Datensicherheit

Definition

Allgemein versteht man unter Datensicherheit

die Vertraulichkeit (nur autorisierte Benutzer haben Zugang zu übertragenen und gespeicherten Daten),

die Integrität (Schutz vor beabsichtigten oder unbeabsichtigten Veränderungen), die Verfügbarkeit (Gewährleistung des ständigen Zugriffs auf die Daten) und

die Kontrollierbarkeit (Prüfung der Maßnahmen durch Protokollierung). Datensicherheit hat also zum Ziel, beliebige Daten vor Schäden wie Manipulation und Nicht-Verfügbarkeit schützen.

Hierzu zählen unter anderem **Aspekte** wie die physische Sicherheit, der Schutz vor Fremdzugriffen, der Schutz vor internen Zugriffen, die Verschlüsselung der Kommunikation, die Datensicherung wie auch Updates und Patches.

Beispiele

Sicherheitsmaßnahmen können beispielsweise durch Verschlüsselungs- bzw. Kryptographieverfahren, Firewalls, Virenscanner, Backups oder Protokollierung getroffen werden.

Datensicherheit ist eine Illusion

Elektronisch erfasste Daten scheinen nirgends sicher zu sein. Selbst die Rechner von Nachrichtendiensten und Regierungen werden gehackt. Ist Datenschutz eine Alibi-Veranstaltung?

Datensicherheit ist eine Illusion. Gerade deshalb ist Datenschutz notwendig und die unbedingte Voraussetzung dafür, dass Sicherheitsprobleme nicht in Katastrophen münden.

Bibliotheken speichern haufenweise Daten ihrer Nutzer. Was sollten sie beachten, um Katastrophen zu vermeiden?

Es gibt niemals hundertprozentige Sicherheit. Das bedeutet, dass alle Systeme potenziell löchrig sind. Deshalb sollten Daten gar nicht erst gespeichert werden, und wenn doch, dann nur die Daten, die unbedingt benötigt werden. Zudem sollte eine Speicherung niemals an einem zentralen Ort stattfinden. Beispiel: Wird die Kundendatenbank einer Stadtbibliothek »geklaut«, sind nur die Kundinnen und Kunden einer Bibliothek die gelackmeierten. Das ist schon schlimm genug. Wird dagegen ein Zentralrechner der »Weltbibliothekennutzerverwaltung« angegriffen, sind alle Daten aller Menschen, die je eine Bibliothek nutzten, in schmutzigen Händen.

Das heißt, auch wer sich an die rechtlichen Regelungen hält und technische Schutzmaßnahmen anwendet, hat letztlich keinerlei Garantie dafür, dass seine elektronisch gespeicherten Daten sicher abgelegt sind?

Exakt. Wir können technische Hürden schaffen, aber es könnte sich immer jemand finden, der diese Hürden locker überspringt.

Was hat das wiederum für Konsequenzen für Einrichtungen, die sensible Daten speichern – wie zum Beispiel Bibliotheken?

Kant lesen! Kategorischer Imperativ! Im Ernst: Ich muss mir als Entscheiderin oder Entscheider einer Bibliothek erst einmal gewahr sein, dass ich die verdammte Verpflichtung habe, die mir anvertrauten Daten zu schützen. Und ich muss mich solange weiterbilden, bis ich wirklich begriffen habe, warum diese Daten so schützenswert sind. Denn erst dann lerne ich, dass ich eher ein Merkmal »volljährig« speichere als ein Geburtsdatum, dass ich Bücherlisten physisch lösche und nicht aufbewahre, weil es doch interessant sei, »nach ein paar Jahren noch mal sehen zu können, was man gelesen hat«.

Wie lange sollten Kundendaten überhaupt in einer Bibliothek gespeichert bleiben?

Gar nicht. Vielleicht, solange ein Buch ausgeliehen ist. Aber sobald es wieder da ist: Restlos löschen! Name und Adresse muss auch nicht gespeichert sein. Kann auch auf dem Ausweis stehen und wird nur temporär erfasst, solange ein Buch ausgeliehen ist. Mir würden da einige Szenarien zur Verbesserung einfallen.

Gehört die Speicherung von Daten in der Cloud auch dazu?

Ganz sicher nicht. Die Leitung einer Bibliothek, die dem Speichern von Daten in der Cloud zustimmt, gehört unehrenhaft entlassen.

Unabhängig davon, ob die Cloud-Daten in Deutschland, Europa, USA oder in anderen Ländern gespeichert sind?

Spätestens seit Edward Snowden wissen es alle: Das macht keinen Unterschied.

Wie sieht es mit der Sicherheit beim Szenario »RFID-Technik« aus?

RFID und Datenschutz schließen sich aus. So einfach ist das.

Viele Bibliotheken lagern das Thema Datenschutz an externe Dienstleister aus. Sind sie damit aus dem Schneider?

Sie haben nicht wirklich geglaubt, auf diese Frage etwas anderes als »nein« zu hören? Ich muss schon den Mut haben, mich meines eigenen Verstandes zu bedienen. Das bedeutet, dass ich nicht einfach »passt schon« sagen darf, sondern

dass ich mich selbst informiere und dann erst entscheiden kann, ob mein Dienstleister überhaupt selbst qualifiziert ist. Allerdings wird RFID nicht dadurch datenschutzfreundlicher, indem ich einen Dienstleister beauftrage, »RFID datenschutzfreundlich umzusetzen« und der mir das mit seiner Unterschrift bestätigt. Datenunsicherheit wird nicht dadurch besser, dass ich die Gefahren weglüge oder selbst die Augen davor verschließe.

Datenschutzbeauftragte haben haufenweise gute Ratschläge und kommen im Wettlauf mit den Datenabzockern dennoch regelmäßig hinterher. Was können sie überhaupt ausrichten?

Die amtlichen Datenschutzbeauftragten haben schon einige ordnungsrechtliche Mittel, die sie einsetzen könnten. Datenschutzbeauftragte von Firmen und Behörden haben auch einige Druckmittel, die sie verwenden können. Uns erzählte mal jemand, dass er seinem Chef nur sagen musste, dass »wir als Firma ja keinen Big Brother Award bekommen« wollen – und seither darf er bei Planungstreffen zu Produktentwicklungen gleich mit am Vorstandstisch sitzen.

In Europa soll nun ja alles besser werden. Die Europäische Union ist momentan dabei, mit einem Entwurf für die Datenschutz-Grundverordnung den Datenschutz komplett neu zu regeln. Ist das die Lösung?

Es bleibt abzuwarten, wie sehr dieser Entwurf vor der Verabschiedung noch verwässert wird.

Warum wird in Brüssel gerade beim Datenschutz so wenig auf die Interessen der Verbraucher geachtet?

Verbraucherinnen und Verbrauchern – ich spreche lieber von im Lande lebenden Menschen – ist ihre wichtigste Lobby abhandengekommen: die Parlamente. Deshalb rate ich vielen Menschen, sich auch mit Geldspenden und Mitgliedschaften neue Sprachrohre zu schaffen, die für Grundrechte in der digital vernetzten Welt kämpfen. Deshalb bauen wir meinen Verein »Digitalcourage« zu einer großen NGO, also Nichtregierungsorganisation, aus.

Das neue EU-Gesetz will den bisher wichtigsten Grundsatz bei der Datenerhebung, die Zweckbindung, also die Prämisse, dass Daten nur zu einem zuvor vereinbarten Zweck verwendet werden dürfen, aufheben. Was hätte das für Folgen?

Ich hoffe, dass wir das noch verhindern können. Denn dies liefert uns allen Datenkraken hemmungslos aus. Stellen Sie sich vor, dass Sie auf der Straße alle paar Meter angestarrt, taxiert, angesprochen, angebettelt werden und jemand Ihnen etwas verkaufen will. Statt – bildlich gesprochen – den kurzen Weg zum Bahnhof in 10 Minuten zu gehen, brauchen Sie nun 30 Minuten. Das wirft uns kulturtechnisch mindesten 500 Jahre zurück.

Wie können Volksvertreter auf so eine Idee kommen?

Cherché d‘Argent: Organisationen haben zu wenig Geld, um genügend gegen die Industrie- und Finanzmarktinteressen »anlobbyieren« zu können. Hinzu kommt: Es hat noch kaum jemand die IT-Revolution wirklich verstanden. Digitale Äpfel lassen sich nun mal nur schwer mit analogen Birnen vergleichen. Da fällt es nicht leicht, die richtigen Prioritäten zu setzen.

10 Gebote zum Datenschutz und zur Datensicherheit

Die Verbindung
Wähle deine Verbindung ins Internet sorgfältig – wenn WLAN, dann abgesichert. Wenn man im Intranet der Firma oder im Internetcafe seine Mails liest, bitte nur über sichere, also SSL, Verbindungen. Fühle dich nicht sicher, du bist es nicht – jeder Netzwerkknoten kann heute kinderleicht mitgeschnitten werden. Zuhause gehört immer ein Router mit einfacher Firewall hingestellt, wer keine Antivirus-Lösung und keine Software-Firewall nutzt, hat am/im Netz nichts verloren.
Angabe von personenbezogenen Daten.

Datensparsamkeit ist nicht nur ein Prinzip für verarbeitende Stellen: Es gilt auch für Betroffene. Gib nur das Minimum an, das man braucht. Und: Gewinnspiele und Rabattsysteme braucht man nicht – vor allem brauchen die Betreiber dazu nicht Daten von dir, wie deine Telefonnummer oder deinen Geburtstag.
Wenn es nicht anders geht, überlege erstmal, ob dir die Bestellung oder Registrierung wirklich so wichtig ist. Wenn es vor Ort ist, wo du was unterschreiben sollst: Frag nach, warum du etwas z.B. mit Personalausweisnummer versehen musst. Hast Du das Gefühl lästig zu sein? Nimm es als Kompliment.

Eingabe von personenbezogenen Daten

Wenn Du irgendwo personenbezogene Daten eingibst, etwa Login-Informationen oder Konto- bzw. Kreditkartendaten, tue es nur über eine sichere Verbindung. Tue es nur, wenn unbedingt nötig. Gib deine Kontodaten am besten nie her, bezahle Bar oder bestelle via Rechnung/Nachnahme. Lass dir nichts erzählen: Auf Rechnung zu bestellen ist auch nicht unsicherer für den Verkäufer als eine Lastschrift – die Lastschrift kannst du ja zurückweisen.

Achte immer darauf, verschiedene Passwörter zu nutzen – wenn Dir das zu kompliziert ist, arbeite mit meinem 3-Kategorien-System.

Ausloggen und löschen

Logge dich nach einem Login stets wieder aus. Niemals eine Seite einfach verlassen, immer ausloggen, ausnahmslos. Lass den Cache eines Browsers immer löschen, nicht nur, aber vor allem in offenen Zugangspunkten wie in einem Internetcafe oder einem Arbeitsrechner: Prüfe ob Formulareingaben gespeichert werden. Wenn Du nicht weißt

wie das geht: Informiere dich bevor du an öffentlich zugänglichen Rechnern sensible Daten deinerseits verwendest. Du gefährdest dich selbst.

Keinen Fuss in der Tür: Mails

Stell dir vor ein schmieriger Vertreter steht vor deiner Haustüre und sobald du öffnest schielt er in dein Haus und macht Fotos – das in der Art machen heute schon Mails, die ungehindert (versteckte) Bilder aus dem Netz nachladen. Konfiguriere dein Mailprogramm so, dass interaktive Mails nicht einfach angezeigt werden. Lösche was Schrott ist, ohne es zu öffnen. Wenn Du ein Paket ohne Absender erhältst das tickt (oder vibriert), wirst du es niemals öffnen – wende die Intelligenz auch bei Mails an.

In der heutigen Zeit ist jeder in der Lage, personenbezogene Angaben anderer zu verarbeiten: Schreibst Du in Webforen über deinen Nachbarn oder Arbeitskollegen? Schreibst Du dabei seinen Namen aus? Wen hast du in deinem Handy gespeichert? Sei nicht so naiv zu glauben, das interessiert keinen. Die Zeiten sind vorbei.

Kaufen mit Spuren dank Kartenzahlung

Kartenzahlung macht Spaß: Einfach und schnell, was will man mehr? In einem aktuellen Urteil wurde wiedermal bestätigt, dass das „PIN Verfahren sicher ist“ – wenn deine Karte missbraucht wird, hast du erstmal ein Problem vor deutschen Gerichten. Also überlege dir, wie vielen Dritten du Zugriff auf die Karte gibst. Tust du nicht?

Woher weißt du denn, dass das Gerät beim Discounter das dir unter die Nase gehalten wird, nichts dazwischen geschaltet hat: Deine Pin tippst du ja immerhin ein und der Magnetstreifen wird auch durchgezogen.

Abgesehen davon, dass diese Daten in digitaler Form bei Händler und Bank über Jahre Hinweg aufbewahrt werden. Bar zahlen ist nicht paranoid, es ist praktisch und hilft zudem, einen Überblick über Ausgaben zu behalten. Nutze etwas Nostalgie.

Tipp am Rande: Ich lasse einmal jährlich meine bis dahin aktuellen Kreditkarten sperren und mir neue (mit neuer Kartennummer) erteilen.

Nur zur Sicherheit.

Denke daran, dass heute faktisch jede Kartenzahlung gespeichert wird und wir zur Lebens-Vorratsdatenspeicherung tendieren.

Kaufen mit Spuren dank Registrierung

Jeder kennt es: man kauft ein Gerät, etwa eine Kamera, und muss sich damit online registrieren. Dann gibt es „tolle Extras“ und „wahnsinnigen Support“. Oder einen Brief von der Staatsanwaltschaft, etwa wenn man seine Kamera weiterverkauft und jemand dann damit ein Buch vor der Veröffentlichung fotografiert, wobei in den EXIF Informationen des Bildes die Seriennummer der Kamera steht. Das ist keine Fiktion, sondern geschah so als der Harry Potter Band 7 plötzlich im Internet auftauchte.

Wenn es nur „langweilige Daten“ sind, die man angibt: Warum machen sich die Unternehmen dann die Mühe, aufwändige Registrierungsverfahren oder bundes- bzw. weltweite „Rabattsysteme“ zu schaffen? Warum gibt es inzwischen für jedes noch so kleine Gerät eine einmalige Seriennummer? Und sollte es am Ende nicht selbstverständlich sein, Support erwarten zu können, auch ohne dass man sich registriert? Vielleicht muss man auch dieses Verhalten der Wirtschaft nicht unterstützen.

Lass das Handy mal zu Hause

Das Handy ist schön: Wir sind immer erreichbar. Wir können damit sogar gegen unseren Willen abgehört und lokalisiert werden – teilweise so einfach, dass es jeder mit der entsprechenden Software aus dem Internet könnte. Vielleicht mal hin und wieder ausgehen und das Handy zu Hause lassen. Einfach mal so, auch um selber zu merken, dass es nicht weh tut, mal ein paar Stündchen nicht erreichbar zu sein. Geht auch, versprochen.

Kenne und nutze deine Rechte

Informiere dich. Lies Blogs und Nachrichten, behalte einen Blick auf das, was geschieht. Wenn Du Fragen hast: Frage. Frage in Blogs, frage die Datenschutzbeauftragten der Länder und des Bundes. Lass Dir nichts erzählen: Du hast etwas zu verbergen. Und Du kannst auch diskutieren. Keinesfalls lass dich einschüchtern, auch nicht am Straßenrand.
Du hast Rechte, die man dir nicht nehmen kann, sagt der §6 BDSG und die musst du mindestens kennen. Frage regelmässig bei Firmen, was über dich gespeichert ist, lass dich nicht abwimmeln und lasse deine Daten dort löschen wo du sie nicht mehr als nötig ansiehst. Wenn dir einer quer kommt: Ruf den Datenschutzbeauftragten an. Wehre dich, sei mündig und aufgeklärt.

Aktualisierte Broschüre: "Sicher unterwegs im Netz"

Etwas im Internet nachschlagen, online einkaufen, per E-Banking bezahlen oder mit Freunden chatten - jeder Klick im Netz hinterlässt Spuren. Doch alle Informationen, die Nutzer über sich preisgeben, können missbraucht werden. Die Broschüre gibt Tipps, wie jeder sich vor Datenmissbrauch schützen kann.

Datenschutz fängt im Kopf an

Jeder sollte genau überlegen, welche persönlichen Angaben er im Netz hinterlässt. Die Broschüre "Sicher unterwegs im Netz" informiert darüber, wie geeignete Passwörter und andere Maßnahmen verhindern können, zu viel über sich preiszugeben.

Hilfreiche Tipps gibt es auch, um sich gegen ungewollte Werbung, sogenannte Pishing-Mails und Spam zu wehren. Ein weiteres Kapitel ist der Frage gewidmet, wie Nutzer sich vor Schadprogrammen schützen können.

Darüber hinaus informiert das Prospekt auch über die Maßnahmen der Bundesregierung zum digitalen Verbraucherschutz.

Die Broschüre können Interessierte als Download herunterladen oder in der Printversion bestellen.
https://www.bundesregierung.de/Content/DE/Artikel/2016/06/2016-06-08-broschuere-datensicherheit.html
Mittwoch, 8. Juni 2016

Datensicherheit

Schutz vor Verlust und Diebstahl von Daten

In einer digitalen Welt, die durch das Internet weltweit verbunden ist, wird die Sicherung von sensiblen Daten immer wichtiger.
Der Missbrauch von Hacking-Methoden findet im enormen Umfang durch wirtschaftliche Unternehmen, aber auch durch der Kontrolle enthobene Regierungsapparate statt, wie die Aufdeckung u.a. durch Whistleblower und Ex-NSA-Mitarbeiter Edward Snowden bekannt wurde.

Der Anbieter für Software-Schutz McAfee bezifferte den weltweiten Schaden, der durch die Verletzung der Datensicherheit durch Datenklau oder Cybercrime entstehen würde mit 400 Milliarden US-Dollar jährlich.

Gründe und Ursachen für Datenverlust

Back-up und Cloud

Datensicherheit bedeutet zum einen die Sicherung von Daten vor Verlust, aber auch die Möglichkeit bei zerstörter Hard- oder fehlerhafter Software Daten wiederherzustellen. Auch Schutz vor Viren oder Datenklau ist Datenschutz.
Während Datensicherheit im Sinne eines Back-up relativ leicht und auf vielerlei Arten lösbar ist, ist Datensicherheit im Sinne des Datenschutzes immer schwerer zu gewährleisten.

Die Verletzung von Datensicherheit

Datensicherheit bedeutet für viele Menschen Informationssicherheit und Datenschutz, aber auch die Ahndung und Verfolgung bei Missbrauch und Datendiebstahl.

Noch fehlt es an einem schlüssigen und gesetzlich verankerten Datensicherheitskonzept, dass auch weitreichend, vielleicht sogar global bindend wäre. Für eine weltweite Verunsicherung und Empörung und einer Verletzung von Datensicherung in gigantischen Ausmaß, sorgte die weltweite Datensicherung durch die US-amerikanische Behörde für Spionage, Verschlüsselung und Entschlüsselung, die National Security Agency, kurz NSA, bei der sogar die Handys von Regierungschefs demokratischer Staaten, darunter auch Kanzlerin Angela Merkel, abgehört worden waren.

Wer gewährleistet Datenschutz?

Das Thema Datenschutz umfasst sowohl rechtliche, organisatorische als auch technische Aspekte. Aber auch rechtspolitische Fragestellungen, wie der Umgang mit Daten und Information auf nationaler und internationaler Ebene müssten geregelt werden.

Involviert sind dabei die Forschung und die Politik, Verantwortliche für Datenschutz und Datensicherheit in Unternehmen und Behörden: Techniker und Juristen, IT-Praktiker und Wissenschaftler, Softwareentwickler und IT-Sicherheitsbeauftragte sowie betriebliche und behördliche Datenschutzbeauftragte und natürlich auch jede Privatperson, die Datensicherheit z.B. für Cloud oder Dropbox und wünscht.

Gründe und Ursachen für Datenverlust

Mögliche Gründe für Datenverlust

- Technischer Systemausfall
- Systemmissbrauch, durch illegitime Ressourcennutzung, Veränderung von publizierten Inhalten, etc.

- Sabotage
- Spionage
- Betrug und Diebstahl

Ursachen und Mittel

Back-up und Cloud

Datensicherheit oder auch Informationssicherheit sollte für die Informationsverarbeitenden und die Informationslagernden bzw. -speichernden Systeme gelten.

Wer große Mengen Daten speichern will oder muss und wer Zugang zu seinen Daten über unterschiedliche Endgeräte haben möchte, nutzt oft eine sogenannte Cloud.

Endgeräte untereinander aktualisieren sich durch einen Back-up und können Daten aktualisieren. Da diese Daten dann extern gespeichert oder auf privatwirtschaftlichen Servern gespeichert werden, muss das Vertrauen der Anwender und Kunden in die Datensicherheit gewährleistet sein.

Immer mehr Unternehmen gehen dazu über, die Daten nur noch auf den direkten Endgeräten der Kunden zu speichern, nicht mehr auf Zwischenstationen.
Im Transfer werden Daten verschlüsselt, sodass ein fremder Zugriff nicht möglich ist.

Eins lässt sich mit Sicherheit sagen: Hundertprozentige Sicherheit gibt es heute für keinerlei Daten.

Susanne Schwab, Arbeitsstand 20.11.2016