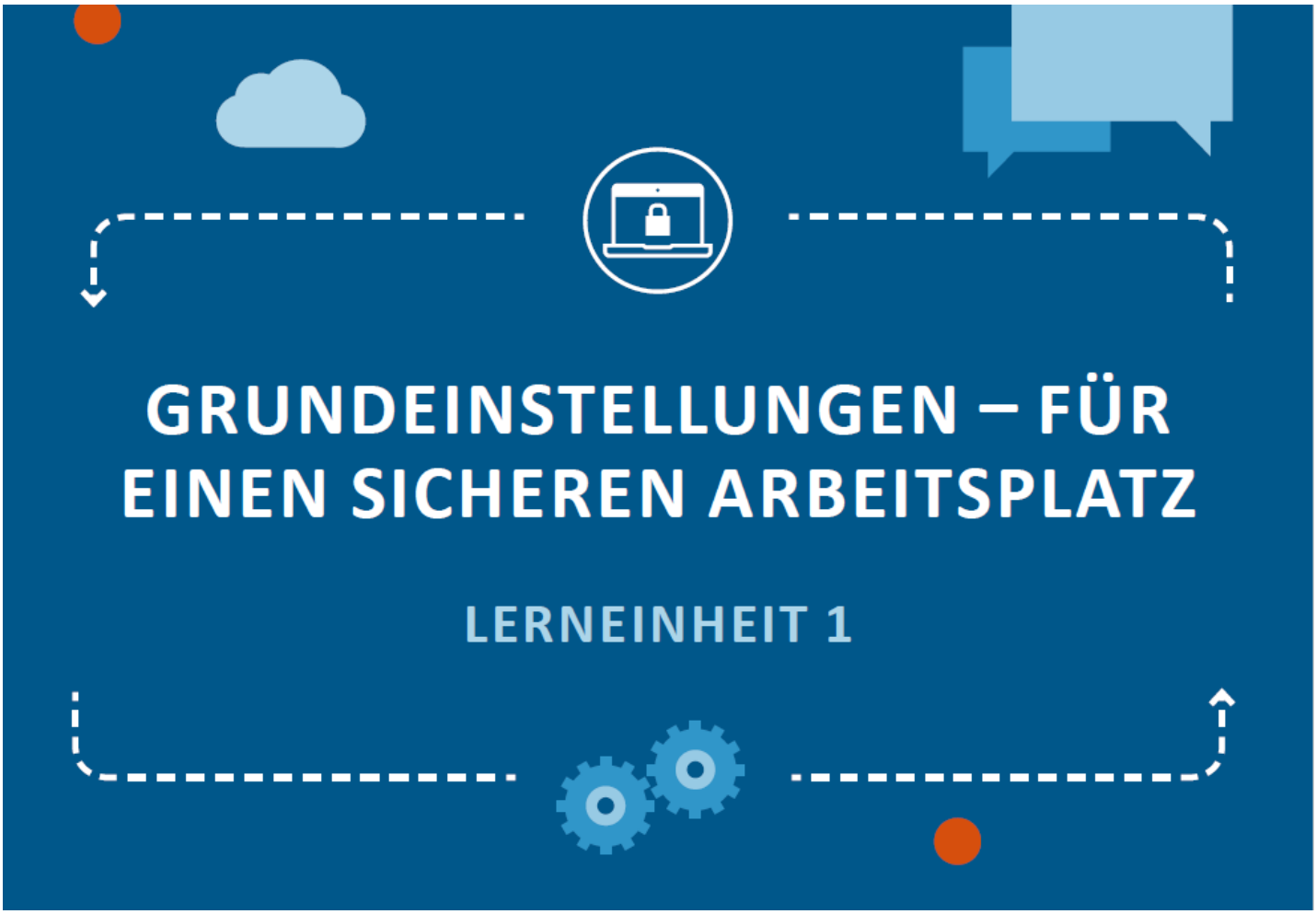
SCHÜLERMAPPE

SELBSTLERNEINHEIT



Berufsschüler BOTTOM-UP! für IT-Sicherheit

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:

*Obwohl aus Gründen der Lesbarkeit im Text die männliche Form gewählt wurde, beziehen sich die Angaben auf Angehörige aller Geschlechter.

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

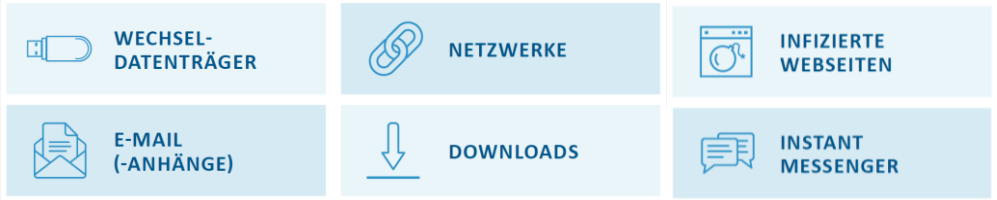
Malware vom engl. malicious Software = Schadsoftware.

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 (sogenannter **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.

ANREGUNG

Überlegen Sie: Welche Schadprogramme kennen Sie?
Waren sie selbst bereits schon betroffen?

LINKTIPP

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

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.

Schadsoftware wird häufig durch Anhänge übertragen.

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

Überlegen Sie: 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.

ANREGUNG

Überlegen Sie: 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.

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**).

(D)DoS-Attacken stehen für (Distributed) Denial of Service Angriffe: dabei wird von einer Vielzahl von infizierten Botrechnern z.B. eine Website gleichzeitig aufgerufen, so dass der Webserver unter der Last zusammenbricht. Die Website ist dadurch dann nicht mehr aufrufbar für andere Nutzer.

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, Virenscanner 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-Virenscanner

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.

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

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.

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

Die Leistung von Virenschutzprogrammen

Virenscanner erkennen **Schadprogramme** (Viren, Würmer, Trojaner etc.) auf zwei Weisen: Der Anbieter des Virenscanners analysiert neue Viren, ermittelt deren Signatur und aktualisiert diese in der Datenbank, mit der sich der Virenscanner in regelmäßigen Abständen – oder manuell ausgelöst – zum Abgleich verbindet. Aus diesem Grund ist es wichtig, dass die Datenbanken von Virenscanner regelmäßig aktualisiert werden. Es gibt auch Virenscanner, 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.

Firewall: Beschränkt Netzwerkzugriff und überwacht den Datenverkehr.

Die Firewall: Der Türsteher des Netzwerks

Ein **Virenscanner** 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

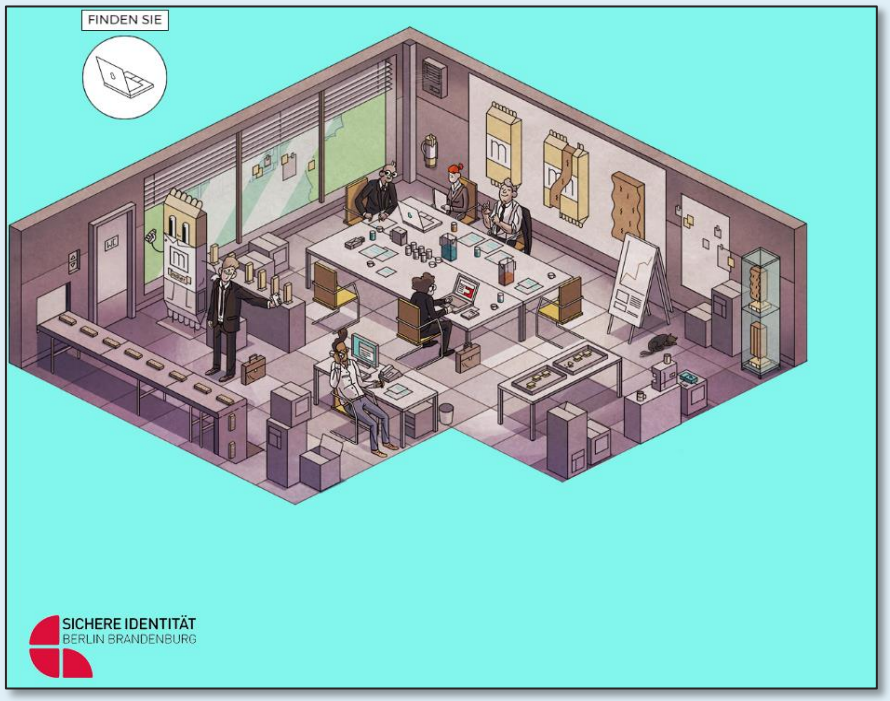
> nur präventiv schützen

> 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.

Nützliche Plug-ins und Filter

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

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"-Häckchen 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 Werbeblocker 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 Datenschutzrisiko 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!

4. DAS SICHERE PASSWORT IM ARBEITSALLTAG: 123456?

Schwache Passwörter können durch Dictionary-Attacken leicht geknackt werden.

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.

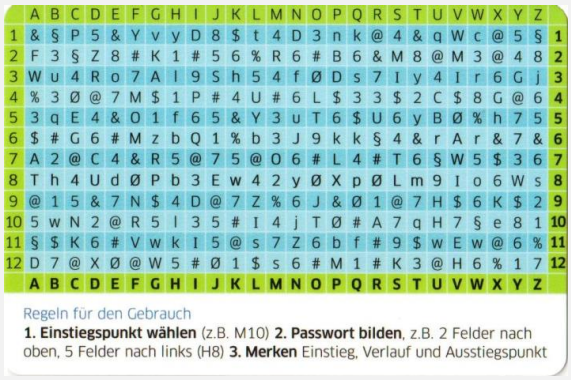
Mit der **Passphrasen-Methode** kann ein sicheres Passwort generiert werden, das alle Sicherheitsregeln erfüllt und dennoch einfach zu merken ist. Dazu überlegt man sich einen Satz, der aus Wörtern und Zahlen besteht und jeweils die Anfangsbuchstaben zu einem Passwort zusammensetzt.

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.



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

ANREGUNG

Entwickeln Sie mit Hilfe der vorgestellten Methoden ein sicheres Passwort!

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.

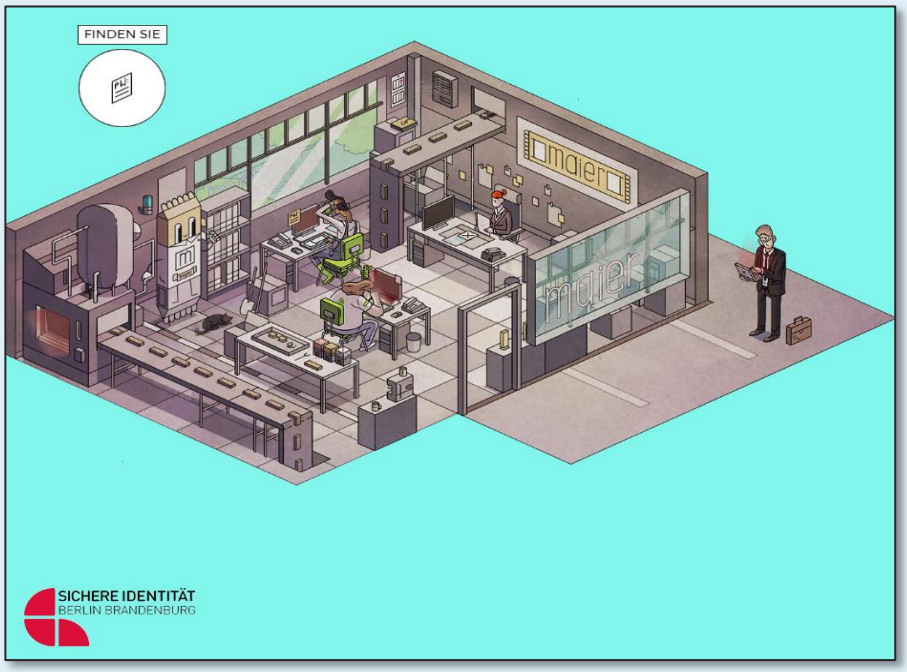
LINKTIPP

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/

LÜCKENTEXT L1 „COMPUTERVIRUS IN DER FIRMA!“

ARBEITSBOGEN

Den folgenden Lückentext können Sie alternativ auch in Form eines Online-Spiels direkt auf ihrem Computer ausfüllen.

Der Online-Lückentext ist verfügbar auf der Bottom-Up-Webseite unter: https://www.dsin-berufsschulen.de/unsere-online-lueckentexte.

Arbeitsauftrag

Füllen Sie auf Basis der Inhalte im vorangegangenen theoretischen Teil entsprechend die Lücken des folgenden Textes.

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, Virenscanner, löschen, Firewall

LÜCKENTEXT L1 „COMPUTERVIRUS IN DER FIRMA!“

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.

QUIZ Q1

(Mehrfachnennung möglich)

Sie können das folgende Quiz alternativ auch in Form eines Online-Spiels direkt auf ihrem Smartphone oder Computer durchführen.

Das Online-Quiz ist verfügbar auf der Bottom-Up-Webseite: https://www.dsin-berufsschulen.de/unsere-online-quiz.

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 Virenscanner 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 Sicherheits-funktionen 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

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:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Im Rahmen der Initiative:
IT-Sicherheit IN DER WIRTSCHAFT

Ein Projekt von:
DsiN Deutschland sicher im Netz

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.