9	\$	w	E	w	@	6	%	11
12	D	7	@	X	0	@	W	5	#	0	1	\$	s	6	#	M	1	#	K	3	@	H	6	%	1	7	12
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	

Regeln für den Gebrauch

1. Einstiegspunkt wählen (z.B. M10) **2. Passwort bilden**, z.B. 2 Felder nach oben, 5 Felder nach links (H8) **3. Merken** Einstieg, Verlauf und Ausstiegspunkt

Mit der **Muster-Passwortkarte von DsiN** lassen sich einfach und effektiv sichere Passwörter kreieren: Von einem beliebigen Startpunkt auf dem Koordinatenfeld nimmt man einen „Weg“ in eine beliebige Richtung vor (und merkt sich gegebenenfalls nur die Zahl sowie den Buchstaben am Rand)

Beispiel: 2C = 2F3\$PC

Die meisten Menschen können sich trotz Eselsbrücken nur wenige sichere Passwörter merken. Denn Passwörter sollten aus Sicherheitsgründen nicht mehrfach verwendet, sondern immer nur für einen Zweck eingesetzt werden. Gelangt das Passwort in unseriöse Hände, sind dann nicht gleich mehrere Dienste und Systeme betroffen. Auch Passwörter aufschreiben oder im Computer speichern, empfiehlt sich nicht, da Einbrecher oder Schadsoftware solche Verstecke leicht finden. In dieser Situation können **Passwort-Verwaltungsprogramme** eine sichere Alternative sein.

Passwort-Verwaltungsprogramme helfen, die eigenen Passwörter **sicher zu verwalten**. Die Passwörter werden dabei in einer verschlüsselten Datenbank gespeichert, die man mithilfe eines Master-Passwortes absichert. So muss man sich nur ein sicheres Passwort merken.

„Passwörter sind wie Schleifpapier. Sie müssen regelmäßig gewechselt werden.“





ARBEITSBOGEN LÜCKENTEXT L1

LÖSUNG FÜR DIE LEHRKRAFT

Arbeitsauftrag

Bei der im Folgenden dargestellten Situation sollen nach der Erarbeitung der Inhalte im vorangegangenen theoretischen Teil seitens der Schüler*innen die Lücken im Text entsprechend gefüllt werden.

Ziel

Die sich aus dem unten beschriebenen Szenario ergebende Situation soll den Schüler*innen verdeutlichen, welche Gefahr von Schadprogrammen ausgeht und welche Sicherheitsvorkehrungen sinnvoll sind. Dieser Arbeitsbogen stellt auch eine schriftliche Alternative zum Rollenspiel dar, falls hierfür keine Zeit oder Kapazitäten vorhanden sein sollten.

Lösung

Der Geschäftsführer Karl Löschner ist entsetzt über den Angriff und spricht mit seinen Mitarbeiter*innen: „Wie konnte so etwas passieren?“. Die Mitarbeiterin Simone Fürst hat sich bereits vor dem Gespräch informiert, wie es zu einem Schadprogrammbefall kommen kann und was bei dem Thema Virenschutz zu beachten ist. Sie erklärt in der Runde: „Wir haben uns sicher einen **Wurm oder Trojaner** eingefangen. Diese Schadprogramme **löschen** mitunter Daten auf dem befallenen Rechner. Man kann sich unbewusst Schadsoftware durch das Aufsuchen einer Webseite auf den Rechner laden. Außerdem kann das Klicken auf einen unbekannten **Link** sowie der **Download** von verseuchten Dateien, vor allem von nicht vertrauenswürdigen Quellen, zum unbemerkten Herunterladen von Viren führen. Wichtig ist, dass wir alle Dateien auf den Rechnern nun durch einen **Virenscanner** prüfen lassen und eine **Firewall** einrichten, damit so etwas nicht noch einmal passiert.“ Auszubildender Nils Böhme ergänzt: „Wir müssen unbedingt darauf achten, keine **Anhänge** von unbekannten E-Mails zu öffnen!“ Simone pflichtet ihm bei: „Richtig. Außerdem bieten sichere **Passwörter**, die **Groß- und Kleinbuchstaben sowie Ziffern** enthalten und regelmäßig geändert werden, einen wichtigen Schutz.“ „Ich prüfe außerdem, ob es neue **Softwareaktualisierungen** und nützliche **Plug-ins** gibt, die wir installieren sollten.“, schlägt Nils vor.



LÜCKENTEXT L1 „COMPUTERVIRUS IN DER FIRMA!“

ARBEITSBOGEN FÜR DIE SCHÜLER*INNEN



Das Szenario

Böses Erwachen am Montagmorgen in der Glaserei „Durchblick“: Die firmeneigenen Computer wurden von einem Computervirus befallen. Viele Ordner mit vertraulichen Kontaktdaten von laufenden Aufträgen wurden gelöscht.



Lückentext

Der Geschäftsführer Karl Löschner ist entsetzt über den Angriff und spricht mit seinen Mitarbeiter*innen: „Wie konnte so etwas passieren?“. Die Mitarbeiterin Simone Fürst hat sich bereits vor dem Gespräch informiert, wie es zu einem Schadprogrammbefall kommen kann und was bei dem Thema Virenschutz zu beachten ist. Sie erklärt in der Runde: „Wir haben uns sicher einen _____ eingefangen. Diese Schadprogramme _____ mitunter Daten auf dem befallenen Rechner. Man kann sich unbewusst Schadsoftware durch das Aufsuchen einer Webseite auf den Rechner laden. Außerdem kann das Klicken auf einen unbekannten _____ sowie der _____ von verseuchten Dateien, vor allem von nicht vertrauenswürdigen Quellen, zum unbemerkten Herunterladen von Viren führen. Wichtig ist, dass wir alle Dateien auf den Rechnern nun durch einen _____ prüfen lassen und eine _____ einrichten, damit so etwas nicht noch einmal passiert.“ Auszubildender Nils Böhme ergänzt: „Wir müssen unbedingt darauf achten, keine _____ von unbekannten E-Mails zu öffnen!“ Simone pflichtet ihm bei: „Richtig. Außerdem bieten sichere _____, die _____ enthalten und regelmäßig geändert werden, einen wichtigen Schutz.“ „Ich prüfe außerdem, ob es neue _____ und nützliche _____ gibt, die wir installieren sollten.“, schlägt Nils vor.



Fehlende Wörter:

Download, Groß- und Kleinbuchstaben sowie Ziffern, Link, Plug-ins, Anhänge, Softwareaktualisierungen, Wurm oder Trojaner, Passwörter, Virens Scanner, löschen, Firewall



ARBEITSBOGEN: QUIZ Q1

(Mehrfachnennung möglich)

1. **Warum ist ein Virenschutzprogramm für Internetnutzer zu empfehlen?**
 - A Um die Auflagen des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu erfüllen.
 - B Weil das Internet ohne Virenschutzprogramm viel zu langsam wäre.
 - C Um vor dem Zugriff von Schadprogrammen besser geschützt zu sein und selbst nicht ungewollt Viren zu verbreiten.
2. **Über welche Wege können sich Computerviren oder Schadsoftware verbreiten?**
 - A Webseiten
 - B USB-Sticks
 - C E-Mails
3. **Was ist bedenklich an dem Ausführen von sogenannten Skripten (kleine Programme) wie JavaScript, um multimediale Inhalte auf einer Webseite anzuzeigen?**
 - A Skripte sammeln Daten über das Nutzerverhalten und spähen den Nutzer aus.
 - B Angreifer können über häufig bestehende Sicherheitslücken in Skripten Schadsoftware auf den Rechner des Nutzers laden.
 - C Der Virens Scanner muss deaktiviert werden, damit diese Skripte korrekt ausgeführt werden.
4. **Welches der folgenden Passwörter ist am sichersten?**
 - A SabineMueller123
 - B Schatzi1991
 - C 4oqr5asRT#%?a
5. **Warum sind Softwareaktualisierungen wichtig?**
 - A Um durch den Hersteller erkannte Sicherheitslücken, die von Angreifern ausgenutzt werden können, sofort zu schließen.
 - B Um neue Funktionen der Software nutzen zu können.
 - C Weil sonst die Passwörter für bestimmte Programme nicht mehr funktionieren.
6. **Was sind Plug-ins?**
 - A Plug-ins sind Computerviren, die sich in Programmen einnisten.
 - B Erweiterungen, die unter anderem den Browser mit zusätzlichen Sicherheitsfunktionen ausstatten können.
 - C Private Nachrichten, die man sich in sozialen Netzwerken oder Chaträumen senden kann.
7. **Was sind Cookies?**
 - A Hierbei handelt es sich um eine sehr gefährliche Art eines Computerwurms.
 - B Das sind wichtige Updates, die der Internetbrowser automatisch installiert.
 - C Textdateien, in denen Daten über den Besuch von Webseiten gespeichert werden.

Lösung: 1 C, 2 A+B+C, 3 B, 4 C, 5 A, 6 B, 7 C



QR-CODE-RALLYE QR1

ARBEITSANWEISUNG FÜR DIE LEHRKRAFT



Beschreibung

1. Die QR-Codes ausdrucken, an der gestrichelten Linie ausschneiden und einzeln an verschiedenen Stellen im Klassenraum oder anderen Räumen anbringen.
2. Die Schüler*innen erhalten den Fragebogen, den sie mit Hilfe der QR-Codes beantworten können. Hinter jedem Code verbirgt sich eine richtige Antwort, die auf dem Display angezeigt wird, wenn der Code mit einer QR-Code-Scanner-App eingescannt wird (diese muss ggfs. installiert werden, bitte beachten Sie die Hinweise dazu aus Lerneinheit 4: insb. Zugriffsrechte prüfen!).
3. Die Schüler*innen schreiben die richtige Antwort unter die passende Frage auf ihrem Arbeitsblatt. Den Buchstaben des QR-Codes setzen sie in das Kästchen der entsprechenden Frage. So erhalten sie am Ende ein Lösungswort.





E



K



C



QR-CODE-RALLYE QR1

LÖSUNG FÜR DIE LEHRKRAFT

1. Warum ist ein Virenschutzprogramm für Internet-Nutzer zu empfehlen?

Um vor dem Zugriff von Schadsoftware besser geschützt zu sein und selbst nicht ungewollt Viren zu verbreiten.

C

2. Über welche Wege können sich Computerviren oder Schadsoftware verbreiten?

Zum Beispiel über Webseiten, USB-Sticks u. E-Mails.

O

3. Was ist bedenklich an dem Ausführen von sogenannten Skripten wie JavaScript, um multimediale Inhalte auf einer Webseite anzuzeigen?

Angreifer können über häufig bestehende Sicherheitslücken in Skripten Schadsoftware auf den Rechner des Nutzers laden.

O

4. Welches Passwort ist sehr sicher?

4oqr5asRT#%?a

K

5. Warum sind Softwareaktualisierungen wichtig?

Um durch den Hersteller erkannte Sicherheitslücken, die von Angreifern ausgenutzt werden können, sofort zu schließen.

I

6. Was sind Plug-ins?

Erweiterungen, die unter anderem den Browser mit zusätzlichen Sicherheitsfunktionen ausstatten können.

E

7. Was sind Cookies?

Textdateien, in denen Daten über den Besuch von Webseiten gespeichert werden.

S



QR-CODE-RALLYE QR1

ARBEITSBOGEN FÜR DIE SCHÜLER*INNEN



Arbeitsauftrag

1. Installieren Sie auf Ihrem Smartphone einen QR-Code-Scanner. Wichtig: prüfen Sie zuvor die Zugriffsrechte und Vorsicht bei Drittanbieter-Stores!
2. Hinter jedem der im Raum verteilten Codes verbirgt sich eine richtige Antwort, die auf dem Display angezeigt wird, wenn der Code mit einer QR-Code-Scanner-App eingescannt wird. Finden Sie für jede der folgenden Frage die passende Antwort und notieren Sie diese.
3. Den Buchstaben des QR-Codes setzen Sie in das Kästchen der entsprechenden Frage. In abfallender Reihenfolge ergeben alle Buchstaben das richtige Lösungswort.

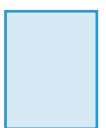
- 1. Warum ist ein Virenschutzprogramm für Internet-Nutzer zu empfehlen?**



- 2. Über welche Wege können sich Computerviren oder Schadsoftware verbreiten?**



- 3. Was ist bedenklich an dem Ausführen von sogenannten Skripten wie JavaScript, um multimediale Inhalte auf einer Webseite anzuzeigen?**





4. Welches Passwort ist sehr sicher?

5. Warum sind Softwareaktualisierungen wichtig?

6. Was sind Plug-ins?

7. Was sind Cookies?

*„Ein guter Handwerker
verleiht weder Werkzeug
noch Passwort!“*





ROLLENSPIEL R1

ARBEITSANWEISUNG FÜR DIE LEHRKRAFT

Nach der Beschäftigung mit den theoretischen Inhalten soll nun eine konkrete, sicherheitskritische Situation in Form eines Planspiels bearbeitet werden. Die sich aus den unterschiedlichen Rollen und damit verbundenen verschiedenen Standpunkten ergebene Diskussion soll den Schüler*innen verdeutlichen, welche **Grundeinstellungen für einen sicheren Arbeitsplatz** wesentlich sind. Dabei kommt der Darstellung der Transfersituation des Wissens in das Unternehmen eine besondere Rolle zu, d.h. die Schüler*innen simulieren im Rahmen des Planspiels auch die Übertragung des vermittelten Wissens in das Unternehmen.

Das Planspiel ist in drei Schritte unterteilt: Briefingphase – Spielphase – Auswertungsphase.

1. BRIEFINGPHASE

Das Ziel ist es, zu einer gemeinsamen Lösung des Sicherheitsproblems durch die Entwicklung von Handlungsschritten zu kommen. Dabei werden auch Empfehlungen zum zukünftigen Schutz vor dieser Sicherheitsproblematik erarbeitet.

Ausgangslage des Spiels: Das Szenario „Passwörter geknackt“

Großes Durcheinander am Montagmorgen: Beim Groß- und Außenhandelsunternehmen „Ex und Hopp“ wurden die firmeneigenen Computer von Hackern angegriffen. Vertrauliche Daten des Unternehmens sowie Adresskarteien wurden ausspioniert. Die Kriminellen haben Passwörter der Mitarbeiter*innen geknackt. Alle Kolleg*innen haben sich unverzüglich im Büro des Geschäftsführers Holger Frei einzufinden, um das Problem gemeinsam zu lösen.

Die unterschiedlichen Rollen: Die Interaktion

Auf dieser Grundlage spielt jede*r Schüler*in einen der folgenden Charaktere. In dieser zugewiesenen Rolle versuchen die Schüler*innen, ihre beschriebenen Standpunkte einzunehmen und zu vertreten. Dabei können auch Gruppen gebildet werden.

- > Der Geschäftsführer Holger Frei (53) ist entsetzt über den Angriff und möchte sich für die Zukunft absichern.
- > Der arglose Mitarbeiter Otto Schwarz (32) hat sich extra ein einfaches Passwort ausgesucht, weil er sich schwierige Passwörter nicht merken kann. Er kann sich nicht vorstellen, dass ein Hackerangriff schwerwiegende Folgen haben kann.
- > Die übermotivierte Mitarbeiterin Hina Wang (29) hat alles kommen sehen und hatte schon zuvor das Thema Passwort-Sicherheit beim Chef angesprochen.
- > Der überkorrekte Mitarbeiter Kai Fuchs (24) notiert sich seine komplexen Passwörter per Post-it am Bildschirm und glaubt, alles richtig gemacht zu haben.
- > Der Auszubildende Nico Koslow (22) hat ein paar Vermutungen, wie die Hacker an die Passwörter gekommen sein können und hat ein paar nützliche Tipps.



2. SPIELPHASE

Hinweise an die Spieler

- > Freie und spontane Interaktion
- > An die vorgegebenen Rollen und Vorgaben halten
- > Realistisch bleiben

Hinweise an die Beobachter

- > Keine Einmischung von außen
- > Führen eines Beobachtungsbogens für die spätere Auswertung ist hilfreich

Requisiten

- > Rollenunterstützung durch Requisiten, z.B. Kittel für die Arbeiter, Krawatte für Vorgesetzten, Pinsel für den Maler, Schere für die Friseurin
- > Trennung von Beobachter und Spielszene, z.B. in einer Ecke im Klassenraum wird das Rollenspiel gespielt.

Leitfragen, die es im Rollenspiel zu klären gilt

1. Warum konnten die Hacker vertrauliche Daten ausspionieren?
2. Welche Fehler können bei der Passwort-Vergabe gemacht werden?
3. Wie sieht ein sicheres Passwort überhaupt aus?
4. Welche Vorkehrungen sind zukünftig zu treffen?

Regeln

Die Lehrkraft fungiert als Spielleitung und greift in die Handlung ein, sobald diese in eine Richtung abgelenkt, die themen- und sicherheitsmäßig nicht relevant ist. Die Spielleitung sorgt für einen störungsfreien Ablauf und besitzt die Funktion bei Konflikten zwischen Personen einzugreifen. Während der gesamten Rollenspielphase sorgt die Spielleitung dafür, dass die Rollen von den Schüler*innen ernstgenommen werden.

3. AUSWERTUNGSPHASE

Im Anschluss an das Planspiel erfolgt eine gemeinsame Spielanalyse mit einer Bewertung des Szenarios und einer Kritik an den Lösungsschritten.

Bei der Auswertung werden in der Regel vier Phasen unterschieden:

1. Intuitive Spielanalyse (Was ist passiert? Was haben die Spieler*innen empfunden?)
2. Spielreflexion und Distanzierung (Wie lässt sich der Spielverlauf erklären?
Wie bewerten die Gruppen das Spielergebnis? Was hat das Ergebnis beeinflusst?)
3. Transfer (Welche Aspekte des Szenarios und des Spielverlaufs waren realistisch, welche nicht? Welche Relevanz hat das Ergebnis des Planspiels für unseren Blick auf die Realität?)
4. Spielkritik (Was haben wir gelernt? Was nicht? Was nehme ich persönlich mit?
Wie könnte man das Spiel verbessern?)



ARBEITSAUFGABE LE1: GRUNDEINSTELLUNGEN FÜR EINEN SICHEREN ARBEITSPLATZ

ARBEITSANWEISUNG FÜR DIE LEHRKRAFT



Ziel

Die Arbeitsaufträge und die bereitgestellten Transfermaterialien unterstützen die Schüler*innen, das erworbene Wissen zum Thema IT-Sicherheit in die Ausbildungsbetriebe zu tragen. Sie fördern damit die praktische Anwendung des im Unterricht gelernten Sicherheitswissens.

Mit Hilfe der folgenden Schritt-für-Schritt-Anleitung können die Schüler*innen die vermittelten Inhalte der Lerneinheit 1 „Grundeinstellungen für einen sicheren Arbeitsplatz“ dialogorientiert und interaktiv mit Vorgesetzten und Kolleg*innen thematisieren.

Beschreibung

Teilen Sie den Arbeitsauftrag zur LE1 *Grundeinstellungen für einen sicheren Arbeitsplatz* sowie das Anschreiben für den Ausbildungsbetrieb an die Schüler*innen aus. Zur Erfüllung des Arbeitsauftrags benötigen die Schüler*innen zudem folgende Transfermaterialien:

- Quiz aus LE1 (Entweder in Printform austeilen oder per digitalem Zugriff über die Bottom-Up Webseite unter <http://t1p.de/4ppb>)
- Checkliste zu LE1
- Muster-Passwortkarte von DsiN

Hinweis

Die Schüler*innen sollten selbst entscheiden, ob sie die einzelnen Arbeitsaufträge gestaffelt nach jeder Lerneinheit im Betrieb durchführen, oder ob sie am Ende der letzten Unterrichtseinheit einen größeren Arbeitsauftrag mit allen Lerneinheiten durchführen.

Die Festlegung eines Durchführungstermins für die Arbeitsaufträge wird empfohlen. Die Ausgabe der Teilnahmebescheinigung ist im besten Fall an die erfolgreiche Ausführung des Arbeitsauftrags gekoppelt.



ARBEITSAUFTRAG LE1: GRUNDEINSTELLUNGEN FÜR EINEN SICHEREN ARBEITSPLATZ

ARBEITSBOGEN FÜR DIE SCHÜLER*INNEN



Zuvor

- > Geben Sie Ihrer bzw. Ihrem **Vorgesetzten** das beigefügte Anschreiben.
- > Bitten Sie, diesen Arbeitsauftrag mit dem Vorgesetzten durchzuführen. Alternativ ist auch die Umsetzung mit Kollegen möglich.
- > Das gesamte Vorhaben dauert ca. 20 – 30 Minuten.

Durchführung

1. Erklären Sie Ihrem Vorgesetzten/Ihren Kollegen kurz Ihr Vorhaben.
2. Führen Sie das **Online-Quiz 1** „Grundeinstellungen für einen sicheren Arbeitsplatz“ durch (Das Quiz ist auf der Bottom-Up Webseite unter <http://t1p.de/4ppb> verfügbar. Alternativ erhalten Sie den Arbeitsbogen in Printform von Ihrer Lehrkraft).
3. Diskutieren Sie mit den Teilnehmenden über die richtigen Lösungen.
4. Stellen Sie die **Checkliste 1** „Der sichere Arbeitsplatz“ vor und geben Sie jeweils ein Exemplar an die Teilnehmenden weiter. Gehen Sie danach gemeinsam die Checkliste durch und überprüfen Sie die aufgelisteten Punkte (Die Checkliste erhalten Sie von Ihrer Lehrkraft).
5. Stellen Sie die **Muster-Passwortkarte** von DsiN vor und zeigen Sie wie Sie mit Hilfe dieser Methode ein sicheres Passwort entwickeln können.
6. Führen Sie gemeinsam mit ihrem Vorgesetzten/Ihren Kollegen eins der **Online-Spiele** zum Thema „Allgemeine IT-Sicherheit“ und „Sichere Passwörter“ von Sichere Identität Berlin Brandenburg durch (Die Spiele sind verfügbar unter <http://www.sichere-identitaet-bb.de/sicheriminternet/>).

Deutschland sicher im Netz e.V. | Albrechtstraße 10b | 10117 Berlin

Anschreiben IT-Sicherheit im Ausbildungsbetrieb

Berlin, August 2017

Sehr geehrte Damen und Herren,

Ihr Auszubildender / Ihre Auszubildende nimmt an einer Schulung zu IT-Sicherheit und Datenschutz teil. Für den erfolgreichen Abschluss der Schulung ist die Ausführung eines Arbeitsauftrags nötig, mit dem das neu Erlernte in der Praxis angewandt wird. Wir bitten Sie daher kurz um Ihre Unterstützung und Mithilfe.

Der Schutz der IT und Daten spielt eine immer wichtigere Rolle für Unternehmen und Betriebe. Schon kleine Beeinträchtigungen in der Verfügbarkeit von Systemen, Endgeräten oder Daten können heutzutage unangenehme Folgen mit sich bringen. Der Faktor Mitarbeiter spielt hierbei eine tragende Rolle: Unsachgemäße Handhabung, Nachlässigkeit und sehr häufig ein fehlendes Sicherheitsbewusstsein sind hier Risikoquellen.

Nur regelmäßige Mitarbeiterschulungen können Abhilfe schaffen. Hier setzt das Lehrangebot *Bottom-Up* jetzt bereits in der Berufsschule an: Auszubildende werden anhand praxisnaher Lehrmaterialien auf die Herausforderungen der Digitalisierung im Arbeitsalltag vorbereitet.

Die Durchführung des Arbeitsauftrags nimmt zehn bis fünfzehn Minuten in Anspruch. Wir würden uns freuen, wenn Sie Ihren Auszubildenden / Ihre Auszubildende unterstützen – auch für mehr IT-Sicherheit in Ihrem Ausbildungsbetrieb! Mehr Informationen zum Projekt finden Sie unter www.dsin-berufsschulen.de.

Mit freundlichen Grüßen

Sascha Wilms
Projektleiter

Über Deutschland sicher im Netz e.V.

Produktneutral und herstellerübergreifend leistet DsiN als zentraler Ansprechpartner für Verbraucher*innen und mittelständische Unternehmen konkrete Hilfestellungen für mehr Sicherheitsbewusstsein im Netz. Informieren Sie sich über alle Angebote von DsiN unter: www.sicher-im-netz.de

Initiative „IT-Sicherheit in der Wirtschaft“

Die Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie will vor allem kleine und mittelständische Unternehmen beim sicheren Einsatz von IKT-Systemen unterstützen. Gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung soll eine Grundlage dafür geschaffen werden, um die Bewusstseinsbildung in der digitalen Wirtschaft beim Thema IT-Sicherheit im Mittelstand zu stärken. Unternehmen sollen durch konkrete Unterstützungsmaßnahmen dazu befähigt werden, ihre IT-Sicherheit zu verbessern. Weitere Informationen zur Initiative und ihren Angeboten sind unter: www.it-sicherheit-in-der-wirtschaft.de

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Im Rahmen der Initiative:



Ein Projekt von:





BOTTOM-UP: BERUFSSCHÜLER FÜR IT-SICHERHEIT

hat zum Ziel, die Mitarbeiter von morgen bereits während der dualen Ausbildung auf die Herausforderungen des digitalen Arbeitsalltags im Hinblick auf IT-Sicherheit und Schutz von Daten vorzubereiten. Damit leistet Bottom-Up einen wichtigen Beitrag zu mehr IT-Sicherheit in kleinen und mittleren Unternehmen.

www.dsin-berufsschulen.de

Bottom-Up ist ein Angebot von

Deutschland sicher im Netz e.V.
Albrechtstraße 10
10117 Berlin

www.sicher-im-netz.de

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Im Rahmen der Initiative:



Ein Projekt von:



Initiative „IT-Sicherheit in der Wirtschaft“ Die Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie will vor allem kleine und mittlere Unternehmen beim sicheren Einsatz von IKT-Systemen unterstützen. Gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung soll eine Grundlage dafür geschaffen werden, um die Bewusstseinsbildung in der digitalen Wirtschaft beim Thema IT-Sicherheit im Mittelstand zu stärken. Unternehmen sollen durch konkrete Unterstützungsmaßnahmen dazu befähigt werden, ihre IT-Sicherheit zu verbessern. Weitere Informationen zur Initiative und ihren Angeboten sind unter: www.it-sicherheit-in-der-wirtschaft.de abrufbar.