Sicherheit Lektion 1
Grundlagen zu Daten und Sicherheit

- Sicherheitsbewusstsein
- Datenbedrohung
- Wert von Informationen
- Sicherheitsstrategien und 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

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 Passwortstrategie?
- 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 Freunde 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 EKZ öffentlich?

Im Netz verhält es sich genauso.

- E-Mails und IM (Kapitel 7)
  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?

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.

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* genannt)
- Cyber-Mobbing, Cyber-Terrorismus, Cyber-Stalking, Verhetzung

Hacking – Cracking – ethisches Hacking
Sowohl *Hacker* als auch *Cracker* umgehen die Zugriffsbarrieren zu Netzwerken. Streng genommen sind Cracker in böswilliger Absicht unterwegs. Hacker zeigen Schwachstellen auf. Experten und Expertinnen, die in Systeme eindringen um Sicherheitslücken zu finden, nennt man *ethische Hacker*.

Vis major
Daten gehen unter Umständen durch Feuer, Wasser, andere Umweltkatastrophen oder Krieg verloren. Nur die regelmäßige Datensicherung auf externen Datenträgern

© Daniela Wagner | www.computertraining4you.eu | Autorin, IT-Coachin & Fachtrainerin nach ISO 17024

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.

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 Mitarbeitende sabotieren oder spionieren Daten aus

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.

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 7 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 Kollegen und Kolleginnen das Gehalt anderer Mitarbeiten-den 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.

Das Datenschutzgesetz regelt den Schutz der personenbezogenen Daten. Lesen Sie dazu im Training IKT Kapitel 2 / Lektion 3 nach.

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 denjenigen 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

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 heran-kommen. 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 ihre Opfer, nennt man das *Smishing*. Von *Vishing* spricht man, wenn der Angriff über ein Video Call Programm erfolgt.

© Daniela Wagner | www.computertraining4you.eu | Autorin, IT-Coachin & Fachtrainerin nach ISO 17024

Shoulder Surfing
Haben Sie sich schon mal Gedanken darüber gemacht, wer Ihnen über die Schulter schaut, wenn Sie Geld am Bankomat 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. Sicherheit / Lektion 8).

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 der Identität
Personenbezogene Daten können verwendet werden, um Ihre Identität zu missbrauchen oder gar zu stehlen.

6. Sicherheit für Daten

Prüfen Sie die Makro-Sicherheitseinstellungen und wählen Sie ein sicheres Passwort (vgl. Sicherheit / Kapitel 4). Zusätzlich verschlüsseln Sie wichtige Daten. Dazu vergeben Sie entweder beim Speichern ein Kennwort oder Sie nutzen ein Programm – beispielsweise *Truecrypt* von www.truecrypt.org - zum Verschlüsseln der gesamten Festplatte.

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?

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?

Notizen

© Daniela Wagner | www.computertraining4you.eu | Autorin, IT-Coachin & Fachtrainerin nach ISO 17024