Inhalt

Grundbegriffe zu Sicherheit

In vielen Bereichen des täglichen Lebens wird großer Wert auf Sicherheit gelegt. Im sozialen Umfeld, im Berufsleben, am Arbeitsplatz und auch im Bereich von Partnerschaften und Familie. Aber auch im technischen Bereich ist Sicherheit natürlich ein wichtiges Thema, niemand wird sich heute noch ein Auto ohne Sicherheitsmerkmale wie Sicherheitsgurte, Kopfstützen oder Airbag kaufen.

Wie ist es nun im Bereich der Computertechnologie und Kommunikation mit der Sicherheit bestellt?

Dieses Kapitel beschäftigt sich mit Datenbedrohungen im Allgemeinen, mit dem Wert, den Informationen darstellen und wie Sie die Einflüsse auf persönliche Sicherheit und Sicherheit für Dateien verstehen und verbessern können.

Datenbedrohungen

Beinahe jeder Haushalt ist heute mit dem Internet verbunden. Aber ist dieser Zugang auch sicher, und ist diese Sicherheit auch notwendig? Bin ich selbst Fachmann genug dafür?

Diese Fragen werden sich sicherlich viele Computerbenutzer stellen.

Wenn in einem Haushalt ein Internetanschluss vorhanden ist, dann wird dieser Anschluss meist von mehreren Personen gemeinsam genutzt. Diese Nutzung ist allerdings je nach Person unterschiedlich. So wird das Internet genutzt zum Download von Daten, Kommunikation über Chat-Programme, zum Lesen aktueller Nachrichten, zum Recherchieren von Informationen, Austausch von E-Mails, Überweisungen etc. Das Internet bietet heute eine solche Vielzahl von Möglichkeiten, so dass nur ein Bruchteil davon von jedem Einzelnen genutzt werden kann.

Bei vielen dieser Nutzungsmöglichkeiten ist es notwendig, Formulare auszufüllen und Angaben zur Person oder zum Benutzer zu machen. Zusätzlich gibt es manchmal Fragebögen und Umfragen, die auf Webseiten auszufüllen sind, ehe man auf die gewünschten Inhalte zugreifen kann.

Zu diesem Zeitpunkt spätestens ist es wichtig, zu wissen, **welche** Informationen man preisgibt und **wem** man diese Informationen zur Verfügung stellt.

Dazu ist erst einmal eine grundsätzliche Unterscheidung von Information und Daten hilfreich.

Daten und Informationen

Daten sind im Sinne der Datenverarbeitung maschinenlesbare und -bearbeitbare Zeichen, die in den meisten Fällen auch in digitaler Form gespeichert werden, als Dateien auf einem Computer oder ähnlichen Geräten. Diese Daten sind in einer vom bearbeitenden System vorgegebenen Syntax oder Form gespeichert und unterliegen strengen Regeln. Diese Daten können dann von geeigneten Programmen in Bezug gesetzt und interpretiert werden. Dadurch können Daten auch weiterverarbeitet werden und die darin enthaltenen ***Informationen*** unterschiedlich verwendet und ausgewertet werden. Gespeichert werden Daten in den meisten Fällen in binärer Form, in so genannten Bits (binary digit). Ein Bit ist dabei die kleinste Einheit. Diese bilden ein Muster, welches interpretiert wird und dann zusammengefasst Informationen ergibt. Die unterschiedlichen Gruppen von Daten werden als Datenfelder, Datensätze, Dateien, Ordner oder auch Datenbanken bezeichnet.

Datenschutzrechtlich betrachtet, sind Daten, mehr allgemein formuliert, Informationen, die einer bestimmten Person zugeordnet werden können. Information ist damit eigentlich ein Überbegriff, und die Informationen, die im Internet zur Verfügung gestellt werden, sind sehr umfangreich. Das ist solange harmlos, solange die Angaben, die ein User auf einer Internetseite in einem Formular macht, nicht eindeutig dem User zugeordnet werden können. Und auch wenn dies der Fall ist, ist das noch kein Problem, solange der Herausgeber des Formulars vertrauenswürdig ist.

Wenn also auf einer Webseite die Aufforderung erscheint, vertrauliche Informationen wie PINs oder Bankzugangsdaten, Kennwörter etc. einzugeben, und das ist nicht die Webseite der Bank des Vertrauens, dann sollten die inneren Alarmglocken läuten. Die Zugangsdaten zur Bank sind die persönlichen Daten, die für die Sicherheit der Verbindung garantieren,

und die sollte nur der Besitzer des Kontos kennen, und nicht die große Gemeinschaft der Internet Fans einer bestimmten Webseite.

Ob es für Dritte interessant ist, jemandes Lieblingsspeise oder Lieblingsgetränk zu kennen, kann jeder für sich beurteilen. Allerdings darf nicht vergessen werden, dass auch aus scheinbar harmlosen Informationen, die nicht direkt einer bestimmten Person zugeordnet werden können, im Laufe der Zeit, durch viele Umfragen und durch Zusammentragen und Auswerten dieser Informationen ein Bild entstehen kann, das Rückschlüsse auf die Person und deren Verhalten zulässt. Dann werden aus vielen harmlosen Informationen plötzlich sehr persönliche Informationen, die vielleicht so nicht für andere bestimmt sind.

Was kann nun mit Daten und Informationen geschehen, und wer kann diese zu welchen Zwecken verwenden?

Es gibt viele Möglichkeiten, die von harmlos bis höchst kriminell reichen und auch echte, schwerwiegende Schäden verursachen können.

Es ist nicht unbedingt zweckmäßig und sinnvoll auf der Webseite eines sozialen Netzes oder in einem Forum zu veröffentlichen, dass man gedenkt, die nächsten drei Wochen auf einer Kreuzfahrt zu verbringen. Man teilt damit nur vielen Leuten mit, dass die Wohnung verlassen ist, und diese in aller Ruhe während dreier Wochen ausgeräumt werden kann. Eine durchaus harmlose Information, für Freunde gedacht, kann auf kriminelle Weise missbraucht werden, um Schaden zu verursachen.

Datenbedrohung durch Internetkriminalität

Wenn das Internet dazu verwendet und missbraucht wird, um sich auf nicht legalem Weg, Zugang zu Daten zu verschaffen oder kriminelle Handlungen zu begehen, dann wird dieses Vorgehen als ***Internetkriminalität*** oder auch ***Cyber-Crime*** bezeichnet.

Die Erscheinungsformen dieser kriminellen Handlungen können sehr vielfältig sein: Internetbetrug, Ausspähen von Daten, Illegales Verbreiten urheberrechtlich geschützter Inhalte, wie Filme oder Musik, sind nur einige Delikte. Auch Terrorismus und ***Cyber-Mobbing*** sind Begriffe die unter Internetkriminalität zu finden sind.

Hacker

Die Personen, die solche Handlungen durchführen oder zum Teil dafür mitverantwortlich sind, werden oft als ***Hacker*** bezeichnet und ihre Handlungen dementsprechend als ***Hacking***. Dabei gibt es mehrere Unterscheidungen von Hackern.

Die ursprüngliche Bedeutung meinte weniger einen kriminellen Zusammenhang, sondern war eine Bezeichnung für Personen, die **technische Enthusiasten** waren und sich in computertechnischen Bereichen ein umfassendes Wissen aneignen konnten. Diese Leute wurden auch dazu genutzt, um Sicherheitslücken aufzuspüren und dann entsprechende Sicherheitsmechanismen zu implementieren.

Hacker agieren mit der Absicht, Schäden zu verursachen, die von ihnen ausgehende Bedrohung ist also **meist** beabsichtigt.

Nicht jeder Hacker dringt in böser Absicht in ein System ein, um es dann in krimineller Absicht zu nutzen. Die Technologien der Hacker werden auch verwendet, um Schutzeinrichtungen zu testen und Sicherheit zu überprüfen. Diese Art des Hackens wird auch als ***Ethical Hacking*** bezeichnet. **Diese** Hacker sind in der Regel vertrauenswürdige Personen und arbeiten für Sicherheitsunternehmen.

Cracker

Ein weiterer Begriff, der mit dem Hacker eng verwandt ist, ist der ***Cracker***. Dabei handelt es sich nicht um ein Gebäck, sondern um jemanden der Sicherheitsmechanismen umgeht. Die bekanntesten Beispiele sind wohl Kopierschutzmechanismen, die umgangen werden und Produktaktivierungen, die ausgehebelt werden, um für Musik oder Programme nichts zahlen zu müssen. Die Handlungen werden dann als ***Cracking*** bezeichnet. Das betrifft eine Vielzahl von Mechanismen und wird leider oft als Sport angesehen. Wer umgeht zuerst den Kopierschutz für das neue Spiel oder Betriebssystem? Dadurch entsteht natürlich sehr hoher finanzieller Schaden und es wird auch sehr viel Geld in die Entwicklung von Schutzmechanismen gesteckt, die allerdings auch nicht immer zielführend sind.

Datenbedrohung durch höhere Gewalt

Aber nicht nur böse Absichten können zu Schäden im Bereich der IT führen. Es gibt auch noch Katastrophen, gegen die man sich nicht so einfach schützen kann, denkt man beispielsweise an Feuer, ein Hochwasser, ein Erdbeben oder sogar an Krieg. Aber auch gegen Datenverlust durch höhere Gewalt können Schutzmaßnahmen gesetzt werden. Gegen Beschädigungen durch einen Brand können Daten beispielsweise geschützt werden, indem eine ***Datensicherung*** (***Backup***) außerhalb aufbewahrt wird, das kann ein Bankschließfach, ein Safe oder einfach eine Zweigniederlassung eines Unternehmens sein. Außerhalb der eigene Räumlichkeiten deshalb, damit im Falle einer Beschädigung nicht Originaldaten **und** Datensicherung verloren sind. Auch für Privatpersonen sind hier recht einfache Schutzmaßnahmen möglich, es muss nicht immer eine teure Lösung sein.

Datenbedrohung durch menschliches Fehlverhalten

Die Sicherheit ist aber leider nicht immer nur von außen bedroht, wie durch Hacker oder Erdbeben, sondern auch von innen. Hacker sind nicht die einzigen Personen von denen eine Bedrohung ausgehen kann.

Leider kann eine **Bedrohung auch durch unbeabsichtigtes Fehlverhalten einzelner Personen** entstehen. Diese Gefahren gehen von Personen aus, die nicht die Absicht hegen, Schaden anzurichten. Ein versehentliches Löschen von Daten durch einen Mitarbeiter oder ein Familienmitglied kann zu Datenverlust führen. Das versehentliche Abziehen eines USB-Sticks, ohne ihn sicher zu entfernen, kann zur Beschädigung des Datenträgers führen und die Urlaubsfotos der letzten Jahre sind verloren. Im Unternehmen kann ein ungeschulter Mitarbeiter versehentlich den gesamten Betrieb lahmlegen, wenn er die falschen Informationen löscht.

Diese Bedrohungen sind schwer zu vorauszusehen und es ist fast unmöglich sich davor zu schützen. Leider wird auf Bedrohungen aus dem täglichen Leben oft zu wenig geachtet. Schon eine kleine Unachtsamkeit wie das Umwerfen eines Glases mit Wasser kann zum Totalverlust eines Rechners und aller darauf befindlichen Daten führen.

Wenn ein Benutzer innerhalb des Unternehmens durch Unwissenheit Fehler begeht und es dadurch zu einem unberechtigten Datenzugriff

kommt, kann das ebenso zu Datenbedrohung führen, wie durch ein falsch konfiguriertes Gerät, z.B. eine Firewall oder ein Internetrouter, der von einem Provider, also von einem externen Dienstleister kommt. Es kann also auch passieren, dass **Betreuung durch externe Unternehmen** zu solchen Fehlern führt. Unbeabsichtigtes Fehlverhalten ist schlimm, kann aber geschehen, noch bedenklicher ist es natürlich, wenn es mit Absicht geschieht, um Schaden anzurichten oder Daten auszuspionieren.

Es geschieht auch in **böswilliger Absicht**, dass ein verärgerter Dienstnehmer, Daten aus dem Unternehmen an Dritte weitergibt, um sich entweder selbst zu bereichern oder um dem Arbeitgeber zu schaden. Nicht zuletzt können auch externe Personen (beispielsweise Kunden) mutwillig oder versehentlich Schaden anrichten und Daten vernichten. Ein Dienstleister, der den Familien PC reparieren soll und nicht weiß, dass die Datenplatte verschlüsselt war und er den Schlüssel bei den Reparaturversuchen gelöscht hat. Auch andere Dienstleister, wie Handwerker oder Lieferanten können mutwillig oder versehentlich Geräte beschädigen und Daten vernichten. Ein Gerät, das von einem externen Dienstleister zur Benutzung zur Verfügung gestellt wird, kann absichtlich falsch konfiguriert sein, denn nicht zuletzt gibt es Organisationen die viel Geld damit verdienen, Daten auszuspionieren und die Informationen zu verkaufen.

Datenbedrohung durch Cloud-Computing

Cloud-Computing macht es möglich, Daten über das Internet jederzeit und von überall zu verwalten. Sie legen Ihre Daten dabei nicht lokal auf einer Festplatte ab, sondern im Internet auf einem Server, man spricht auch von ***Onlinespeicher*** oder ***Cloudspeicher***. Da heute diese Verwendung von Speicherplatz „in der Cloud“ bereits von vielen genutzt wird, ist auch hier eine gewisse Vorsicht nötig. Wenn diese Dienste falsch eingeschätzt werden, nämlich in gutem Glauben, dass die Daten geschützt sind, kann das zu missbräuchlichem Datenzugriff führen. Denn nicht immer ist der Schutz der Privatsphäre gegeben und nicht immer liegt die Kontrolle beim Benutzer. Es ist also notwendig, darauf zu achten, dass Unbefugte nicht auf die Daten zugreifen können und dass die Zugriffskontrolle vom Benutzer durchgeführt werden kann und nicht vom Anbieter der Dienste.

Daher ist es ratsam, nur vertrauenswürdige Anbieter zu nutzen und genau auf die Datenschutzeinstellungen und Richtlinien zu achten.

Wert von Informationen

Worin liegt nun der Wert der gespeicherten Daten und Informationen? Dieser Wert hängt unter anderem davon ab, ob es sich um Daten einer Person, also persönliche und private Daten handelt, oder ob es Unternehmensdaten sind.

Personenbezogene Daten

Wenn der Computer eines Benutzers mit persönlichen, privaten Daten darauf defekt ist, so sind die Daten (in den meisten Fällen), abhängig von der Art des Defekts, wahrscheinlich verloren.

Wenn eine Datensicherung existiert, können sie allerdings wiederhergestellt werden.

Was aber, wenn Daten zwar nicht verloren gehen, aber von Dritten missbräuchlich genutzt werden?

Die Möglichkeiten, Daten einer Person betrügerisch zu verwenden, sind vielfältig. Die Palette reicht von einfachen E-Mails, gesendet im Namen eines Dritten, bis hin zum Missbrauch des E-Banking Zugangs und damit verbundenem Plündern des Bankkontos.

Deshalb ist es notwendig, die verschiedenen Bedrohungen zu kennen und sich davor so gut es geht zu schützen. Wenn ein Dritter Zugang zu sensiblen, persönlichen Daten bekommt, so kann er die Identität der Person annehmen und als diese agieren. Diese Form des Missbrauchs personenbezogener Daten wird im Allgemeinen als ***Identitätsdiebstahl*** oder ***Identitätsmissbrauch*** bezeichnet. Je mehr Daten über die Person dabei genutzt werden können, umso leichter ist es, sich als diese auszugeben.

Wichtige Daten in diesem Zusammenhang:

Name, Geburtsdatum, Wohnadresse, Sozialversicherungsnummer, Führerschein- und Reisepassnummer, Fahrzeugdaten, Kontonummer, Kreditkartennummer etc.

Sie sollten sich bewusst sein, dass mit solchen Daten wichtige Informationen über eine Person ausgewertet werden können, die von großem Wert sind. Gehen Sie daher mit Ihren Daten sorgfältig um, vermeiden Sie es,

Ihre Daten weiterzugeben bzw. geben Sie Ihre Daten nur an wirklich vertrauenswürdige Dritte weiter.

Firmendaten

Ein Datenmissbrauch, betrifft nicht nur Personen, auch Unternehmen sind diesen Risiken ausgesetzt, sogar noch in einem viel größeren Ausmaß. In Unternehmen gibt es ungleich mehr Daten, die einen enormen Wert darstellen und die daher vor Diebstahl oder betrügerischer Verwendung zu schützen sind. Auch Datenverlust und Sabotage können die Folge sein.

Wichtige Daten in diesem Zusammenhang:

Personaldaten, Kundendaten, Finanzdaten, Patentschriften, Forschungsdaten, Produktionsdaten, Verträge etc.

Schutz durch Passwörter und Verschlüsselung

Die Frage, was gegen Datenmissbrauch unternommen werden kann, stellt sich für das Unternehmen genauso wie für die einzelne Person.

Eine Maßnahme ist eine ***Zugangsbeschränkung***, indem man den Zugang zu Daten auf einen bestimmten Personenkreis einschränkt. Damit kann der Datendiebstahl schon grundsätzlich vermieden werden.

Solche Zugangsbeschränkungen können vielfältig sein. Ziel ist es aber generell, dass nicht jeder an einem Computer arbeiten kann und Zugriff auf Unternehmensdaten bekommen soll. Im Netzwerk sollten sensible, vertrauliche Ressourcen außerdem nur bestimmten Gruppen von vertrauenswürdigen Mitarbeitern zu Verfügung stehen.

Sensible Daten können zusätzlich ***verschlüsselt*** gespeichert sein, so dass ohne geeignetes ***Kennwort*** oder passendem Schlüssel ein Zugriff auf die Daten nicht möglich ist. ***Verschlüsselung*** ist ein Vorgang, bei dem Daten in einen unlesbaren Geheimtext umgewandelt werden. Durch eine ***Entschlüsselung*** werden die Daten dann wieder lesbar gemacht. Hier können verschiedene Verfahren genutzt werden, die zwar zum Teil erheblichen Aufwand verursachen, aber eine entsprechende Datensicherheit gewährleisten.

Datensicherheit

Datensicherheit ist dann gegeben, wenn einige grundlegende Merkmale erfüllt sind, wie Vertraulichkeit, Integrität und Verfügbarkeit.

Vertraulichkeit

Vertraulichkeit ist der Schutz der Daten vor dem Zugriff durch Unbefugte. Die Daten sollen nur von berechtigten und vertrauenswürdigen Benutzern gelesen und bearbeitet werden können.

Integrität

Die Integrität der Daten ist dann gewahrt, wenn Daten, davor geschützt sind, missbräuchlich **verändert** zu werden. Ein solches unbefugtes Verändern von Daten und Informationen schränkt die Glaubwürdigkeit stark ein.

Verfügbarkeit

Dass wichtige Daten bei Bedarf verfügbar sein müssen, klingt eigentlich selbstverständlich, ist aber nicht immer gegeben.

Wenn nun beispielsweise unberechtigte Dritte unbefugt Daten löschen und verändern können, dann sind gleich alle drei grundlegenden Merkmale der Datensicherheit nicht mehr gegeben.

Datenschutz

Der Datenschutz regelt den Schutz vor dem Missbrauch personenbezogener Daten. Er basiert auf dem Gedanken, dass jeder selbst entscheiden kann, wann er wem welche persönlichen Daten zukommen lassen will. Der Datenschutz hat in den letzten Jahren immer mehr an Bedeutung erlangt, nicht zuletzt durch die weit verbreiteten Technologien der elektronischen Datenverarbeitung und des Internets.

Grundsätzlich dient der Datenschutz sowohl dem Einzelnen als auch Firmen. Dabei entsteht allerdings ein Konflikt mit den Interessen der Kriminalitätsbekämpfung, die mitunter Zugriff auf gesammelte Daten benötigt. Dabei müssen **die allgemeinen Grundsätze des Datenschutzes**, des Schutzes der Privatsphäre, der Datenaufbewahrung und Datenkontrolle