ELEKTROHANDELSPROFI
Aus- & Weiterbildung im Elektrohandel

Lehr- und Lernunterlagen

Schwerpunkte Elektro- und Telekommunikationshandel

Datensicherheit und Datenschutz

von Wolfgang Mehnert

Inhaltsverzeichnis

Datensicherheit und Datenschutz

1 Grundlagen und Begriffserklärung

Der Begriff Datensicherheit beschreibt alle Maßnahmen zum Schutz von Daten vor Verfälschung, Zerstörung, Verlust, unrechtmäßiger und unerwünschter Weitergabe.

Beispiele zur Datensicherheit: Jemand erarbeitet Unterlagen für seinen Arbeitgeber und speichert die Unterlagen falsch ab und hat später keinen Zugriff mehr auf seine Daten. Damit sind die Daten verloren und die Arbeit war umsonst.

Der Laptop eines Geschäftsmannes fällt auf den Boden und ist kaputt. Weil er die Daten seines Geschäfts nur am Laptop gesichert hatte, sind diese verloren und es kann sein, dass der Geschäftsmann seine Tätigkeit nur mehr schlecht oder auch gar nicht mehr ausüben kann.

Ein Unternehmen forscht an einem zukunftsweisenden Produkt. Über eine nicht gesicherte Internetleitung gelangen Hacker auf den Server des Unternehmens und stehlen die Forschungsdaten. Die Daten werden an die Konkurrenz verkauft, die die Daten in ein Produkt umsetzt und damit viel Geld verdient, während das Forschungs-Unternehmen auf den Kosten für die Forschung sitzen bleibt und auch nichts verdient.

1.1 Zahlungsarten

Die meisten kriminellen Handlungen in der digitalen Welt haben mit Geld-Transaktionen zu tun. Kriminelle versuchen permanent an die Konten und damit an das Geld von Usern zu kommen. Daher ist es wichtig die unterschiedlichen Zahlungsarten und Möglichkeiten und deren Vorteile und Risiken zu kennen.

1.1.1 Kreditkartenzahlung

Kreditkarten sind zum Kauf im Internet unerlässlich geworden. Wer einen Onlinekauf tätigen möchte, muss seine Kreditkarten-Daten hinterlegen. Anschließend wird automatisch vom webbasierten Zahlungssystem die Gültigkeit der Kreditkarte und der Kreditrahmen des Kunden bei der Kreditkartenfirma abgefragt. Das alles passiert extrem schnell, ohne dass ein Mensch bei diesem Vorgang eingreifen müsste.

Bei der Zahlung mit Kreditkarten im Internet gibt es vier Daten, die einzugeben sind:

die Kreditkartennummer
das Gültigkeitsdatum
den Namen des Karteninhabers
die Kartenprüfnummer auf der Rückseite der Kreditkarte

Wer diese Daten besitzt kann somit, auch ohne Unterschrift, Bestellungen oder Einkäufe online tätigen. Bei der Bezahlung im Einzelhandel oder Restaurants muss meist noch eine Unterschrift am Zahlungsbeleg geleistet werden. Auch haben die meisten Kreditkarten heute einen vierstelligen PIN-Code, der für zusätzliche Sicherheit beim Einkauf im Geschäft oder im Restaurant sorgt.

Kreditkarten-Vorderseite: Kreditkartennummer, Gültigkeitsdatum und Name des/r Inhabers/in

Kreditkarten-Rückseite: Kartenprüfnummer. Bei dieser Karte: 012 *Fotos: Fotolia*

Der Kauf im Internet per Kreditkarte birgt somit Gefahren, die es gilt zu vermeiden. Die Kreditkarten-Daten müssen daher unbedingt geschützt werden. Sie dürfen keinesfalls leichtfertig weitergegeben werden! Zum Schutz dieser Daten sollte man immer auch prüfen, auf welchen Websites man seine Daten eingibt. Große Handelsplattformen oder Unternehmen werden sehr darauf bedacht sein, die Daten ihrer Kunden geheim zu halten und viel Geld für ein sicheres Online-Zahlungssystem aufzuwenden. Schlecht gesicherte Zahlungssysteme können von Hackern geknackt werden und wenn sie an die Kreditkarten-Daten von Kunden gelangen, kann damit zumindest kurzfristig viel Schaden angerichtet werden. Dies ist Hackern in der Vergangenheit immer wieder gelungen.

Zur Erhöhung der Sicherheit wurden für Kreditkarten zusätzlich Secure-Codes eingeführt. Wie beim Zahlen im Geschäft muss man einen vierstelligen Code eingeben, wenn man online bezahlt. Das macht aber das Online-Bezahlen wieder etwas umständlicher und daher verzichten viele darauf.

Besondere Gefahr im Internet stellen gefakte Websites dar. Diese Websites schauen den Websites von Banken oder großen Unternehmen sehr ähnlich und es besteht hohe Verwechslungsgefahr. Auf diesen Websites werden oft besonders günstige Produkte oder Dienstleistungen angegeben und man wird rasch aufgefordert seine Kreditkarten-Daten einzugeben. Den Betreibern dieser unsicheren Websites geht es nur darum an die Kreditkartendaten anderer Menschen zu kommen.

Sollte ein Kreditkarteninhaber fahrlässig mit seinen Daten umgehen, so muss im Missbrauchsfall die Kreditkartenfirma den Schaden nicht bezahlen. Gelangen Hacker über eigentlich für sicher gehaltene Bezahlsysteme an die Daten von Kunden und es entsteht ein Schaden, müsste der Kreditkartenbetreiber oder das betroffene Unternehmen, das die Website und das gehackte Bezahlsystem betreibt, den Schaden begleichen. Oft verzögern aber Rechtsstreitigkeiten dann die Rückzahlung des Schadens an Kreditkarteninhaber.

Um das Risiko für einen Inhaber oder eine Inhaberin nicht zu groß werden zu lassen, verfügen Kreditkarten über ein Limit, das von der Bank und dem Kunden gemeinsam festgelegt wird. Verfügt ein Kunde über wenig Geld wird das Limit von Bank und Kunden eher im unteren Bereich festgelegt werden. Verfügt ein Bankkunde über viel Geld, wird die Bank, die meist auch die Ausgabe der Kreditkarte abwickelt ein hohes Limit bekommen.

Eine Kreditkarte ist somit immer mit dem Bankkonto eines Kunden verbunden. Abgebucht werden alle Kreditkartenbewegungen meist am Monatsende. Somit werden Einkäufe oft erst einen Monat nach dem Kauf auch wirklich vom Konto abgebucht. Daher stammt auch der Name der Karten. Man kann kaufen, obwohl das Geld am Konto eigentlich dazu im Moment nicht ausreichen würde und bezahlt wird erst später, also wie ein kleiner Kredit. Es ist daher auch möglich Transaktionen im Internet vor Ablauf dieses Monats rückgängig zu machen. Sollte ein Geschäft schieflaufen, kann man sich mit der Kreditkarten Firma in Verbindung setzen und die Auszahlung möglicherweise verhindern.

Neben den jährlichen Kreditkartengebühren verdienen Kreditkartenfirmen damit, dass der Händler einen gewissen Prozentsatz (zwischen 0,7 und 1,7 Prozent) vom Umsatz bei Kartenzahlung an die Kreditkartenfirma abgeben bzw. bezahlen muss. Im Einzelhandel verzichten daher nach wie vor einige Händler darauf, diese Zahlungsform den Kunden anzubieten.

1.1.2 Paypal

Ein zusätzliches Bezahlsystem für Online-Käuferinnen und Käufer bietet ein privates Unternehmen Paypal an. Dabei werden die Kreditkarten- oder Kontodaten bei Paypal hinterlegt. Das Eingeben der Daten für unterschiedliche Transaktionen ist damit nicht mehr notwendig. Zusätzlich wirbt Paypal damit, dass der Käufer bei Problemen (Ware wird nicht geliefert oder ist beschädigt) einen Schutz genießt und man bei einem berechtigten Schaden die Kaufsumme zurückerstattet bekommt.
Mit Paypal können Geldbeträge auch an andere Paypal-Nutzer überwiesen werden. Das Angebot des Dienstleisters überschneidet sich mit dem von Banken und Kreditkartenfirmen. Der Nutzen liegt sicher in einer unkomplizierten Abwicklung und ist vor allem als zusätzliches Angebot am Online-Bezahlmarkt. Kosten entstehen Nutzern bei diesem Dienst nicht. Die Kosten werden auch hier vom Händler getragen, der Paypal als Zahlungsform auf seiner Website anbietet.

Foto: Mehnert

1.1.3 Bankeinzug und Bezahlung per Nachname

Online-Händler bieten auch das Bezahlen per Online-Banking an. Dies ist für Kunden gedacht, die über keine eigene Kreditkarte verfügen oder nur selten online einkaufen. Hierbei wird der fällige Betrag bei Bestellung vom Konto abgezogen. Das Risiko liegt daher eher beim Kunden. Anders ist es bei einer Bezahlung per Nachname. Dabei wird die Ware mit einer Rechnung geliefert. Die Zahlung erfolgt erst nach der Lieferung und kann vom Kunden eventuell auch verzögert werden. Das Risiko bei einem Kauf per Nachname liegt daher eher beim Verkäufer.

1.1.4 Über Telefonrechnung (Mehrwertdienste)

Bezahlungen von Einkäufen sind auch über die Telefonrechnung möglich. Solche Zahlungen finden meist im Zusammenhang mit der Nutzung eines Smartphones statt. Diese Zahlweise wird auch Mehrwertdienst genannt. In der Vergangenheit sind vor allem Jugendliche Opfer von zu teuren Mehrwertdiensten geworden. Allein das Anklicken eines Buttons in einer App oder einer Nachricht reichte, dass die Telefonrechnung zusätzlich belastet wurde. Es gilt daher im Zusammenhang mit solchen Diensten eine gewisse Skepsis und Vorsicht walten zu lassen. Vor allem, weil mit Mehrwertdiensten leicht die Übersicht über das ausgegebene Geld verloren gehen kann.

1.1.5 NFC

NFC (Near Field Communications) ist eine Technik, bei der Daten durch einen Chip über geringe Distanzen übertragen werden können. Der internationale Übertragungsstandard zum kontaktlosen Austausch von Daten funktioniert auf Basis elektromagnetischer Induktion. Meist wird der Chip, der in EC- bzw. Kreditkarten oder auch im Smartphone eingebaut ist, durch Auflegen auf einen Bezahlterminal abgelesen und aktiviert.

Mit dem Smartphone oder der Kreditkarte können bei Kontakt am Zahlungsterminal Zahlungen durchgeführt werden. *Foto: Fotolia*

Bezahlen per NFC ist die Bezahlform der näheren Zukunft. Es gibt sogar einzelne Menschen, die sich einen Chip unter die Haut einpflanzen haben lassen, damit sie zum Bezahlen keine Karte oder Gerät mehr brauchen. Per NFC können auch Zahlungen von Smartphone zu Smartphone getätigt werden. Meist handelt es sich aber aus Sicherheitsgründen um kleinere Beträge, die nur mit Berührung bezahlt werden können. In Österreich liegt das Limit bei Bankomatkarten meist bei 25 Euro. Wer höhere Beträge bezahlen möchte, muss einen PIN-Code eingeben. Die NFC-Technik ist vergleichbar mit der W-LAN-Technik, nur dass die Reichweite stark eingeschränkt und auf das nahe Umfeld begrenzt ist.

Es gibt Berichte darüber, dass Kriminelle mit speziellen NFC-Lesegeräten in Menschenmengen die Nähe zu den Menschen nutzen, um unbemerkt Überweisungen von kleineren Beträgen von den Smartphones der

nichts ahnenden Handynutzer zu tätigen. Die Kriminellen halten dabei das Lesegerät einfach nahe an Hosen- oder Handtaschen, in denen sie die Smartphones vermuten und erhalten damit automatisch die Erlaubnis per NFC zur Überweisung eines Geldbetrages. Bei vielen Geschädigten kann somit ein relativ hoher Betrag ergaunert werden. Handy Nutzer sollten daher Ihre Smartphones im Umfeld von größeren Menschenmengen so aufbewahren, dass ein Ablesen nicht einfach möglich ist.

2 Datensicherheit

2.1 Regeln zur Datensicherheit

• Seien Sie misstrauisch!	Öffnen Sie keine Nachrichten, deren Absender Sie nicht kennen oder deren Absender Sie misstrauen Texte mit vielen sprachlichen Fehlern könnten auf internationale Cyber-Kriminelle hinweisen, die die Texte per Internet übersetzt haben.
• Betrachten Sie Anhänge immer besonders kritisch!	In Anhängen ist oft Schadsoftware (Viren) versteckt. Beim Öffnen wird die Software aktiv
• Betriebssysteme und Apps sollten immer am aktuellsten Stand gehalten werden!	Mit Updates werden oft Sicherheitslücken der Betriebssoftware und von Apps geschlossen. Damit erschwert man Hackern den Zugriff
• Verwenden Sie sichere Passwörter!	Sichere Passwörter enthalten Groß- und Kleinschreibung, mindestens acht Zeichen sowie Sonderzeichen. **Z. B. Klasse_!2B** Neueste Erkenntnisse zum Thema Passwort haben ergeben, dass die meisten User Standard-Passwörter wie 123_Max verwenden. Solche Passwörter sind unsicher. Daher empfehlen Experten Passwörter, die einmalig sind. Zum Beispiel ein Satz, den man sich gut merken kann und den man leicht abwandelt. Beispiel: **Max!ohne!Stock?** Die Webseite „haveibeenpwned.com“ stellt einen Dienst zur Verfügung, mit dem man überprüfen kann, ob das eigene Passwort schon in diversen Listen im Internet zu finden ist.

• Veröffentlichen Sie keine öffentlich zugänglichen Daten von sich im Internet **(digitaler Fingerabdruck)**	Wer zum Beispiel Daten auf Facebook öffentlich zugänglich macht (voller Name, Geburtsdatum, Wohnort) gibt Kriminellen genug Daten, um zum Beispiel ein Fake-Profil zu erstellen und unter Ihrem Namen kriminell vorzugehen.
• Verwenden Sie Virenschutz-Apps oder Software!	Virenschutz-Apps oder Software bietet zusätzlichen Schutz. Aber Achtung. Virenschutz bedeutet nicht, dass alle Viren abgehalten werden. Virenschutz muss auch immer aktuell gehalten werden!
• Vorsicht bei offenen WLAN-Hotspots!	Beim Surfen in offenen WLAN-Netzwerken (im Zug, im Imbiss-Restaurant, auf öffentl. Plätzen usw) können Kriminelle mit der richtigen Software und Hardware schnell auf Daten Ihres Smartphones oder PCs zugreifen. Auch die Übernahme des gesamten Gerätes ist möglich. Geldgeschäfte oder heikle Informationen sollte man in offenen WLAN-Netzen nicht tätigen bzw. versenden.
• Schützen Sie Ihren WLAN-Router zu Hause mit einem starken Passwort!	Router und internetfähige Geräte zu Hause oder in der Firma arbeiten oft mit voreingestellten WLAN-Passwörtern, die Kriminellen bekannt sind. Sie suchen dann im Web nach den Geräten und übernehmen diese oder stehlen Daten und Geld von den Nutzern.
• Verwalten Sie Ihre Passwörter nicht digital!	Speichern Sie keinesfalls Passwörter oder Zugangsdaten am Smartphone oder PC ab. Eine mögliche Sicherung ist das schriftliche Notieren von Passwörtern und Zugangsdaten in Notizbüchern, die man sicher zu Hause oder in der Arbeit aufbewahrt. Dass Hacker am digitalen Gerät einbrechen und zur gleichen Zeit bei Ihnen zu Hause, ist sehr unwahrscheinlich.

2.2 Viren und Fallen am PC und Smartphone

Foto: Fotolia

Cyber-Kriminelle verbreiten seit dem Beginn des digitalen Zeitalters aus verschiedenen Gründen Programme, die sich als Schadsoftware entpuppt. Genannt werden diese Programme umgangssprachlich Viren, weil sie sich unbemerkt vom User oder der Userin am Smartphone oder Computer einnisten, wie bei einer Krankheit. Diese Kriminellen, oft auch Hacker genannt, versenden Viren oft, um an Informationen zu gelangen (Spähprogramme), um Informationen zu verbreiten oder um den Opfern Geld zu stehlen. Viele Cyberangriffe haben aber keinen anderen Sinn, als die Zerstörung der gespeicherten Daten. Meist bleiben die Kriminellen unentdeckt und können nicht zur Verantwortung gezogen werden. Angriffe erfolgen auch mit der scheinheiligen Begründung Sicherheitslücken in Systemen aufzuzeigen. Der Schutz vor Cyber-Angriffen verschlingt in der Zwischenzeit weltweit Milliarden-Beträge und wird immer wichtiger.

In der Zwischenzeit haben auch Staaten das Potenzial von Cyber-Attacken erkannt und betreiben regelrechte Cyber-Kriege (Cyber-Wars) gegen andere Staaten. Angriffe auf Websites großer Unternehmen, auf die Stromversorgung von Ländern oder auch Social-Media Dienste wie Facebook oder Twitter gehören heute bereits zum Standard im Wettkampf und Krieg der Staaten untereinander. Mit den Angriffen können wichtige Daten gestohlen werden oder einem anderen Land finanzieller Schaden zugefügt werden. Selbst Wahlen waren bereits Ziele von Cyber-Attacken (z. B. die Präsidenten-Wahlen in den USA 2016).

2.2.1 Computer-Würmer, Viren, Trojaner und Spyware (Tracking)

Als Computer-Wurm bezeichnet man ein Schadprogramm (= Maleware), das sich nach dem Infizieren automatisch verbreitet und vervielfältigt. Ein Computer-Wurm nutzt für die Verbreitung eine bestehende Infrastruktur am Rechner, also Programme wie Browser, E-Mailsoftware usw. Der Wurm nutzt dabei eingetragene E-Mail-Adressen um sich auch auf andere Rechner weiter zu verbreiten.

Ein Virus setzt sich im Booth-Bereich oder in einer Datei eines Computers fest. Durch Datenträger wie Speicherkarten oder USB-Sticks wird die Schadsoftware dann weiterverbreitet. Wird die infizierte Datei am zweiten Rechner aktiv vom User kopiert oder geöffnet, verbreitet sich der Virus weiter. Viren werden meist erst erkannt, wenn Dateien oder Programme beschädigt sind. Weil Viren so tief in das Software-System eines Gerätes vordringen, können sie besonders großen Schaden anrichten, bis hin zum Totalverlust jeglicher Software und damit auch Dateien. Selbst die Hardware kann im schlimmsten Fall durch Viren beschädigt werden. Im Gegensatz zu Viren-Software, die vom User unbewusst durch Kopieren oder Öffnen weiter verbreitet wird, verbreiten sich Würmer von alleine über E-Mail-Programme oder Websites und andere Kommunikations-Software.

Foto: Fotolia

Ein Trojaner ist eine als nützliches Programm oder Skript getarnte Schadsoftware. Im Hintergrund führt die Software dann aber eine ganz andere meist bösartige Funktion aus. Meist werden mit Trojanern Dateien und Daten unbrauchbar gemacht. Mit Hilfe von Trojanern wurden in der jüngeren Vergangenheit immer wieder Daten auf PCs und Smartphones unbrauchbar gemacht. Die User bekamen dann die erpresserische Nachricht, dass sie gegen Bezahlung eines gewissen Geldbetrages die Daten wieder entschlüsselt bekommen und sie wieder verwendet werden können. Die Polizei rät von Zahlungen in solchen Fällen dringend ab, da die kriminellen Hacker die Daten in den meisten Fällen auch nach einer Zahlung nicht wieder frei geben. Der einzige Schutz für Daten-Kidnapping ist das regelmäßige Sichern der Daten als Backup. Bei einem Angriff per Trojaner können die schadhaften Daten gelöscht und über das Backup wieder auf den PC oder das Smartphone geladen werden. Für User ist es sehr schwierig zwischen Computer-Viren, Würmern und Trojanern zu unterscheiden. Daher wird Schadsoftware oft generell als Computer-Virus bezeichnet. Durch die Verbreitung des Internets sind die meisten Schadprogramme heute Computer-Würmer.

Eine weitere unerwünschte Form von Software ist die sogenannte Spyware. Laut Wikipedia Eintrag zum Thema Spyware dienen Spyware-Programme meist dazu, das Nutzungsverhalten, insbesondere das Surfverhalten im Internet, zu analysieren. Die gewonnenen Daten werden kommerziell verwertet. Häufig geschieht dies durch das Einblenden gezielter Werbebanner oder Pop-ups, die an die möglichen Interessen des Internetbenutzers angepasst sind, wovon sich die Werbeunternehmen eine Steigerung der Wirksamkeit ihrer Methoden erhoffen. Spyware funktioniert auf vielfältige Weise. Im einfachsten Fall werden Schadprogramme auf dem Rechner hinterlegt, die nach dem Start automatisch aktiviert werden. Wird eine Verbindung zum Internet hergestellt, so werden die gesammelten Daten übermittelt. Beliebt ist ebenfalls die Tarnung der Spyware als Symbolleiste für den Webbrowser, die angeblich praktische Funktionen – wie das aktuelle Wetter oder ein Eingabefeld zur direkten Suche auf einer Website – enthält. Als Tracking bezeichnet man die Aufzeichnung und Auswertung des Nutzerverhaltens im Internet. Dies passiert direkt beim Besuch der Website. Dort wird im Hintergrund erfasst, was man wann und wie lange angeschaut hat. Cookies helfen beim Tracking. Cookies speichern für eine gewisse Zeit Daten, die beim Surfen auf einer Website anfallen. Mit Hilfe von Cookies kann der Anwender Websites für sich anpassen (Sprache, Schriftgröße usw.). Weil aber mit Hilfe von Cookies auch Daten gesammelt und an die Betreiber von Websites weitergeleitet werden können, sind diese in Verruf geraten. Cookies sind daher bei vielen Browsern deaktiviert. Besucht man eine Website, deren volle Nutzung die Aktivierung von Cookies erfordert, werden User aufgefordert Cookies generell zu aktivieren bzw. einmalig frei zu schalten.

Smartphone-Einstellungen ermöglichen Cookies zu blockieren und Tracking zu verhindern. *Foto: Apple*

2.2.2 Mehrwertdienste

Umgangssprachlich werden gleich mehrere kostenpflichtige Dienste (WAP-, WEB- und SMS-Dienste), die am Smartphone abgerufen werden, als Mehrwertdienste bezeichnet. WAP- und WEB-Dienste beschreiben Transaktionen oder Abos, die entgeltlich aus einem App-Store bezogen werden. Diese Geschäfte mit Drittanbietern haben nichts mit dem eigentlichen Netzbetreiber (A1, T-Mobile, Drei usw.) zu tun, werden aber über die monatliche Telefonrechnung des Netzbetreibers abgerechnet. Auf der Handy-Rechnung findet man solche entgeltlichen Dienste zum Beispiel wie bei A1 unter dem Punkt „Ihre Entgelte für Online-Dienste & Downloads“ abgerechnet.

Foto: Fotolia

Ein Mehrwertdienst beschreibt Dienstleistungen, die über entgeltliche Mehrwertnummern (0800, 0900) abgerechnet werden. Vor allem kostenpflichtige Service-Hotlines, SMS Chats oder Votings im TV nützen diese 0900-Mehrwertnummern zur Abrechnung. Zum Schutz der Konsumenten müssen die anfallenden Kosten für eine Telefon-Minute am Beginn des Gesprächs angesagt werden. Die Kosten für ein solches Gespräch können zum Teil beträchtlich sein. Seriöse Unternehmen und TV-Sender finanzieren mit diesem System den Aufwand für Service-Leistungen (Beratung am Telefon) oder Votings. Unseriöse Firmen oder Kriminelle nutzen Mehrwertdienste aus, um Kunden um viel Geld zu bringen. Vor allem Mehrwertdienste, die für den Kunden unbemerkt über das Ausland laufen, können extrem hohe Telefonrechnungen zur Folge haben. Kriminelle rufen oft auch wahllos Menschen am Telefon an und legen sofort auf. Handynutzer, die dann achtlos die Nummer zurückrufen, werden auf eine extrem teure Mehrwertnummer im EU-Ausland umgeleitet, die extrem hohe Kosten verursacht und einem Diebstahl gleichkommt. Netzbetreiber setzen daher auf Aufklärung und eigens gesetzte Limits bei der Telefonrechnung. Um sich selbst oder seine Kinder vor ungewollten Kosten durch Mehrwerttelefonnummern zu schützen, können diese Dienste über den Netzbetreiber auf Wunsch gesperrt werden.

2.2.3 Handy-Abo

Manche Kunden verlieren vor allem bei Abo-Abschlüssen (Abo = Abonnement) die Übersicht über die Anzahl der geschlossenen Handy-Abos (Klingelton-Abos, Wetterdienst-SMS usw.). Sogenannte Abo-Manager, angeboten von den Netzbetreibern, sollen dabei helfen den Überblick nicht zu verlieren. Ein Abo-Manager setzt jedoch auch eine gewisse Fähigkeit in Umgang mit dem Smartphone voraus. Oft sind es aber gerade Menschen, die nicht sehr gut mit der Smartphone Technik umgehen können, die in solche Abo-Fallen tappen. Auch bei Abos im Internet oder App-Store gibt es schwarze Schafe, die Abos so tarnen, dass sie der Kunde oft gar nicht als entgeltliches Service erkennt. Es gibt Abos ohne automatische Verlängerung und welche, mit automatischer Verlängerung. Vor allem die zweite Kategorie birgt Gefahren in sich. Oft wird dem Kunden auch der Ausstieg unmöglich gemacht, in dem die Kündigung des Abos erschwert oder gar keine Möglichkeit zur Kündigung angeboten wird. Es ist daher ratsam, sich bereits vor Abschluss eines Handy-Abos darüber zu informieren, wie man sich später auch wieder vom Abo lösen kann. Kunden sollten hier auch unbedingt die notwendigen Daten wie Passwörter und Zugangsdaten notieren, die man braucht, um das Abo abzuschließen und dann später auch wieder zu beenden.

2.2.4 In-App-Käufe

Vor allem Spiele-Apps bieten sogenannte In-App-Käufe (= Kauf innerhalb der App) an. In der Regel werden diese Käufe über den Netz- oder den App-Store-Betreiber abgerechnet. Mit In-App-Käufen können zusätzliche Funktionen, eine eigene Spielwährung oder Bonusinhalte freigeschaltet werden. Viele Apps bieten den Kunden die Möglichkeit die App zuerst kostenlos zu starten und kennen zu lernen und verlangen erst später für die weitere Nutzung der App Geld über In-App-Käufe. Seriöse Anbieter kennzeichnen Ihre Apps so, dass erkennbar ist, dass In-App-Käufe möglich sind. Vor allem bei Spiele-Apps besteht die Gefahr, dass User süchtig werden nach dem Spiel und um voran zu kommen Unsummen an Geld in In-App-Käufe investieren. Manche Spiele sind so aufgebaut, dass man ohne In-App-Käufe gar nicht mehr vorankommen kann.

Die meisten Apps sind zuerst kostenlos. Die Hersteller finanzieren sich meist mit in-App-Käufen für Zusatzleistungen. *Screenshot: Mehnert*

In-App-Käufe werden aufgeschlüsselt in aufbrauchbare und nicht aufbrauchbare Käufe. Aufbrauchbare Käufe wie eine Spielwährung, Spielhinweise oder der Export in ein neues Dateiformat müssen immer wieder neu erworben werden, wenn die Leistung „aufgebraucht“ ist. Nicht aufbrauchbare In-App-Käufe sind zum Beispiel ein Upgrade der App, Freischalten von Funktionen, Entfernen von Werbung oder Karten für Navigationssysteme. Diese Dienste werden einmal gekauft und stehen dem User dann für immer zur Verfügung.

Sogar der Übertrag auf ein neues Smartphone ist möglich. Voraussetzung für einen Übertrag des In-App-Kaufes ist, dass man sich die notwendigen Zugangsdaten aufgeschrieben hat.

2.2.5 Gefahren durch Mailings und Pishing

Viele Viren, Würmer oder Trojaner wurden mit Massen-Mailings per E-Mail versendet. Durch die Verbreitung steigt aber auch die Zahl von Angriffen auf User über Social-Media-Plattformen wie Whats-App oder Facebook. User sollten daher besonders bei Mails und Nachrichten von unbekannten Absendern Vorsicht walten. Anhänge oder Verlinkungen stellen dabei die größte Gefahr dar. In den Anhängen oder Verlinkungen wird von den Hackern und Kriminellen die Schadsoftware versteckt. Einmal angeklickt verbreitet sich die schädliche Software am Smartphone, Tablet oder PC.

Gefahr droht auch durch Massen-Mailings über die diversen Kommunikations-Dienste. Kriminelle senden dabei wahllos Aufrufe zum Geldüberweisen oder dem Eingeben von Konto- oder Kreditkartendaten (Pishing genannt) an hunderttausende Menschen bzw. Adressen und Telefonnummern. Die Verbrecher agieren nach dem Kalkül, dass bereits viel Geld verdient werden kann, wenn nur wenige Menschen auf das Betrugsmailing reagieren. Die Texte, mit denen eine Überweisung gefordert wird, zielen meist auf die Gier der Menschen. Es werden Produkte zu extrem billigen Preisen angeboten, wenn man schnell einen

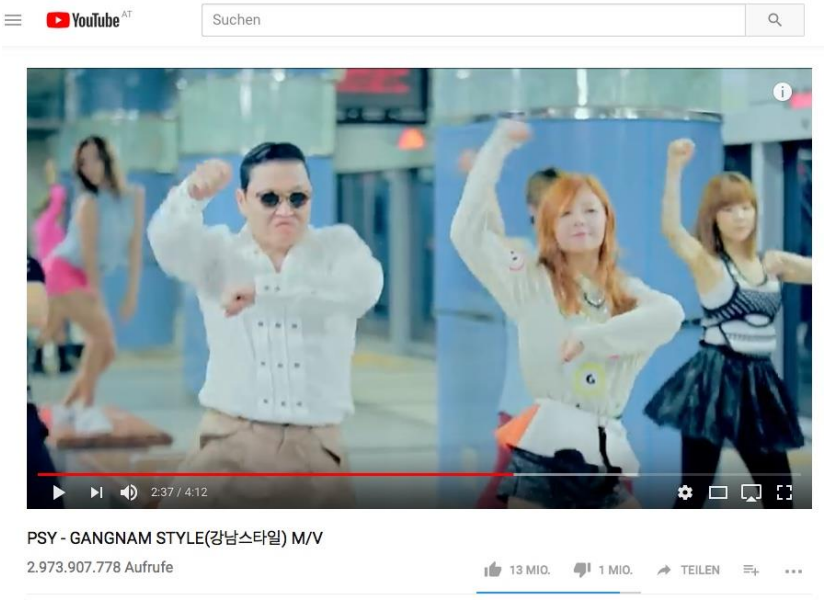
gewissen Geldbetrag überweist. Das Produkt wird natürlich nie geliefert. Das Interesse wird auch mit dem Gewinn bei einem Gewinnspiel geweckt, an dem man aber nie teilgenommen hat. Durch Zahlung eines kleineren Betrages bekommt man dann die Luxusreise oder das Auto. Auch hier gilt der Grundsatz: „Niemand im Internet hat etwas zu verschenken. Seriöse Gewinnspiele sind immer gratis und man muss daran teilnehmen, um gewinnen zu können. Unerwünschte Mails nennt man auch Spam- oder Junk-Mails (Spam und Junk sind Wörter aus dem Englischen und bedeuten Abfall). Beim Pishing, also dem Versuch User zur Herausgabe von Konto- oder Kreditkartendaten zu bringen, setzen Hacker auch darauf Websites von Banken oder anderen Instituten im Aussehen zu kopieren. Nur an der falschen Webadresse könnte der aufmerksame User den Betrug rechtzeitig bemerken. Es wird daher geraten, dass man seine Online-Bank-Geschäfte immer über die im Browser (unter Lesezeichen bzw. Favoriten) fix hinterlegten echten Webadressen der Bank aufruft und tätigt. Wer sein Onlinebanking über Suchdienste aufruft kann schnell bei Unachtsamkeit auf gefälschte Seiten im World Wide Web stoßen.

Beim Pishing wird versucht an Konto- oder Kreditkartendaten und deren Passwörter zu kommen. *Foto: Fotolia*

2.3 Social Media: Chancen und Gefahren

Der Begriff Social Media ist in aller Munde. Mit dem Siegeszug des Internets und des Smartphones ist es uns möglich geworden mit jedem und überall zu jedem Zeitpunkt zu kommunizieren. Früher standen dem Normalbürger zur Kommunikation nur wenige Medien wie Briefe oder das Telefon zur Verfügung. TV, Radio und Zeitungen waren eindimensionale Medien, die zwar konsumiert werden konnten, aber vom Leser, Zuseher oder Zuhörer nicht mitgestaltet werden konnten. Soziale Medien können nicht nur benutzt werden, um sehr schnell über große Distanzen hinweg auf unterschiedliche Art und Weise zu kommunizieren, sondern auch um seine eigenen Gedanken der gesamten Welt zur Verfügung zu stellen.

Mit einer eigenen Website, seiner eigenen Facebook-Seite, seinem Youtube-Kanal oder einem Blogg kann jeder User Millionen von Menschen erreichen. Klassische Medien wie das Fernsehen oder Zeitungen stehen deswegen unter großem Druck und verlagern ihr Angebot immer mehr in das Internet. Onlinezeitungen werden in der Zwischenzeit oft mehr gelesen als die Printversionen der Zeitungen. TV-Sender bieten Ihre Sendungen „on-demand“, also „auf Abruf“ in



Musikvideos werden auf Youtube am meisten aufgerufen. Fast drei Milliarden Aufrufe hat das Video Gangnam Style.

Foto: Youtube/Psy/Mehnert

sogenannten Internet-Mediatheken an. Auf diese Mediatheken kann dann dank des immer schneller werdenden Internets mit jedem Smartphone, Internet-TV-Gerät, PC oder Tablet zugegriffen werden. Die neuen Möglichkeiten der Kommunikation können eine Chance darstellen. Das im Internet gesammelte Wissen kann von jedermann abgerufen werden. Vom Rezept für einen Kuchen bis hin zu wissenschaftlichen Begriffen sind Informationen heute sofort abrufbar, während früher Wissen nur für wenige Menschen frei zugänglich war.

Wahrheit oder erfunden? Im Internet ist es oft schwer richtige von falschen Fakten zu unterscheiden. *Foto: Fotolia*

Die Gefahr am in sozialen Netzwerken (Social Media) verbreiteten Wissen ist, dass Menschen auch in der Lage sind, falsche Informationen zu verbreiten oder gefährliche Informationen – wie den Bauplan einer Bombe – abzurufen. In den klassischen Medien der westlichen Welt werden Informationen vor der Veröffentlichung auf ihren Wahrheitsgehalt geprüft und versucht ihre Relevanz einzuschätzen. Dies passiert bei der Veröffentlichung in sozialen Medien kaum bis gar nicht. So werden soziale Medien (auch digitale Medien genannt) immer mehr genutzt, um Falschmeldungen (Fake News) zu verbreiten. Interessensgruppen, Konzerne, ganze Staaten oder einzelne Menschen streuen bewusst Falschinformationen, um ihre Ziele zu erreichen. Was früher vor allem von Geheimdiensten in Kriegszeiten angewendet wurde, kann heute von Jedermann im World Wide Web gemacht werden.

Es gilt daher für alle Anwender (User), die das Internet und die darin enthaltenen sozialen Medien nutzen, eine Sorgfaltspflicht beim Veröffentlichen von Inhalten und auch beim Konsumieren von Informationen. Man sollte immer darauf achten, wer die Informationen im Internet verbreitet, ob diese Informationen geprüft sind und ob sie vielleicht gefälscht sein könnten.

2.3.1 Meistgenutzte Kommunikations-Apps

Die meistgenutzten Kommunikations-Apps, also Social-Media Plattformen (auch Multimedia Messaging Services MMS genannt) sind unter anderem: Whats-App, Facebook, Instagram, Pinterest, Snapchat, Flickr, Twitter, Tumblr, Xing, Youtube, Vimeo

Man kann diese Dienste auch noch genauer unterteilen in Beziehungsnetzwerke (z. B. Facebook), Bildnetzwerke (Instagram, Snapchat, Flickr usw), Blogging-Netzwerke (Twitter, Tumblr), berufliche Netzwerke (Xing, Linkedln) und Videonetzwerke (Youtube, Vimeo). Während Facebook unter Jugendlichen immer mehr an Bedeutung verliert, sind What-App, Snapchat, Youtube und

Grafik: Mehnert

Instagram aus dem Leben der jungen Internetnutzer nicht mehr weg zu denken. Für Netzbetreiber (A1, T-Mobile, Drei usw.) sind Plattformen wie Whats-App und Instagram zu einem Problem geworden, weil die Handynutzer heute praktisch zur Gänze auf das Schreiben von SMS verzichten und lieber diese Internet-Dienste nutzen. Whats-App und Co nutzen dabei die Infrastruktur der Netzbetreiber, ohne aber dafür zu bezahlen. Die Einnahmen aus dem früheren SMS-Geschäft fehlen heute den Netzbetreibern, was langfristig zu höheren Tarifen führen könnte.

Beschimpfungen über soziale Medien sind heute an der Tagesordnung und können für Betroffene schwerwiegende Konsequenzen nach sich ziehen.
Foto: Fotolia

Obwohl man sich auf Plattformen wie Whats-App, Instagram und Co. in einem relativ abgeschirmten Bereich befindet (hat man doch nur Kontakt mit jenen Menschen, deren Telefonnummer man auch eingespeichert hat und damit in den meisten Fällen auch kennt) lauern auch innerhalb dieser sozialen Medien Gefahren. Vor allem das gegenseitige Beschimpfen in diesen Kommunikations-Apps kann Nutzer extrem unter Druck setzen.
Vor allem bei Jugendlichen kann es innerhalb von Kommunikations-Gruppen zu Beschimpfungen einzelner kommen. Dieses Phänomen hat sogar einen Namen: Cyber-Mobbing. Für die Betroffenen sind Angriffe oder Beschimpfungen in sozialen Medien extrem unangenehm und können zu Depressionen führen. Meist können die Beteiligten nicht mit der Situation umgehen. Ein Entkommen aus einer Cyber-Mobbing-Spirale ist daher oft nicht möglich.

Ebenfalls sehr gefährlich sind falsche Behauptungen über Personen in sozialen Netzwerken. Einmal getätigt, werden diese Behauptungen als Wahrheit von anderen Nutzern übernommen. Für die betroffenen Menschen, die unter den falschen Anschuldigungen leiden, ist es sehr schwer diese Lügen wieder aus dem Gedächtnis des Internets zu löschen. Weltweit gab es in den letzten Jahren viele Fälle, in denen zu unrecht beschuldigte Menschen versucht haben, Einträge im Internet durch Betreiber von sozialen Plattformen wie Facebook, löschen zu lassen. Anfangs gab es keinerlei rechtliche Grundlagen auf die sich die betroffenen Menschen stützen hätten können. In der Zwischenzeit gibt es eigene Gesetze, die Menschen im Internet vor Falschmeldungen schützen sollen. Aus Sicht einiger Datenschützer sind das noch zu wenige Gesetze. Aber die Problematik ist erkannt und der österreichische Staat versucht vor allem durch Aufklärung, vor allem in Schulen, vor den Gefahren im Umgang mit sozialen Medien zu informieren und Jugendliche sowie Erwachsene davor zu bewahren.

Während sich Twitter in anderen Ländern großer Beliebtheit erfreut, hat die Kommunikations-App in Österreich nur wenige regelmäßige User. Wie weit die Möglichkeiten von sozialen Netzwerken in der Zwischenzeit reichen, sieht man am US-Wahlkampf von 2016. Experten vermuten, dass der permanent twitternde US-Präsident Donald Trump seinen Wahlsieg zu einem großen Teil seinen Veröffentlichungen auf Twitter verdankt. Dieses Medium erlaubte ihm seine Gedanken ungefiltert weiter zu geben, was ihm mit klassischen Medien nicht möglich gewesen wäre.

2.3.2 Digitaler Fingerabdruck

Wer im Internet unterwegs ist und soziale Medien nutzt, hinterlässt einen sogenannten „digitalen Fingerabdruck“. Jeder Eintrag auf Facebook wird gespeichert, jede Veröffentlichung auf einer Website oder jeder Eintrag in einem Blogg kann von anderen Menschen abgerufen werden. Im Laufe der Zeit entsteht über jeden Menschen ein Bild, das sehr viel über ihn verrät.

Alte Jugendsünden oder unüberlegte Kommentare könnten somit später bei der Jobsuche zu einem Hindernis werden. Auch können Kriminelle oder Hacker all die Einträge über eine Person nutzen, um sie zu manipulieren. Wer auf Facebook zum Beispiel öffentlich postet, dass er vor Abreise in den Urlaub steht, gibt Einbrechern die Information, dass eine Wohnung nun leer stehen wird und sie ungestört dort einbrechen können. Manche Menschen stellen auch ohne darüber nachzudenken Fotos von sich ins Internet, die später im Leben für peinliche Momente sorgen können. Experten empfehlen daher, dass User nicht zu viele Informationen über sich selbst ins Internet stellen und sich immer genau überlegen sollten, was sie posten und wer Zugriff auf diese Informationen hat.

2.3.3 Firmen checken social Media-Plattformen

In den vergangenen Jahren ist es üblich geworden, Menschen zu „googeln“. Das bedeutet, dass man sich Informationen über eine Person aus dem Internet holt. Lernt man jemanden beim Ausgehen kennen, kann man schnell und anonym an Informationen über die neue Bekanntschaft gelangen, wenn man nur den Namen kennt. Auch Firmen nutzen immer mehr die Möglichkeit leicht an Informationen über potentielle neue Mitarbeiter zu kommen und „googeln“ nach. Freizügige Fotos oder politische Bemerkungen könnten einer Anstellung dann im Wege stehen. Auch riskante Hobbys oder der Umgang mit dem falschen Freundeskreis könnte Firmen abschrecken jemand neu einzustellen.

2.4 Begriffe aus dem digitalen Zeitalter

2.4.1 Cyber Mobbing

Das Thema ist so aktuell, dass das österreichische Bundeskanzleramt eine eigene Seite dazu online gestellt hat. Darauf wird der Begriff folgendermaßen beschrieben: Cyber-Mobbing und Cyber-Bullying meinen das bewusste Beleidigen, Bedrohen, Bloßstellen oder Belästigen mit elektronischen Kommunikationsmitteln wie dem Handy oder im Internet. Im Internet werden vor allem Foto- und Videoplattformen (z.B. Flickr oder YouTube) und Soziale Netzwerke (z.B. Facebook) für diese Angriffe missbraucht.
Cyber-Mobbing findet meist auf der verbalen und/oder psychischen Ebene statt. Aber auch physische Gewalt als Antwort auf psychische Attacken oder in Form von „Happy Slapping“ können Teil von Cyber-Mobbing sein (Als „Happy Slapping“ bezeichnet man körperliche Angriffe auf unbekannte Personen, Mitschüler oder Lehrer, die gefilmt und im Internet veröffentlicht werden) . Seit dem 1. Jänner 2016 ist „Cyber-Mobbing“ strafbar. Der im Strafgesetzbuch (StGB) verwendete Titel des Delikts lautet „Fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems“. Mehr dazu können Sie unter www.help.gv.at erfahren.

2.4.2 Digitale Industriespionage

Industrie-Spionage verursacht weltweit einen Milliarden-schaden. Ideen und teure Entwicklungs-Pläne werden gestohlen und kopiert. *Foto: Fotolia*

Der Begriff Industrie-Spionage beschränkt sich heute nicht nur mehr auf Betriebe mit industrieller Produktion. Auch Dienstleister können davon betroffen sein. Beschrieben wird damit der Versuch von außen an geheime oder vertrauliche Informationen eines Betriebes zu kommen. Früher wurden dafür extra Menschen angeheuert, die als Spione in einem Betrieb versucht haben an gewinnbringende Informationen zu gelangen. Im digitalen Zeitalter werden immer mehr Angriffe über das Internet auf Unternehmen durchgeführt. Mit Hilfe von Viren oder digitalen Schlupflöchern wird von Kriminellen, Konkurrenten oder Staaten versucht, auf die Server der Unternehmen zu gelangen. Dort werden dann Forschungsergebnisse oder Konstruktionspläne gestohlen. Die digitalen Diebe sparen sich so viel Geld für die Entwicklung eines Produktes oder einer Dienstleistung. Denken Sie nur daran, dass die Entwicklung eines Autos bis zu einer Milliarde Euros kosten kann. Sollten die Pläne für das fertige Fahrzeug in die Hände der Konkurrenz gelangen, könnten sie das Fahrzeug in abgeänderter Form viel billiger auf den Markt bringen.

2.4.3 Cyber War

Durch die voranschreitende Vernetzung weltweit werden wir immer abhängiger von funktionierenden digitalen Abläufen. Fällt zum Beispiel das Datennetzwerk eines Flughafens aus, muss der Flugverkehr heute sofort eingestellt werden. Auch in der Praxis eines Arztes geht ohne digitale Verarbeitung der Daten der Patienten praktisch nichts mehr. Stromerzeuger steuern riesige Stromnetze über eine einzige Zentrale. Sollte diese ausfallen, wäre die Stromversorgung unterbrochen, was extreme Auswirkungen haben kann.

Sollten also Netzwerke von Unternehmen oder Staaten von außen angegriffen werden, kann ein beträchtlicher Schaden angerichtet werden. Sind es in Kriegen meist Bomben, die Schaden anrichten, werden bei einem Cyber-War (Cyber-Krieg) Schäden durch digitale Viren verursacht, die die Infrastruktur eines Landes lahmlegen. Die USA führten zum Beispiel gegen den Iran einen Cyber-War, in dem Sie die Computer eines Atom-Kraftwerkes infizierten und lahmlegten. Die USA vermuteten, dass in diesem Atom-Kraftwerk die Grundlagen zum Bau einer Atombombe geschaffen werden.

2.4.4 Sexting

Als Sexting wird das Versenden von privaten Fotos oder Nachrichten mit sexuellem Inhalt bezeichnet. Eine österreichische Studie von SaferInternet hat ergeben, dass Sexting unter Jugendlichen zwischen 14 und 18 Jahren weit verbreitet ist. Das leichtfertige Weitergeben von intimen Fotoaufnahmen oder Nachrichten kann aber weitreichende Folgen für jene haben, die sie versenden. Immer wieder kommt es vor, dass Fotos - vom Sender oder der Senderin - ungewollt von der Empfängerin oder dem Empfänger an Dritte weiter gegeben werden. Ein unkontrolliertes Weiterverbreiten der Daten ist somit vorprogrammiert.

Auch werden Jugendliche, die keine intimen Fotos von sich versenden wollen, von anderen unter Druck gesetzt, bis sie die gewünschten Fotos oder Nachrichten senden. In der Folge gibt es oft auch Drohungen und Erpressungsversuche mit den gesendeten Fotos und Nachrichten. Daten- und Jugendschützer raten daher dringend davon ab Nachrichten und Fotos mit sexuellem Inhalt zu versenden. Zu groß ist die Gefahr, dass die Daten missbräuchlich oder gegen die Absender verwendet werden.

2.4.5 Digitaler Einbruch

Ein Einbruch in die eigene Wohnung oder das eigene Haus ist meist ein dramatisches Erlebnis. Nicht nur der Verlust von Gegenständen oder Wertsachen sorgt bei den Betroffenen für Unbehagen, sondern vor allem der Verlust der Privatsphäre. Die Tatsache also, dass jemand in den geschützten, privaten Bereich eingedrungen ist. Neben dem Einbruch in die eigenen vier Wände gibt es auch einen Einbruch in die digitale Privatsphäre. Durch unsichere Datenverbindungen und mit der geeigneten Hardware können Hacker oder Kriminelle auch einen fremden PC oder Smartphone übernehmen.

Sie können dabei alles mitverfolgen, was am Smartphone, Tablet oder PC geschrieben oder bearbeitet wird. Mikrophone können freigeschaltet werden, sodass alles mitgehört wird, was gesprochen wird. Auch können die integrierten Kameras eingeschaltet werden, sodass der User oder die Userin live beobachtet werden können. Immer wieder wird zum Beispiel darauf aufmerksam gemacht, dass vernetzte Videokameras nach dem Kauf mit Standardpasswörtern ausgeliefert werden. Über IP-Adressen können Hacker somit ganz einfach auf die Kameras zugreifen und mitverfolgen, was auf den Kameras zu sehen ist.

Jeder User bekommt im Internet eine IP-Adresse zugewiesen. Wie eine Adresse vom zu Hause kann man sich so identifizieren aber auch gehackt werden.

Foto: Fotolia

Usern wird daher dringend dazu geraten, sich mit den Sicherheitsbestimmungen für die verwendeten Geräte zu beschäftigen. Vor allem das Eingeben neuer, sicherer Passwörter bei der Nutzung von W-LAN Routern oder W-LAN-fähigen Geräten wie Videokameras ist unumgänglich. Auch zum permanenten Updaten auf die aktuellsten und sichersten Software Anwendungen wird geraten. Da auch moderne Flachbild-TV- Geräte in Wahrheit internetfähige Hightech-Computer mit Bildschirm sind, sind selbst TV Geräte von Hacker-Angriffen und einem digitalen Einbruch oder Angriff nicht ausgeschlossen.

Bei einem großen, weltweiten Cyber-Angriff wurden selbst vernetzte Kühlschränke oder Drucker und Kopierer missbraucht, um große Serversysteme mit vorgetäuschten Anfragen zu überfluten und damit außer Betrieb zu setzen. Die Besitzer der Kühlschränke und Drucker haben von dem Missbrauch nicht das Geringste mitbekommen.

2.5 WLAN-Sicherheit

2.5.1 Offenes W-LAN

Weil das drahtlose Internet W-LAN immer mehr an Bedeutung gewinnt, bieten bereits zahlreiche Einrichtungen oder Unternehmen ein offenes W-LAN Netz an. Weltweit nutzen täglich Millionen von Smartphone- und Tablet-User dieses Angebot. Aber genau diese offenen W-LAN Netzwerke stellen eine große Gefahr dar. Befindet sich nämlich gleichzeitig ein Hacker im selben offenen W-LAN Netz (am Bahnhof, im Schnell-Imbiss-Restaurant, im Hotel usw.) so hat er leichtes Spiel und muss nur wenig Energie aufwenden, um Zugriff auf die fremden Geräte zu bekommen. Viele Anbieter von offenen W-LAN Netzwerken sichern sich gegen Schadensersatzansprüche ab, in dem man vor der Nutzung einer Nutzungsbedingung zustimmen muss, die eben dies ausschließt. Darin wird auch auf die Gefahren des offenen Netzwerkes hingewiesen. Die meisten User stimmen den Nutzungsbedingungen ohne sie zu lesen zu.

Wer sich in offenen W-LAN-Netzwerken befindet, der sollte dringend vermeiden auf heikle Daten wie dem Online-Bankkonto zuzugreifen. Zu einfach könnten Hacker die Zugangsdaten ausspähen. Das Lesen der Onlinezeitung in offenen Netzwerken erscheint weniger problematisch zu sein. Wer heikle Daten auf seinem mobilen PC gespeichert hat, sollte offene W-LAN Netzwerke aus Sicherheitsgründen vermeiden.

Offenes W-LAN im Einkaufszentrum ist praktisch, kann aber auch gefährlich sein. *Foto: Fotolia*

Die Internet-Plattform Macwelt.de rät zum sicheren Surfen in offenen W-LAN Netzwerken zur Nutzung einer VPN-Lösung. Diese schützt wie eine zusätzliche Schutzschicht ein- und ausgehende Datenverbindungen. Der Internet-Browser Opera bietet zum Beispiel die kostenlose Lösung Opera VPN an. Aber auch immer mehr Anti-Virensoftware-Hersteller bieten VPN-Dienste an.

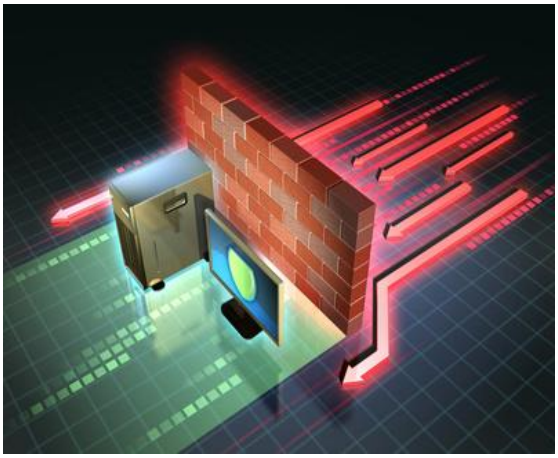
2.5.2 Geschütztes W-LAN

Ein geschütztes W-LAN Netzwerk ist durch ein starkes Passwort und einer Verschlüsselungs-Software geschützt. WPA2 nennt sich der derzeit sicherste Verschlüsselungsstandard bei herkömmlichen W-LAN-Routern. Dieses Verschlüsselungsverfahren verhindert das einfache Mitlesen der empfangenen und gesendeten Daten. Wer sein eigenes W-LAN-Netzwerk zu Hause sicherer gestalten und somit gegen unerwünschten Zugriff von Dritten schützen möchte, sollte sich unbedingt mit den Einstellungsmöglichkeiten des eigenen Routers beschäftigen. Die meisten Router bieten Sicherheitseinstellungen an, die von den Usern dann aber oft nicht genutzt werden. Wer sich über die Sicherheit beim Internetempfang über eine SIM-Karte mit 4G oder LTE informieren möchte, kontaktiert am besten seinen Netzanbieter. Dieser gibt zusätzliche Ratschläge zur idealen Absicherung am Smartphone oder Tablet. Grundsätzlich sind die Internetverbindungen über die großen Netzanbieter (Provider) gut gesichert und sollten kleineren Angriffen von außen Stand halten.

2.6 Virensoftware

2.6.1 Anti-Virensoftware für den PC mit Microsoft Betriebssystem

Während es für herkömmliche PCs und Laptops eine Vielzahl von Virensoftware im Handel gibt, ist der Markt für Viren-Apps für Smartphones sehr überschaubar. Vor allem Computer mit einem Microsoft Betriebssystem waren in der Vergangenheit Ziele von Hacker-Attacken. Der Wunsch nach Sicherheit schuf ein großes Angebot an Anti-Virensoftware. Zu den bekanntesten Produkten gehören: Kaspersky Internet Security, Avira, Norton, McAfee oder Bitdefender. Mit Windows 10 bietet Microsoft nun auch selbst ein ins Betriebssystem integriertes Anti-Viren-Programm mit Namen „Windows Defender“ an. Gegenüber den Bezahl-Virenprogrammen bietet „Windows Defender“ mit eingeschränkten Funktionen einen guten Grundschutz an. Allen Usern von PCs und Laptops ist der Einsatz einer Anti-Viren-Software dringend anzuraten. Ohne guten Schutz sind Microsoft-basierende Geräte immer wieder Cyber-Attacken ausgeliefert. Nur mit einer aktuellen und gut funktionierenden Anti-Virensoftware, können solche Attacken zumindest zum Großteil abgewehrt werden.



Eine Firewall-Software schützt vor unerwünschten Daten, bevor sie auf den Rechner oder das Smartphone gelangen. *Foto: Fotolia*

Einen weiteren Schutz vor Viren bietet die sogenannte Firewall. Im Gegensatz zur Virensoftware beschränkt eine Firewall den Netzwerkzugriff, in dem gefährliche Dateien oder unerwünschter Datenverkehr unterbunden wird. Der Einsatz einer Firewall-Software kann ein gesamtes Netzwerk betreffen oder aber auch nur einen einzelnen Rechner. Mit Hilfe einer Firewall oder einer ähnlich aufgebauten Filtersoftware kann auch der Zugang zum Internet für Kinder auf alterstaugliche Inhalte beschränkt werden. Am Smartphone bieten die Netzwerkbetreiber solche Kinderschutzfilter an.

2.6.2 Anti-Viren-Programme für Apple Geräte

Anti-Viren-Software für Apple Geräte gibt es nur sehr wenige. Die Computer des amerikanischen Herstellers waren nur selten Cyber-Angriffen ausgesetzt. Zu klein war die Zahl der Nutzer und zu abgeschirmt sind die Betriebssysteme gegenüber Eingriffen von außen. Das Abschirmen der Software macht die Geräte zwar weniger flexibel für Anpassungen durch die User. Im Zusammenhang mit Viren wirkt das geschlossene System aber als eine Art Festung, die kaum zu erobern ist.

Mit dem Erfolg von Apple beim Verkauf seiner Smartphones und Tablets stieg auch die Gefahr vermehrt Opfer von Hacker-Angriffen zu werden. Die Spyware Pegasus richtete sich direkt gegen IOS-Geräte. Trotzdem verbannte Apple jede Virensoftware aus dem App-Store. Grund dafür ist, dass Viren-Apps – wie alle anderen Apps auch – keinen Zugriff auf das Betriebssystem oder andere Apps haben. Somit können die Anti-Virenprogramme nichts scannen oder überprüfen. Da Mails und deren Anhänge ohnehin vom Provider oder Firmenserver gescannt werden, machen Viren-Programme auch beim Scannen von Anhängen kaum einen Sinn.

Fazit der Plattform www.macwelt.de: „Apple erlaubt keine Antivirensoftware im App Store, das ist auch gerechtfertigt. Eine App, die das iPhone auf einen Jailbreak (= nicht-autorisierte Entfernen von

Nutzungsbeschränkungen bei Computern) überprüft fehlt leider. Will man unterwegs mehr Datensicherheit, wäre als Zusatzversicherung eine VPN-Lösung zu empfehlen. Um das Erkennen von Bauernfänger-E-Mails und den Schutz seiner persönlichen Daten muss sich am Ende doch jeder Nutzer selbst kümmern - dies nimmt einem auch auf Mac und PC keiner ab.“

2.6.3 Anti-Viren-Programme für Android- und Microsoft-Geräte

Die bekanntesten Anti-Viren-Programme für Android und Microsoft Betriebssysteme sind:

Norton by Symantec
G Data
Bitdefender
Kaspersky
Avira
McAfee
Avast

Grafik: Mehnert

Die meisten Hersteller von Anti-Virensoftware bieten gratis Versionen Ihrer Produkte mit eingeschränkten Funktionen an. Wer mehr Sicherheit und Funktionen möchte, kann dann nach einer Testphase die gesamte Software kaufen oder sich monatlich binden und die Software mieten.

Für Smartphones und mobile Geräte mit dem Betriebssystem Android bieten fast alle großen Anti-Viren-Software-Hersteller eigene Versionen für Android an. Darüber hinaus gibt es auch eine Reihe von App-Anbietern, die Software nur für Android im Play-Store anbieten. Android ist offener programmiert wie es bei Apples IOS der Fall ist. Somit können Sicherheits-Apps auch tiefer ins System schauen und Schadsoftware erkennen.

Folgende Android-Antiviren-Apps gibt es unter anderem: Bitdefender Mobile Security, Kaspersky Mobile Security, ESET Mobile Security, McAfee Mobile Security, G DATA für Android, F-Secure Mobile Security
Die Apps enthalten dabei je nach Anbieter unterschiedliche Funktionen wie: Anti Malware, Anti Phishing, Anti Tracking, Anti Spyware, Anti Wurm, Anti Trojaner, Spamschutz, Cloud Scanner, Fern-Sperrung, Fern-Löschung, lokalisieren, Call Blocker, Message Filter, Backup Funktion, Daten Verschlüsselung. Die guten Anti-Viren-Apps für Android liefern somit ein komplettes Sicherheitspaket, das alle Bereiche umfasst, die für die Datensicherheit und den Datenschutz relevant sind.

3 Datensicherung

3.1 am Server

Wesentlicher Bestandteil der Datensicherheit ist die richtige Datensicherung. Zum Speichern von Daten steht eine Reihe von Hardware zur Verfügung. In Firmen und Institutionen gibt es Großrechner-Einheiten, Server genannt, die alle am Netzwerk angeschlossenen Computer und Netzwerkgeräte wie Drucker und Kopierer miteinander verbinden. Auf diesen Servern können Daten relativ sicher gespeichert werden. Ein gutes Serversystem ist meist auch gegen Viren-Attacken gesichert und bietet daher auch eine relativ hohe Datensicherheit an. Zusätzlich sollte jedes Serversystem über ein Backup-System verfügen, das alle gesicherten Daten ein zweites Mal auf einem externen Speichermedium sichert. Dies passiert meist automatisch und täglich oder mindestens wöchentlich.

3.2 Per Cloud Speicher

Immer wichtiger für die Datensicherung werden sogenannte Cloud-Speicher. Das sind Speicher-Plattformen, die über das Internet angeboten werden. Das immer schnellere Internet legt den Grundstock dafür, dass auch große Datenmengen in kurzer Zeit auf ferne Server der Anbieter übertragen werden können. Der Vorteil am Cloudspeicher liegt daran, dass man mit jeder Internetanbindung Zugriff auf seine Daten erhalten kann. Der Nutzer muss sich nicht um die Infrastruktur (Server, Software usw) kümmern.

Cloud-Speicher von Apple: icloud. *Foto: Mehnert*

Die Betreiber (Google – google drive, Dropbox, Apple – icloud, Microsoft one usw) bieten einen relativ hohen Schutz gegen das Eindringen von außen an und haben alle Daten auch über ein Backup-System doppelt abgesichert. Bedenken von Nutzern und Datenschützern gibt es allerdings gegen die Betreiber selbst. Sie haben theoretisch vollen Zugriff auf die Daten der Kunden. Eine Kontrolle, ob der Datenschutz vom Betreiber selbst eingehalten wird, gibt es nicht.

3.3 Am Computer oder Smartphone

Von einer lokalen Datensicherung spricht man, wenn Daten direkt auf dem Rechner (PC, Smartphone, Tablet) gespeichert werden. Die Daten sind schnell und leicht abrufbar, aber bei einem Defekt des Gerätes sind meist auch alle Daten komplett verloren. Auch bei einem Virenbefall sind die Daten verloren. Je nach eingebautem Speicherplatz können mehr oder weniger Daten gespeichert werden. Vor allem private Nutzer speichern ihre Daten ausschließlich direkt am Gerät und sind somit der Gefahr des kompletten Datenverlustes ausgeliefert.

3.4 Auf einem externen Speichermedium

Externe Speichermedien sind zum Beispiel externe Festplatten, auf denen größere Datenmengen gespeichert werden können, USB-Sticks oder SD-Karten. Diese Datenspeicher sind flexibel und auch mobil einsetzbar.

Daten können mit ihrer Hilfe transportiert oder doppelt abgesichert werden. Die Gefahr bei diesen Speichermedien liegt darin, dass Viren leicht übertragen werden können und sich mit Hilfe der externen Speichermedien auch von Gerät zu Gerät übertragen lassen.

Doppelt gesichert hält länger: Doppelte Datensicherung mit Hilfe einer externen Festplatte.
Foto: Fotolia

3.5 Doppelte Datensicherung

Bei der doppelten Datensicherung werden einzelne, wichtige Daten auf einem zweiten oder sogar dritten Medium - wie einem Cloud-Speicher, einer externen Festplatte oder einem USB-Stick - abgespeichert. Geht die Originaldatei verloren oder wird sie beschädigt, kann auf die Kopien der Datei zurückgegriffen werden. Es ist zu empfehlen, dass man bei der Erstellung von wichtigen Daten bereits in der Erstellungs-Phase Kopien auf externen Medien anfertigt. Sollte während der Erarbeitung ein Fehler am Hauptrechner auftreten, ist zumindest die letzte gespeicherte Version noch verfügbar. Immer wieder kommt es während der Erstellung von Dokumenten zu dramatischen Vorfällen, bei denen vor der endgültigen Fertigstellung der Datensatz verloren geht und die gesamte bereits geleistete Arbeit vernichtet wird.

Neuere Betriebssysteme bieten für solche Fälle Lösungen an, bei denen Dokumente automatisch zwischengespeichert werden und bei kleineren Vorfällen (z. B. einem Stromausfall) nicht verloren gehen. Eine optimale Sicherheit liefern diese Zwischenspeicher allerdings nicht. Nur das rechtzeitige und doppelte Sichern wichtiger Daten schützt vor deren Verlust.

Bei der Sicherung von Daten und Dateien spielt das richtige und organisierte Benennen von Dateien eine wichtige Rolle. Auch der Ort, an dem die Daten gesichert werden ist wesentlich dafür, dass die Dateien wiedergefunden werden können. Bei ungeschickter Dateibenennung und Unachtsamkeit bei der Speicherplatz-Wahl kann es vorkommen, dass man seine eigenen Dateien aufwendig suchen muss oder gar nicht mehr findet, was einem Datenverlust gleichkommt.

3.6 Backup

Ein Backup beschreibt die doppelte Sicherung von Daten und Programmen oder Apps von einem Computer, Server, Smartphone oder Tablet mit Hilfe einer speziellen Software. Am Computer kann sogar eine komplette Spiegelung bzw. Kopie des gesamten Datenvolumens über ein sogenanntes Image erstellt werden. So können weitere Geräte schnell und einfach mit identischer Software aufgesetzt werden. Bei einem Hardware-Schaden kann ein neuer PC rasch neu aufgesetzt werden.

Bei Smartphones oder Tablets bieten die Betriebssysteme IOS und Android automatische Backup-Einstellungen an. Bei Aktivierung werden jene Teile der Daten im Hintergrund doppelt auf dem vom Hersteller angebotenen Cloud-Speicher gesichert. So können Kontakte, Fotos, Videos, Terminkalender oder Apps gesichert werden. Bei Verlust des Smartphones bleiben die Daten erhalten und können über den Cloud-Speicher auf ein neues Gerät übertragen werden.

4 Datenschutz

Der Begriff Datenschutz wird oft unterschiedlich betrachtet. Im Großen und Ganzen geht es aber um den Schutz der persönlichen Rechte bei der Verarbeitung von Daten von Menschen (Rechtsbegriff = natürliche Person) oder Personenvereinigungen (Rechtsbegriff = juristischen Personen). Jeder Mensch oder Personenvereinigung hat demnach das Recht und den Schutz auf Privatsphäre selbst zu bestimmen, ob die eigenen Daten verarbeitet werden dürfen oder nicht. Gesetze zum Datenschutz sollen verhindern, dass

ungewollt zu viele Daten in die Hände von Organisationen, Staaten oder großer Betriebe gelangen und dass vor einer Verarbeitung der Daten die Zustimmung der natürlichen oder juristischen Person notwendig ist.

Zur Kontrolle des Datenschutzes wurde in Österreich sogar eine eigene Behörde gegründet. Die Datenschutzbehörde (www.dsb.gv.at), früher Datenschutzkommission genannt, sorgt für die Einhaltung des Datenschutzes in Österreich. Österreich war einer der ersten europäischen Staaten mit einer Behörde für den Datenschutz. Sie wurde mit dem ersten Datenschutzgesetz, BGBl. Nr. 565/1978, geschaffen. Mit der Datenschutzrichtlinie 95/46/EG der EU wurde das Datenschutzrecht in ganz Europa auf eine neue Grundlage gestellt. In Österreich wurde diese Richtlinie durch das Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999, umgesetzt. Die Datenschutzbehörde ist auch zuständig für das Datenverarbeitungsregister DVR. Dieses dient zur Transparenz der in Österreich durchgeführten Datenverarbeitungen. Wer in Österreich personenbezogene Daten verarbeiten möchte (Unternehmen und Behörden), muss sich bei der Datenschutzbehörde registrieren und die gewünschten Datenanwendungen verpflichtend melden. Geregelt wird von der DSB auch der internationale Datenaustausch. Firmen, die personenbezogene Daten austauschen wollen, brauchen die Genehmigung der Behörde.

Jeder Mensch oder juristische Person hat in Bezug auf Datenschutz folgende Rechte:

- Recht auf Geheimhaltung (§ 1 Abs. 1 DSG 2000)
- Recht auf Auskunft (§ 26 DSG 2000)
- Recht auf Richtigstellung oder Löschung (§ 27 DSG 2000)
- Recht auf Widerspruch (§ 28 DSG 2000)

Heute gibt es sogar Ausbildungen zum/r betrieblichen Datenschutzbeauftragten. Mitarbeiter/innen in Unternehmen, die sich um die Einhaltung der rechtlichen Vorgaben kümmern sollen. Neben der Datenschutzbehörde gibt es auch mehrere gemeinnützige Organisationen, die sich dem Datenschutz verschrieben haben. So gibt es die ARGE Daten (www.argedaten.at), die sich dem Datenschutz verschrieben hat und versucht, über die aktuelle Rechtslage zu informieren und Probleme im Zusammenhang mit Datenschutz aufzuzeigen. Auch politisch wird das Thema Datenschutz heiß diskutiert. Neue Software und Apps führen immer wieder zu neuen Fragestellungen, auf die Antworten und auch neue Gesetze gesucht werden. Im Anschluss finden Sie ein paar Fragen, die sich im Zusammenhang mit dem Datenschutz stellen.

Fragen zum Datenschutz:

Soll es dem Staat erlaubt sein alle Autos im Straßenverkehr per Video aufzunehmen, um Verkehrsunfälle zu vermeiden? Mit diesen Daten könnte man auch überprüfen wann sich wer wo aufgehalten hat.

Soll es Unternehmen erlaubt sein ohne Zustimmung Daten von allen Menschen zu sammeln, um Ihr Kaufverhalten zu beeinflussen? Stichwort Amazon oder Google. Eine Suchanfrage führt dazu, dass man im Anschluss viel Werbung zu jenen Produkten angezeigt bekommt, die man zuvor nachgeschlagen hat. Damit werden wir unterbewusst dazu verführt Produkte zu kaufen.

Sollte mein Arzt Daten über meine Krankheiten an meinen Arbeitgeber weiterleiten dürfen, wenn mein Arbeitgeber danach verlangt?

5 Arbeitsaufträge

Kundensituation:

Immer wieder kommt es vor, dass Nutzerinnen oder Nutzer ihr Smartphone verlieren, es gestohlen wird oder dass es kaputt wird. Wichtig ist in solchen Fällen, dass es ein Backup der Daten vom Smartphone gibt. Mit diesem Backup können die wichtigsten Daten wie Kontakte und Telefonnummern, Terminkalender sowie Fotos und Videos wiederhergestellt werden. Auch der Verlauf von Apps wie Whats App kann unter bestimmten Voraussetzungen am neuen Smartphone wieder aufgerufen werden. Als Expertin oder Experte im Telekommunikations- bzw. Elektrohandel sollen Sie in der Lage sein, Ihren Kunden zu erklären welche Einstellungen getroffen werden müssen, damit die Daten vom Smartphone automatisch gesichert werden können. Sie sollen aber auch in der Lage sein auf Wunsch diese Einstellungen am Smartphone des Kunden durchzuführen. Aber auch das Übertragen bzw. Wiederherstellen von Daten am neuen Smartphone stellt Kunden oft vor eine nicht zu bewältigende Aufgabe. Auch hier sollen Sie in der Lage sein zu unterstützen oder für den Kunden diese Dienstleistung durchzuführen.

5.1 Arbeitsauftrag 1

1.) Informieren Sie sich über die notwendigen Einstellungen auf Ihrem Betriebssystem, die notwendig sind, dass automatisch Backups von den wichtigsten Daten erstellt werden.

2.) Erstellen Sie im Anschluss einen schriftlichen Leitfaden (Anleitung), in dem Sie Screenshots von den einzelnen notwendigen Schritten auf Ihrem Smartphone machen. Übertragen Sie die Screenshots per Cloud-Speicher auf einen PC und fügen Sie dort die Screenshots in eine Word-Datei ein. Ergänzen Sie die Screenshot mit schriftlichen Bemerkungen und Erklärungen in vollen Sätzen.

3.) Steigen Sie im Anschluss am PC in den Cloud-Speicher Ihres Smartphone-Betriebssystems (icloud, Google Drive) ein und überprüfen Sie dort, ob alle ihre wichtigen Daten bereits gespeichert wurden.

4.) Erstellen Sie auch über den Einstieg in den Cloud-Speicher eine Anleitung mit Hilfe von Screenshots und schriftlichen Erklärungen.

5.) Testen Sie auch die Funktion Smartphone suchen, damit Sie im Falle eines Verlustes Ihres eigenen Smartphones bzw. des Smartphones eines Kunden, diese Funktion anwenden können. Beschreiben Sie auch diese Anwendung mit Hilfe von Screenshots und schriftlichen Erklärungen in Ihrem Leitfaden.

6.) Bilden Sie nach Fertigstellung Ihres Leitfadens Experten-Gruppen (maximal vier Personen) von Schülerinnen und Schülern, die ein Smartphone mit dem gleichen Betriebssystem wie Sie besitzen und nutzen. Tauschen Sie untereinander das gewonnene Wissen aus und vergleichen Sie Ihre Leitfäden. Ergänzen Sie in Ihrem Leitfaden Wissen, das andere festgehalten haben, Ihnen aber noch fehlt.

7.) Mischen Sie neue Gruppen zusammen, sodass in jeder Gruppe gleich viele Personen sind mit einem Android-Betriebssystem und einem IOS-Betriebssystem. Ziel ist es nun Beratungsgespräche durchzuführen, in denen die Android-Experten den IOS-Experten zeigen und vorführen, wie der Android-Leitfaden zum Thema anzuwenden ist. Anschließend erklären die IOS-Experten den Android-Experten Ihren Leitfaden und wie man den Leitfaden Apple-Geräten anwenden sollte.

8.) Geben Sie sich im Anschluss gegenseitig ein Feedback darüber, ob Sie als Kunde oder Kundin mit der Beratung durch Ihre Kolleginnen und Kollegen zufrieden gewesen wären und ob Sie das Erklärte verstanden haben und nun auch selbst anwenden könnten.

5.2 Arbeitsauftrag 2

Datenschutz betrifft uns alle. Die Frage wie viele Daten darf man über Menschen sammeln bewegt unsere Gesellschaft seit Jahren. Firmenchefs und -Chefinnen prüfen heute oft vor einer Einstellung Informationen von potentiellen Bewerberinnen und Bewerbern. Es ist daher ratsam, dass man keine unangebrachten Daten, Fotos oder Beiträge von sich im Internet veröffentlicht, die einem beruflich behindern könnten.

1.) Überprüfen Sie im Internet und sozialen Medien, wie viele und welche Daten Sie von sich dort finden. Listen Sie auch auf, bei wie vielen verschiedenen sozialen Medien Sie angemeldet sind. Egal ob Sie dort jemals aktiv geworden sind oder nicht.

2.) Betrachten Sie Ihre Auftritte in sozialen Medien kritisch. Versuchen Sie Fotos, Informationen und Videos von sich in digitalen Medien aus Sicht eines Firmenchefs oder -Chefin zu beurteilen. Gibt es eventuell veröffentlichte Informationen, die Ihrer beruflichen Karriere schaden könnten?

3.) Überlegen Sie welche Informationen Sie als Firmenchefin oder -Chef von Mitarbeitern im Internet nicht finden wollen würden. Welche Daten im Internet könnten dazu beitragen, dass Sie einen Job nicht bekommen und welche Daten bzw. Informationen Ihnen eine Anstellung eventuell erleichtern würden.

5.3 Arbeitsauftrag 3

Erstellen Sie eine Begriff-Liste mit mindestens 15 Fachbegriffen (z. B. Trojaner, Virus, Datensicherheit usw.), die in diesen Unterlagen erwähnt werden. Erklären Sie diese Begriffe unter Zsuhilfenahme der Unterlagen mit Ihren eigenen Worten und halten Sie diese Erklärung schriftlich fest. Diese Liste soll Ihnen helfen, einen Begriff im Verkaufsgespräch einem Kunden erklären zu können.

Beispiel:

Fachbegriff	**Erklärung**
Backup	Mit einem Backup werden – je nach persönlicher Einstellung – alle Daten komplett oder ausgewählte Datenpakete (Kontakte, Fotos, Terminkalender) an einem zweiten Ort (z. B. externe Festplatte oder Cloud-Speicher) abgespeichert. Ein Backup kann automatisch nach einer gewissen Zeit (einmal pro Woche, einmal pro Monat…) starten oder manuell vom User bei Bedarf gestartet werden. Bei Datenverlust kann auf die im Backup gespeicherten Daten zurückgegriffen werden.

6 WH-Fragen zum Thema Datenschutz und Datensicherung

1. Was versteht man unter dem Begriff Datensicherheit?

2. Welche bei uns üblichen Zahlungsmöglichkeiten im Internet oder mit dem Smartphone gibt es?

3. Benennen Sie mindestens fünf Regeln zur Datensicherheit!

4. Beschreiben Sie die Bedeutung der Begriffe Maleware, Computer-Wurm, Computer Virus und Computer-Trojaner?

5. Was versteht man unter dem Begriff Mehrwertdienst?

6. Was ist ein In-App-Kauf?

7. Was versteht man unter dem Begriff Pishing?

8. Welche Chancen bieten Social Media-Plattformen?

9. Welche Gefahren sind mit Social Media-Plattformen verbunden?

10. Benennen Sie fünf der meistgenutzten Kommunikations-Apps, also Social-Media-Plattformen!

11. In welche Bereiche kann man Kommunikations-App-Dienste auch unterteilen?

12. Beschreiben Sie den Begriff „digitaler Fingerabdruck“!

13. Welche Informationen können Sie einem Kunden geben, der sich über die Nutzung eines offenen W-LANs informiert?

14. Welche Android-Antivirensoftware-Apps gibt es unter anderem? Nennen Sie mindestens fünf App-Hersteller!

15. Welche vier Möglichkeiten der Datensicherung kennen Sie?

16. Was versteht man unter doppelter Datensicherung?

17. Was versteht man unter dem Begriff Backup?

18. Erklären Sie den Begriff Datenschutz?

19. Welche Rechte in Bezug auf Datenschutz hat jeder Mensch und jede juristische Person?

7 WH-Fragen samt Antworten

1. Was versteht man unter dem Begriff Datensicherheit?

Der Begriff Datensicherheit beschreibt alle Maßnahmen zum Schutz von Daten vor Verfälschung, Zerstörung, Verlust, unrechtmäßiger und unerwünschter Weitergabe.

2. Welche bei uns üblichen Zahlungsmöglichkeiten im Internet oder mit dem Smartphone gibt es?

Kreditkartenzahlung, Paypal, Bankeinzug, Bezahlung per Nachname, Über die Telefonrechnung (Mehrwertdienst), mit NFC Technik

3. Benennen Sie mindestens fünf Regeln zur Datensicherheit!

Seien Sie misstrauisch!
Betrachten Sie Anhänge immer besonders kritisch!
Betriebssysteme und Apps sollten immer am aktuellsten Stand gehalten werden!
Verwenden Sie sichere Passwörter!
Veröffentlichen Sie keine öffentlich zugänglichen Daten von sich im Internet (digitaler Fingerabdruck)!
Verwenden Sie Virenschutz-Apps oder Software!
Vorsicht bei offenen WLAN-Hotspots!
Schützen Sie Ihren WLAN-Router zu Hause mit einem starken Passwort!
Verwalten Sie Ihre Passwörter nicht digital!

4. Beschreiben Sie die Bedeutung der Begriffe Maleware, Computer-Wurm, Computer Virus und Computer-Trojaner?

Als Maleware wird ein Schadprogramm am Computer bezeichnet.

Als Computer-Wurm bezeichnet man ein Schadprogramm (= Maleware), das sich nach dem Infizieren automatisch verbreitet und vervielfältigt.

Ein Trojaner ist eine als nützliches Programm oder Skript getarnte Schadsoftware. Im Hintergrund führt die Software dann aber eine ganz andere, meist bösartige Funktion aus.

Ein Virus setzt sich im Booth-Bereich oder in einer Datei eines Computers fest. Durch Datenträger wie Speicherkarten oder USB-Sticks wird die Schadsoftware dann weiterverbreitet. Wird die infizierte Datei am zweiten Rechner aktiv vom User kopiert oder geöffnet, verbreitet sich der Virus weiter.

5. Was versteht man unter dem Begriff Mehrwertdienst?

Umgangssprachlich werden gleich mehrere kostenpflichtige Dienste (WAP-, WEB- und SMS-Dienste), die am Smartphone abgerufen werden, als Mehrwertdienste bezeichnet.

6. Was ist ein In-App-Kauf?

Vor allem Spiele-Apps bieten sogenannte In-App-Käufe (= Kauf innerhalb der App) an. In der Regel werden diese Käufe über den Netz- oder den App-Store-Betreiber abgerechnet. Mit In-App-Käufen können zusätzliche Funktionen, eine eigene Spielwährung oder Bonusinhalte freigeschaltet werden.

7. Was versteht man unter dem Begriff Pishing?

Beim Pishing, also dem Versuch User zur Herausgabe von Konto- oder Kreditkartendaten zu bringen, setzen Hacker auch darauf Websites von Banken oder anderen Instituten im Aussehen zu kopieren. Nur an der falschen Webadresse könnte der aufmerksame User den Betrug rechtzeitig bemerken.

8. Welche Chancen bieten Social Media-Plattformen?

Soziale Medien können nicht nur benutzt werden, um sehr schnell über große Distanzen hinweg auf unterschiedliche Art und Weise zu kommunizieren, sondern auch um seine eigenen Gedanken der gesamten Welt zur Verfügung zu stellen.

9. Welche Gefahren sind mit Social Media-Plattformen verbunden?

Die Gefahr am in sozialen Netzwerken (Social Media) verbreiteten Wissen ist, dass Menschen auch in der Lage sind, falsche Informationen zu verbreiten oder gefährliche Informationen - wie den Bauplan einer Bombe - abzurufen.

10. Benennen Sie fünf der meistgenutzten Kommunikations-Apps, also Social-Media-Plattformen:

Whats-App, Facebook, Instagram, Pinterest, Snapchat, Flickr, Twitter, Tumblr, Xing, Youtube, Vimeo

11. In welche Bereiche kann man Kommunikations-App-Dienste auch unterteilen?

Beziehungsnetzwerke, Bildnetzwerke, Blogging-Netzwerke, berufliche Netzwerke, Videonetzwerke.

12. Beschreiben Sie den Begriff „digitaler Fingerabdruck“.

Wer im Internet unterwegs ist und soziale Medien nutzt, hinterlässt einen sogenannten „digitalen Fingerabdruck“. Jeder Eintrag auf Facebook wird gespeichert, jede Veröffentlichung auf einer Website oder jeder Eintrag in einem Blogg kann von anderen Menschen abgerufen werden. Im Laufe der Zeit entsteht über jeden Menschen ein Bild, das sehr viel über ihn verrät.

13. Welche Informationen können Sie einem Kunden geben, der sich über die Nutzung eines offenen W-LANs informiert?

Weil das drahtlose Internet W-LAN immer mehr an Bedeutung gewinnt, bieten bereits zahlreiche Einrichtungen oder Unternehmen ein offenes W-LAN Netz an. Weltweit nutzen täglich Millionen von Smartphone- und Tablet-User dieses Angebot. Aber genau diese offenen W-LAN Netzwerke stellen eine große Gefahr dar. Befindet sich nämlich gleichzeitig ein Hacker im selben offenen W-LAN Netz (am Bahnhof, im Schnell-Imbiss-Restaurant, im Hotel usw.) so hat er leichtes Spiel und muss nur wenig Energie aufwenden, um Zugriff auf die fremden Geräte zu bekommen. Viele Anbieter von offenen W-LAN Netzwerken sichern sich gegen Schadensersatzansprüche ab, in dem man vor der Nutzung einer Nutzungsbedingung zustimmen muss, die eben dies ausschließt. Wer sich in offenen W-LAN-Netzwerken befindet, der sollte dringend vermeiden auf heikle Daten wie dem Online-Bankkonto zuzugreifen. Zu

einfach könnten Hacker die Zugangsdaten ausspähen. Das Lesen der Onlinezeitung in offenen Netzwerken erscheint weniger problematisch zu sein. Wer heikle Daten auf seinem mobilen PC gespeichert hat, sollte offene W-LAN Netzwerke aus Sicherheitsgründen vermeiden.

14. Welche Android-Antivirensoftware-Apps gibt es unter anderem? Nennen Sie mindestens fünf App-Hersteller:

Bitdefender Mobile Security, Kaspersky Mobile Security, ESET Mobile Security, McAfee Mobile Security, G DATA für Android, F-Secure Mobile Security

15. Welche vier Möglichkeiten der Datensicherung kennen Sie?

Am Server, per Cloud Speicher, Festplatte oder SSD (am Computer oder Smartphone), externe Speichermedien wie USB-Stick, SD-Karte, SSD-Speicher oder externe Festplatte

16. Was versteht man unter doppelter Datensicherung?

Bei der doppelten Datensicherung werden einzelne, wichtige Daten auf einem zweiten oder sogar dritten Medium - wie einem Cloud-Speicher, einer externen Festplatte oder einem USB-Stick - abgespeichert. Geht die Originaldatei verloren oder wird sie beschädigt, kann auf die Kopien der Datei zurückgegriffen werden.

17. Was versteht man unter dem Begriff Backup?

Ein Backup beschreibt die doppelte Sicherung von Daten und Programmen oder Apps von einem Computer, Server, Smartphone oder Tablet mit Hilfe einer speziellen Software. Am Computer kann sogar eine komplette Spiegelung bzw. Kopie des gesamten Datenvolumens über ein sogenanntes Image erstellt werden.

18. Erklären Sie den Begriff Datenschutz?

Beim Datenschutz geht es um den Schutz der persönlichen Rechte bei der Verarbeitung von Daten von Menschen (Rechtsbegriff = natürliche Person) oder Personenvereinigungen (Rechtsbegriff = juristischen Personen). Jeder Mensch oder Personenvereinigung hat demnach das Recht und den Schutz auf Privatsphäre selbst zu bestimmen, ob die eigenen Daten verarbeitet werden dürfen oder nicht.

19. Welche Rechte in Bezug auf Datenschutz hat jeder Mensch und jede juristische Person?

Recht auf Geheimhaltung (§ 1 Abs. 1 DSG 2000)
Recht auf Auskunft (§ 26 DSG 2000)
Recht auf Richtigstellung oder Löschung (§ 27 DSG 2000)
Recht auf Widerspruch (§ 28 DSG 2000)