Security Lektion 1
Grundlagen zu Daten und Sicherheit

Sicherheitsbewusstsein
- ✕ Datenbedrohung
- ✕ Wert von Informationen
- ✕ Persönliche Sicherheit

✓ Wie schützen Sie Ihre Sicherheit im Netz? Neben Schadensprogrammen lauern Skimming, Identitäts- und Datendiebstahl und dergleichen mehr. In dieser Lektion arbeiten Sie an Ihrem Sicherheitsbewusstsein und machen sich Gedanken über den Wert von Informationen.

Aufgabe

Wo finden Sie das Quiz?
Öffnen Sie **www.computertraining4you.eu**. Sie finden jede Lektion für IT Security auch im Internet. Am Ende des Moduls finden Sie ein Quiz mit einer Auswahl von 36 Fragen, die bei jedem Aufruf neu gemischt werden.

1. Sicherheitsbewusstsein

Wir sind nicht nur im direkten, physischen Kontakt verwundbar! Auch im Internet lauern schmerzende Angriffe. Gewiegt im Gedanken einer trügerischen Sicherheit aus dem Netz einerseits und überfordernder Wissensflut in den neuen Technologien andererseits, stecken viele den Kopf in den Sand und tun so, als könnte ihnen – ja, gerade Ihnen - nichts passieren. Nun habe ich einige Fragen zu folgenden Themen an Sie:

- Grundlagen zu Sicherheit, Daten und Informationen (Kapitel 1)
  Wissen Sie, wodurch Ihre Daten bedroht werden und wie Sie Datensicherheit gewährleisten können?
- Malware (Kapitel 2)
  Wissen Sie, welche Arten von Malware es gibt? Haben Sie am Rechner ein Anti-Viren-Programm installiert?
- Netzwerke (Kapitel 3)
  Wissen Sie, wie Sie Netzwerke vor unberechtigten Zugriffen schützen?
- Zugriffskontrollen (Kapitel 4)
  Kennen Sie verschiedene Zugangskontrollen? Haben Sie eine sichere Pass-wortstrategie?
- WWW (Kapitel 5)
  Checken Sie beim Online-Einkauf das Sicherheitszertifikat bzw. achten Sie auf eine sichere Verbindung? Kennen Sie grundlegende Browser-Einstellungen?
- Online Community (Kapitel 6)
  Wissen Sie, welche persönlichen Daten Sie im Chat, auf Facebook oder sonst jemandem im World Wide Web bekannt geben und wissen Sie, wie Sie diese Daten nur für Ihren Freundeskreis zugänglich machen?

In einer unwirtlichen Winternacht schickt die Mutter ihre kleine Tochter durch den verlassenen Hinterhof, entlang der Hauptstraße zum Zigaretten-automaten neben der Spelunke …

Was längst ins Reich der Märchen gehört oder zumindest auf Ablehnung und verständnisloses Kopfschütteln stößt, soll im WWW, in der virtuellen, multimedialen, untereinander vernetzten Welt anders sein? Ganz anders? Sicher?

Nun, die Möglichkeiten, jemanden im WWW zu schädigen sind vielfältig. Aber wer streunt schon nächtens durch einsame, virtuelle Hinterhöfe und Datenbahnen?

Lassen Sie Ihre Geldbörse offen am Kiosk liegen oder machen Ihre Adresse im Einkaufszentrum öffentlich?

Im Netz verhält es sich genauso.

- E-Mails und IM (Kapitel 7)
  E-Mails sind lediglich so sicher wie Postkarten. Wissen Sie, welche Risiken durch E-Mails entstehen können? Kennen Sie Sicherheitsstrategien für elektronische Nachrichten?
- Datenmanagement (Kapitel 8)
  Haben Sie ein Backup Ihrer Daten erstellt und kümmern Sie sich laufend um die Sicherung des Datenbestandes? Kennen Sie zudem den Unterschied zwischen dem Löschen und dem Vernichten von Dateien?

Ja, solche Fragen können nervös machen. Wenn Sie nur eine dieser Fragen mit Nein beantworten, sollten diese Fragen Sie auch nervös machen. Denken Sie darüber nach.

Nun können Sie etwas für Ihre Sicherheit tun.

Information ist gewonnenes oder abgeleitetes Wissen

2. Datenbedrohung

Sind die Daten bedroht oder die Informationen? Nun, in der EDV arbeiten Sie mit digitalen Daten. Aus diesen Daten gewinnen Sie Informationen. In erster Linie sind also die Daten bedroht. Sind diese aber verfälscht oder verloren, dann gewinnen Sie auch keine sinnvollen Informationen mehr.

Daten können zwar auch Informationen sein, aber diese Informationen müssen digital aufbereitet werden. Erfassen Sie beispielsweise die aktuellen Aktienkurse oder Wetterdaten in Excel, dann sind das Daten. Daraus leiten Sie ab, ob eine Aktie gewinnbringend ist und ob Sie kaufen oder verkaufen sollen. Das sind die aus den Daten gewonnenen Informationen.

Die IKT hat aber auch unser tägliches Leben verändert:

- 3-D-Drucker arbeiten nicht nur mehr in großen Konzernen, sondern halten Einzug in unsere Wohnungen.
- Smart Home
- IP für Kühlschrank
- Fingerabdruck anstatt Hausschlüssel
- Vernetzter Badspiegel mit Wetteranzeige und Nachrichten
- Selbst fahrende Autos
- uvm.

Alle elektronischen Daten können gehackt und missbräuchlich verwendet werden.

Machen Sie sich also Gedanken darüber, welche böswilligen und unabsichtlichen Bedrohungen für Daten durch Einzelpersonen, Dienstleister und externe Organisationen entstehen können. Dabei geht es neben den auf Ihren Rechnern gespeicherten Daten und den Accounts bei verschiedenen Foren und sozialen Netzwerken online mittlerweile auch um Daten, die Sie in der Cloud online speichern. Bei Cloud-Diensten stellt sich die Frage, wie weit Ihre Privatsphäre geschützt bleibt. Achten Sie darauf, dass die Zugriffskontrolle in Ihrer Hand bleibt und nicht vom Anbieter kontrolliert wird. Das erreichen Sie am besten durch einen seriösen Anbieter in Ihrem Land.

In der Folge finden Sie einige Möglichkeiten aufgelistet, wie Daten bedroht werden können:

Cybercrime
Unter Cybercrime oder Computerkriminalität fallen Straftaten, die über das Internet oder mit Techniken des Internets geschehen. Dazu gehören unter anderem:

- Der vorsätzliche Betrug mittels eines Computers
- Der Betrug durch gestohlene Kreditkarten und PINs (*Skimming* genannt)
- Die Herstellung und Verbreitung von Viren
- Die Manipulation und Sabotage von Daten
- Das Ausspähen von Daten
- Der Identitätsdiebstahl oder Missbrauch der Identität
- Die Nutzung und Verbreitung von illegaler Software (*Softwarepiraterie*)
- Cyber-Mobbing, Cyber-Terrorismus, Cyber-Stalking, Verhetzung

Laut Statistik werden 69 % aller Menschen irgendwann Opfer von Cybercrime. Das sind 3 aus 4 Personen. 47 % kennen den / die Täter und 1 aus 3 Hacks kommt aus den USA.

Hacking – Cracking – ethisches Hacking [1]
Sowohl *Hacker* als auch *Cracker* umgehen die Zugriffsbarrieren zu Netzwerken. Streng genommen sind Cracker in böswilliger Absicht unterwegs. Hacker zeigen Schwachstellen auf. Hoch ausgebildete Personen, die in Systeme eindringen um Sicherheitslücken zu finden, nennt man *ethische Hacker*.

Hacker bekommen Infos zu 60 % vom PC oder aus dem Abfall, zu 25 % aus einem Hack während jemand online ist und zu 15 % aus dem Diebstahl der Geldbörse.

Vis major
Daten gehen unter Umständen durch Feuer, Wasser, andere Umweltkatastrophen oder Krieg verloren. Nur die regelmäßige Datensicherung auf externen Datenträgern schützt vor diesem Verlust. Private nutzen externe Festplatten oder CDs bzw. DVDs. In Firmen gibt es meist eigene Server. Wichtig dabei ist, dass diese Sicherungen wiederum sicher aufbewahrt werden. Sei es in Safes, in Bankschließfächern oder in verschlossenen Räumen mit feuerfesten Türen. Eine Speicherung online bietet Vorteile, da weder die Haltbarkeit der Speichermedien eine Rolle spielt noch neue Technologien die Speichermedien veralteten lassen – wodurch der Zugriff auf Daten, die auf alten Medien gespeichert wurden, wahrscheinlich nicht mehr möglich ist. Denken Sie an Disketten – viele neue Rechner haben kein Diskettenlaufwerk mehr.

Nicht zu unterschätzen sind auch gehackte Accounts zB bei WordPress, Visa & Mastercard oder Netflix. Beispielsweise wurden in jeweils einem einzigen Angriff auf Visa & Mastercard 1,5 Mio. Accounts gehackt, auf WordPress wurden 18 Mio. Konten gehackt und auf Netflix waren es 100 Mio.

Bedrohung von innen
Die unabsichtliche oder absichtliche Sabotage aus den eigenen Reihen macht den größten Teil des Datenverlusts oder der Datenmanipulation aus. Beispiele dafür sind unter anderem:

- Mitarbeitende verraten Passwörter
- Speichermedien gehen verloren
- Verseuchte Datenträger werden verwendet
- Frustrierte Personen in der Firma sabotieren oder spionieren Daten aus

[1] *Die Online-Ausgabe von „Der Standard" berichtet am 29.7.2016 von einer heiklen Aktion aus Amerika: Das FBI soll 50 Computer in Österreich mit Malware infiziert haben, um an die IP- und MAC-Adressen der Geräte zu gelangen. Der dazu verwendete Trojaner ist in Österreich allerdings illegal. Lesen Sie dazu den gesamten Artikel unter http://derstandard.at/2000042000467/Kinderpornographie-FBI-hackte-illegal-50-Computer-in-Oesterreich*

- Gebäude und Computerräume werden nicht abgeschlossen oder sind einladend für Einbrüche
- Ungenügend ausgebildete Administratoren erkennen Schwachstellen nicht und können so auch keine Gegenmaßnahmen treffen

Dienstleister
Denken Sie auch daran, dass Dienstleister Schaden anrichten können. Wenn beispielsweise ein Rechner extern repariert wird und dabei Daten auf der Festplatte in falsche Hände geraten oder durch das Formatieren des Speichermediums gelöscht werden.

Cloud-Computing
Wenn Sie Ihre Dateien online auf dem Server eines (fremden) Anbieters speichern, können Sie von überall auf der Welt darauf zugreifen und / oder diese Dateien auch an ausgewählte Personen freigeben. Ob diese Daten auch geschützt sind, eine verschlüsselte Datenübertragung eingerichtet wurde und der Server auch 24 Stunden am Tag erreichbar ist, liegt an der Qualität und Seriosität des Anbieters.

3. Wert von Informationen

Im günstigsten Fall erhalten Sie durch die Preisgabe persönlicher Informationen „nur" unerwünschtes Werbematerial. Was aber, wenn jemand vor der Tür steht oder die Identität gestohlen hat!? Schützen Sie Ihre Daten und die Ihnen anvertrauten Daten!

Wie Daten schützen?
Selbst in geschlossenen Systemen, können Viren, die über verseuchte Speichermedien ins System eindringen, Schaden anrichten. Moderne offene Umgebungen sind an andere Rechner und das Internet angebunden. Hier bedrohen auch Hacker Ihre Daten.

Verwenden Sie sichere Passwörter (vgl. dazu Lektion 4). Verschlüsseln Sie sensible Dateien, sowohl bei der Datenübertragung als auch beim Speichern. Laptops, Rechner und Datenträger auf denen irgendwann einmal persönliche und sensible Daten gespeichert wurden, stellen auch beim Entsorgen oder Verkaufen ein Sicherheitsrisiko dar. Weil Windows Dateien nicht wirklich löscht, sondern nur den Verweis auf eine Datei, können diese Daten mit den richtigen Programmen rekonstruiert werden.

Das Austauschen elektronischer Nachrichten, die weit verteilte Speicherung von Daten, E-Commerce, etc. stellen mitunter grobe Bedrohungen durch Missbrauch der Informationen, Veränderung der Daten oder Urheberrechts-verletzungen dar.

Was gewährt Datensicherheit?
Die Datensicherheit muss gewährleisten, dass die Daten vor unbefugter Verwendung geschützt sind. Eine Rolle spielen in diesem Zusammenhang die *Vertraulichkeit*, die *Integrität* und die *Verfügbarkeit* der Daten.

- **Vertraulichkeit** – Vertrauliche Daten müssen geschützt werden. Es dürfen weder Krankendaten, noch die Daten von Reisenden weiter gegeben werden. Nur für den Katastrophenfall gibt es Ausnahmen.
- **Integrität** – Die gesammelten, gespeicherten und verarbeiteten Daten müssen vollständig und unverändert bleiben. Weder sollen Bankdaten manipulierbar sein, noch sollen Personen aus der Kollegenschaft das Gehalt anderer Mitarbeitenden ändern können.
- **Verfügbarkeit** – Sollten Systeme ausfallen, stehen unter Umständen Aufzüge still, geben Bankomaten kein Geld her, Signale im Straßen- oder Zugverkehr funktionieren nicht. Unsere Gesellschaft hängt zu sehr von der Zuverlässigkeit der Computersysteme, als dass wir darauf verzichten könnten.

4. Sicherheitsstrategien

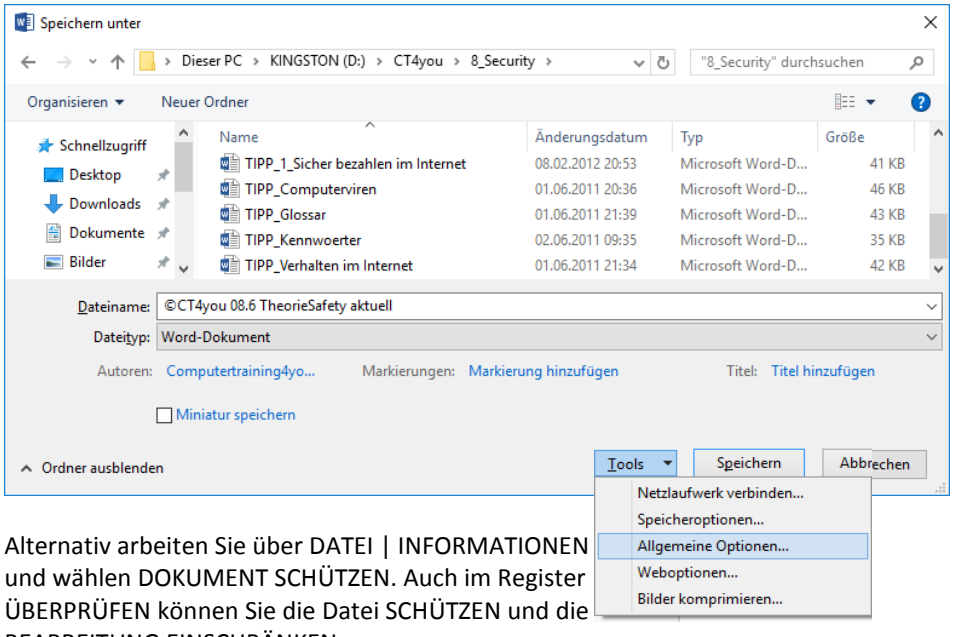
Wer Daten anderer Personen verarbeitet, ist also dazu verpflichtet, sicher zu stellen, dass diese Daten sicher gespeichert sind und der Zugriff unberechtigter Personen auf diese Daten ausgeschlossen ist.

Vorkehrungen

- Sicherungskopien (Backups) des gesamten Datenbestandes regelmäßig erstellen und aktualisieren
- Backups sicher aufbewahren
- Notstromaggregate sichern den unterbrechungsfreien Betrieb
- Zugriff auf die Daten nur Personen gewähren, die mit diesen Daten arbeiten
- Mitarbeitende schulen und sensibilisieren
- Eventuell das Verwenden von USB-Massespeichern oder anderen externen Speichermedien unterbinden
- Notfallpläne aufstellen, denn dann wissen die Mitarbeitenden, wie Sie sich im Fall eines Falles zu verhalten haben und wer zu informieren ist
- Wenn Sie mit mobilen Geräten arbeiten, dann achten Sie besonders darauf, dass Sie sich nur arbeiten können, wenn Sie sich mit einem geheimen Passwort, Code oder biometrischen Verfahren anmelden. Laptops können Sie zusätzlich mit einem Sicherungsschloss schützen. Weil die Firma Kensigton ein Schloss für Laptops, Flachbildschirme und auch Beamer herstellte, wird so eine Diebstahlsicherung gerne *Kensington-Schloss* genannt.

Sicherheit für Daten

Wenn Sie Dateien geheim halten möchten, dann sehen Sie über DATEI | SPEICHERN UNTER in den TOOLS nach (siehe Abbildung). Hier können Sie bei den ALLGEMEINEN OPTIONEN ein Kennwort zum Öffnen einer Datei vergeben. Wählen Sie ein sicheres Passwort (vgl. Sicherheit / Kapitel 4).

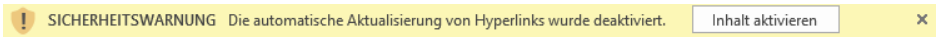


Alternativ arbeiten Sie über DATEI | INFORMATIONEN und wählen DOKUMENT SCHÜTZEN. Auch im Register ÜBERPRÜFEN können Sie die Datei SCHÜTZEN und die BEARBEITUNG EINSCHRÄNKEN.

Möchten Sie komprimierte Dateien schützen, dann brauchen Sie dafür ein zusätzliches Programm. Nutzen Sie zum Beispiel die Gratis-Software von 7-zip.de. Mehr dazu erfahren Sie in Lektion 4 ab Seite **Fehler! Textmarke nicht definiert.**.

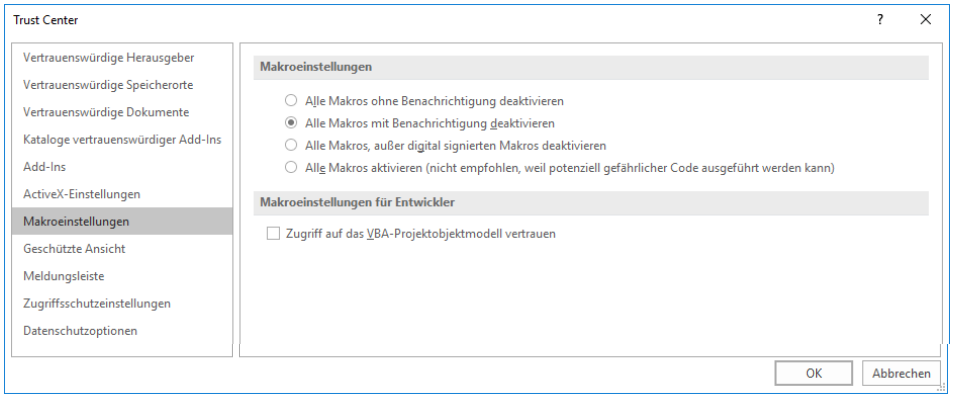
Zusätzlich verschlüsseln Sie wichtige Daten oder die gesamte Festplatte. Dazu nutzen Sie ein Programm, beispielsweise *Truecrypt* von www.truecrypt.org. Das Online-Magazin *PC-Welt* listet einige Gratis-Anbieter unter http://www.pcwelt.de/ratgeber/Daten-Tresore-praktische-Verschluesselungs-Tools-47871.html auf.[2]

In Word und anderen Office-Programmen können Sie Befehle mit Makros automatisieren. Diese Makros werden auch mitgespeichert. Öffnen Sie eine solche Datei, ist es sinnvoll eine Sicherheitswarnung zu erhalten (siehe Abbildung).



Aktivieren Sie den Inhalt nur dann, wenn die Datei vertrauenswürdig ist. Vor allem, wenn Sie eine E-Mail mit einem Dateianhang erhalten, ist es wichtig, dass diese Datei von einer sichern Quelle stammt. Denn Makros könnten auch Schadsoftware enthalten. Wenn Sie den Inhalt nicht aktivieren, wird die Datei ohne Makros geöffnet. Das reicht im Normalfall.

Prüfen Sie die Makro-Sicherheitseinstellungen. So bestimmen Sie, ob Befehle in Dateien automatisch ausgeführt werden dürfen. Wählen Sie dazu DATEI | OPTIONEN | TRUST CENTER | EINSTELLUNGEN FÜR DAS TRUST CENTER (siehe Abbildung).



ALLE MAKROS OHNE BENACHRICHTIGUNG DEAKTIVIEREN bringt maximale Sicherheit. Wenn Sie nie mit Makros arbeiten, bietet sich diese Option an.

ALLE MAKROS MIT BENACHRICHTIGUNG DEAKTIVIEREN ist standardmäßig ausgewählt. Öffnen Sie eine Datei, die Makros enthält, erhalten Sie die auf der vorhergehenden Seite abgebildete Sicherheitswarnung.

ALLE MAKROS AUSSER DIGITAL SIGNIERTE MAKROS DEAKTIVIEREN ist in jenen Firmen die bevorzugte Option, die Makros digital signieren.

ALLE MAKROS AKTIVIEREN ist nicht empfehlenswert, weil Sie damit auch versteckter Malware Zugang erlauben.

---

[2] *Auch auf http://www.computerwoche.de/a/wie-notebooks-sicherer-werden,2484630 finden Sie Informationen zum Thema Festplatten verschlüsseln. Die FAZ vom 16.2.2016 widmet dem Thema einen Artikel unter http://www.faz.net/aktuell/technik-motor/computer-internet/daten-auf-festplatte-durch-verschluesselung-schuetzen-14068877.html.*

Datenschutz
Der Datenschutz regelt den Schutz vor Missbrauch von persönlichen Daten. Es müssen die allgemeinen Grundsätze des Datenschutzes, der Privatsphäre, der Datenaufbewahrung und der Datenkontrolle eingehalten werden. Das bedeutet, es muss transparent sein, welche Daten gespeichert werden, die Speicherung muss notwendig und verhältnismäßig sein und die Speicherung muss für das Ziel angemessen sein.

Die Grundsätze des Datenschutzes sind:
- *Transparenz*
- *Notwendigkeit*
- *Verhältnismäßigkeit*

Via Smartphone, E-Mail und soziale Netzwerke werden viele persönliche Daten veröffentlicht. Neben Personen aus Ihrem Freundeskreis haben Firmen und Staaten großes Interesse an diesen Informationen. Behörden befürworten großteils die Vorratsdatenspeicherung, Firmen überprüfen so die Zahlungsfähigkeit ihrer Kundschaft und Versicherungen werden bald überprüfen, wie gesund Sie wirklich leben.

Leider bleiben Ihre Daten im Internet immer irgendwo abrufbar, das Internet „vergisst" nicht, sagt man. Achten Sie unbedingt darauf, welche Daten Sie also veröffentlichen. Denn diese Daten können auch von anderen Personen verwendet werden.

Das Thema „gläserner Mensch" ist allgegenwärtig. In Dänemark haben viele Firmen beispielsweise begonnen, Kurse für gesunde Ernährung anzubieten. Gut so. In der Kantine fällt es aber nun gleich auf, wenn Mitarbeitende nicht zum gesunden Menü greifen. Und der aktuellste Trend ist, dass Schlafkurse angeboten werden. Weil Ausgeschlafene einfach besser arbeiten. Via App aufs Smartphone aus der Chefetage können sich die Angestellten einfach und unkompliziert anleiten – und auch überprüfen – lassen.

Für Unternehmen, die Daten anderer Personen sammeln, speichern und weiter verarbeiten gibt es je nach Land strenge Datenschutzrichtlinien. Mehr zum Thema Datenschutz finden Sie im IKT-Teil unter Kapitel 2 Lektion 3 ab Seite **Fehler! Textmarke nicht definiert.**.

5. Persönliche Sicherheit

Phishing
So genannte *Phisher* tarnen sich via E-Mails als legitime Personen oder Unternehmen. Sie möchten an Ihre Kontoinformationen, Benutzernamen und Kennwörter herankommen. Sie könnten zum Beispiel in einem fingierten E-Mail aufgefordert werden, persönliche Daten einzugeben. Dazu werden Sie aufgefordert, auf einen Link zu klicken, dann werden Sie auf eine gefälschte Webseite umgeleitet und hier geben Sie fremden Personen Ihre Daten bekannt.

Wenden sich Phisher mit einer Instant Message an die Opfer, nennt man das *Smishing*. Von *Vishing* spricht man, wenn der Angriff über ein Video Call Programm erfolgt.

Pharming
Pharming ist eine Betrugsmethode, bei der die eingegebene Adresse im Web-Browser auf eine gefälschte Seite umgeleitet wird.

Shoulder Surfing
Haben Sie sich schon mal Gedanken darüber gemacht, wer Ihnen über die Schulter schaut, wenn Sie Geld beheben oder an der Kasse mit der Bankomatkarte bezahlen?

Skimming
Das Manipulieren eines Bankomaten durch Kameras, zusätzliche Karteneinzüge oder ausgetauschte Tastaturen, der Betrug durch gestohlene Kreditkarten oder PINs fallen in diese Kategorie.

Pretexting
Wenn sich jemand gefälschter Dokumente oder Websites bedient, damit er oder sie an sensible Daten herankommt, fällt das unter den Begriff Pretexting.

Information Diving oder Dumpster Diving
Werfen Sie weder Ausdrucke noch Speichermedien in den Müll. Shreddern Sie Papiere und achten Sie darauf, dass die Daten auf Speichermedien nicht nur gelöscht, sondern wirklich beseitigt wurden (vgl. Lektion 8).

User Accounts online Hacken
Es gibt dazu verschiedene Taktiken, um User Accounts online zu hacken:

- **Baiting** bedeutet, jemand bekommt ein Speichermedium auf dem Malware vorinstalliert ist.
- **Cross-Site Scripting**, sog. Website-übergreifendes Skripting, bedeutet, dass Sicherheitslücken in Webanwendungen ausgenutzt werden. So kann von einer vertrauenswürdigen Website ein Angriff gestartet werden. Meist sind persönliche Benutzerdaten zum Zweck eines Identitätsdiebstahls das Ziel.
- **Clickjacking** ist eine Technik, bei der ein Hacker eine Webseite mit einem transparenten Layer überlagert und die Nutzer dazu bringt, scheinbar harmlose Mausklicks zu machen.
- **Doxing** bezeichnet das Sammeln und anschließende Veröffentlichen von sensiblen privaten Daten mit dem Ziel, die betroffenen Personen bloßzustellen.

Ob Smart Homes mit IP-Adressen für Ihre Haushaltsgeräte oder ferngesteuerte Autos für Sie vor- oder nachteilig sind, müssen Sie selber entscheiden.

Wenn Sie bei Stromausfall nicht in Ihr Haus können, wird es unlustig. Und wenn Banken und Versicherungen neben Ihren Postings auf Facebook auch auf den Inhalt Ihres Kühlschranks zugreifen möchten oder Ihr Auto während der Fahrt gehackt wird, beginnt die Vernetzung gefährlich zu werden.

(Vgl. Modul Online Zusammenarbeit, Kapitel 1)

Social Engineering
Sie öffnen im WWW eine Seite und erhalten ein seriös wirkendes Fenster mit einer bedrohlichen Virenwarnung. Eine Antiviren-Lösung wird gleich propagiert. Allerdings ist diese „Lösung“ erst recht ein Programm, das Ihren PC mit Malware infiziert. Diese Aktion fällt unter den Begriff *Social Engineering*.

Es gibt verschiedene Formen von Social Engineering:

- **Social Engineering im sozialen Umfeld**
  Hacker fragen schlicht und einfach nach Konto- und Zugangsdaten – und erhalten diese Daten erstaunlich oft.
- **Social Engineering über das Telefon**
  Der Hacker gibt sich als neues Mitglied des Helpdesks aus oder Mitarbeitende des Helpdesks selbst sind das Ziel eines Hacking-Angriffs. Im ersten Fall gibt der Hacker vor, dringend ein Passwort zu brauchen, um ein Problem lösen zu können. Im zweiten Fall gibt der Hacker vor, Probleme mit einem Zugang in der Firma zu haben und bekommt die Einstellungen seinerseits freundlich und genau vom Helpdesk erklärt.
- **Social Engineering online**
  Gewinnmeldungen und Gratis-Angebote verlocken dazu, persönliche Daten in Formulare einzugeben. Obendrein haben viele Nutzende häufig nur ein einziges Passwort, das sie nun einem Hacker preisgegeben haben.
- **Reverse Social Engineering**
  Mit etwas Vorlaufzeit gelingt es Hackern, sich in einer Firma als Mitarbeitende vom Helpdesk mit Name und Telefonnummer vorzustellen. Taucht im Unternehmen ein EDV-Problem auf, wird nun leider der Hacker kontaktiert.

Drive-by-Angriff
Manche Angreifer nutzen Sicherheitslücken älterer Programme aus. Installieren Sie schlicht und einfach die jeweils aktuelle Browser-Version.

Diebstahl und Missbrauch der Identität
Personenbezogene Daten können verwendet werden, um Ihre Identität zu stehen und dann zu missbrauchen. Das kann zu Anzeigen bei der Polizei führen, zu Verurteilungen bei Gericht oder auch zu Verschuldungen. Wenn Sie bei eBay etwas er- oder versteigern, dann muss nach einem Urteil des Oberlandesgerichts Kölns vom 6. 9. 2002 und des Amtsgerichts Erfurt vom 14. 9. 2001 der Verkäufer beweisen, dass der Käufer mit dem Inhaber des Accounts identisch ist. Sollten Sie Opfer eines Identitätsmissbrauchs geworden sein, dann erstatten Sie umgehend eine Strafanzeige bei der Polizei.

Eine Form des Identitätsmissbrauchs wird gerne in sozialen Netzwerken und Foren verwendet. Um nicht die eigene Identität zu verraten, nutzen viele Usende Namen anderer, realer Personen, oft von bekannten Persönlichkeiten. Der Fachbegriff dafür lautet *Nicknapping*.

Sicherheit Schritt eins
Bewusstsein bilden

Übung und Selbststudium

1. Welche Sicherheitsstrategien gewährleisten in Firmen die Datensicherheit? Überprüfen Sie Ihr eigenes Verhalten: Machen sie Sicherungskopien? Wie bewahren Sie diese Kopien auf? Nutzen Sie verschiedene Passwörter? Verwenden Sie USB-Massespeicher?
2. Öffnen oder erstellen Sie ein Word-Dokument oder eine Excel-Arbeitsmappe. Beim Speichern vergeben Sie ein (sicheres) Kennwort.
3. Finden Sie in Word oder Excel heraus, wie Sie die Sicherheitseinstellungen für Makros verwalten.
4. Bei all den Bedrohungen der Daten vergisst man leicht, dass Computersucht das Leben schwer beeinträchtigt. Wie sieht es bei Ihnen mit der Abhängigkeit von Online Gambling, Online Gaming, Online Dating, Online Shopping, Social Networking oder exzessivem Surfen aus?
5. Besuchen Sie https://www.watchlist-internet.at. Hier werde die aktuellen Betrugsmethoden erläutert,
6. Erstellen Sie selber eine Liste von Bedrohungen. Unterteilen Sie dabei in geeignete Kategorien, beispielsweise in
   - Natürliche Bedrohungen
   - unbeabsichtigte Bedrohungen und
   - beabsichtigte Bedrohungen

Testen Sie Ihr Wissen

1. Definieren Sie den Unterschied zwischen Phishing und Skimming.
2. Erklären Sie den Begriff Cybercrime.
3. Was versteht man unter Social Engineering?

In der nächsten Lektion lernen Sie unterschiedliche Typen von Malware kennen.