Citizen

Somebody is watching you!

Security Guide - Part 1

Sprachversion: Deutsch

Louis Melloy

Inhaltsverzeichnis

Louis Melloy

Citizen – Somebody is watching you!

Teil 1

Datenschutz und Privatsphäre

Deutsch

1. Ausführung

2022

artdesign88.com

Vorwort

Auch wenn Informationstechnologie zu meiner täglichen Arbeit gehört, sie mich ernährt und ich dieser viel Positives abgewinnen kann, so muss ich dennoch zugeben, dass sie ebenfalls etwas ist, das am meisten missbraucht und am wenigsten verstanden wird!

Bereits im Jahr 1981 fing ich an, mich mit Personal Computern zu beschäftigen. Ich habe in Universitäten und vielen großen namhaften Firmen zu den unterschiedlichsten IT-Bereichen und Themen unterrichtet. Ebenfalls wirkte ich in einem Projekt in einer Regierungseinrichtung mit und erstellte dort ein Konzept für die Rechteverwaltung. Ab etwa 1996 verlagerte ich meine Neugierde mehr und mehr in Richtung IT-Sicherheit, Internet und Rechte-Management. Inzwischen habe ich in weit über 100 großen IT-Projekten als Berater, Manager und ausführende Hand mitgearbeitet.

Meine jahrzehntelangen Erfahrungen stützen sich auf Tatsachen und viele Projekte, in denen ich tief in der Materie als Planer wie auch federführend mitgearbeitet habe.

Nach und nach stellte ich immer mehr fest, dass IT-Abteilungen wie auch Privatpersonen sowohl mit ihren eigenen wie auch mit Daten ihrer Mitmenschen und Kollegen sehr schlecht bis absolut unmöglich umgehen. Aus diesem Grund entschloss ich mich dieses Buch zu schreiben.

Ich bin guter Dinge, dass Sie meine Worte verstehen werden und auch einen Nutzen daraus ziehen können.

Ich widme mich mit diesen Worten nicht nur an bestimmte Personen, sondern an all diejenigen, die im Trott des Internets und Datenwahns ihre Rechte und Sicherheit aus den Augen verloren haben und damit profitorientierten Datenvermarktern zu immer mehr Reichtum und Macht verhelfen. Dieses Buch ist für alle, die Interesse daran haben, wie es um ihre Privatsphäre bestellt ist und wie sie

ihre Privatsphäre wiederherstellen können, auch wenn es ein längerer Weg wird, einen akzeptablen Zustand zu erreichen.

Die jetzigen Probleme existieren global und nicht nur regional. Wir alle müssen uns vor dem Verlust unserer Daten und dem unserer Privatsphäre schützen, denn ein anderer macht es nicht.

Ich schreibe weder nur für die Europäische Union, Amerika noch für ein einzelnes Land. Wir alle haben das gleiche Problem mit unserer Sicherheit, dem Schutz unserer Daten sowie unserer Privatsphäre. Dies unterscheidet sich sicherlich etwas von Land zu Land, aber das Hauptproblem haben wir alle.

Durch das freizügige Umsichwerfen von privaten Daten wird die Weltbevölkerung in den kommenden Jahren immer mehr zu leiden haben. Das wird viele gravierende und sehr negative Auswirkungen für alle mit sich führen. Das Schlimme daran, die meisten realisieren die dahinter verborgenen Gefahren nicht. Ohne diese gesammelten Daten von all den Menschen sind solche globalen Taten von Reichen und Regierungen nicht möglich.

Leicht- oder gutgläubige Menschen lassen all ihre Freiheit im Internet zurück, indem sie ihre intimsten Geheimnisse offenbaren. Diese intimen und privaten Daten von Millionen Menschen werden zu Zwecken von Profit, Profilgenerierung, Marketing, Manipulation und Verfolgung von einigen Geschäftemachern und Regierungen ausgebeutet.

Wenn wir alle keine Geheimnisse mehr haben, weil alles über uns ausgewertet wird und für jeden online zu sehen ist, dann wird es höchste Zeit, etwas zu ändern. Wir müssen lernen, nicht jedem ohne nachzudenken zu geben, was er von uns wissen möchte.

Denken Sie immer daran: Es gibt nichts kostenlos!

Wir müssen lernen, dass nicht alles harmlos ist, was als solches deklariert wird oder von dem alle behaupten, dass dies der Fall sei. Keine Regierung und niemand innerhalb dieser ist berechtigt, Menschen des Volkes als minderwertig anzusehen, mit ihnen alles noch so erdenklich Abwertende zu tun und seine Mitmenschen auszunutzen. Der Zweck einer Regierung ist meiner Meinung nach ein Volk zu schützen, was aber immer seltener der Tatsache entspricht.

In den vielen Jahren meiner Tätigkeit als Berater und IT-Manager habe ich vieles gesehen und erfahren. Ich sehe (viele Male), wie Firmen all ihr Wissen und ihre internen Prozesse, ohne zu überlegen, online und in einer ›Cloud‹ bei Fremden abspeichern. Geschäftsleute übersetzen vertrauliche Dokumente online über den ›Google Übersetzer‹ oder andere Dienste. Viele Menschen, die ich kenne, schreiben alles, was sie täglich tun, in sogenannten ›Social-Media-Portalen‹ nieder und senden ebenfalls private Fotos und andere Vertraulichkeiten über diese digitalen Wege. Ich sehe immer wieder, wie Zugriffskonten von tausenden Mitarbeitern samt ihrer Passwörter zu Fremden in eine ›Cloud‹ synchronisiert werden. Auf meine Frage warum dies getan wird, erhalte ich Antworten wie: *Wir müssen denen vertrauen.*

Derartige Aussagen zeigen mir, dass hier einiges nicht stimmt!

Privatpersonen wie auch Geschäftsleute speichern Unmengen an vertraulichen Informationen und Daten auf Online-Speicher und auf Systeme in ›Cloud-Umgebungen‹ wie ›DropBox‹ oder ›GoogleDrive‹ ab. Es ist eine Sache, wenn dies Privatpersonen tun, aber eine ganz andere bei Firmen und Personen, die im IT-Bereich arbeiten und es

besser wissen sollten. Mich schockiert immer wieder aufs Neue, dass sich weder die einen noch die anderen um Datenschutz bemühen.

Viele Firmen sind heute pleite und vernichtet, weil deren Bosse und Mitarbeiter alles im Internet hinausposaunen oder Konzeptpapiere online speichern. Denken Sie nur einmal an COVID-19. All dies ist nur mit Daten möglich!

Stellen Sie sich folgende Frage: Wenn ein Freund einen anderen nach seiner Kreditkarte fragt, weshalb gibt dieser Freund dann seine Kreditkarte nicht heraus, aber im Internet oder an der Rezeption im Hotel ohne zu zögern?

Vertrauen wir Fremden mehr als unseren Freunden oder unserer Familie?

Diese Frage sollten Sie sich ehrlich beantworten!

Fast jeder teilt anderen im Internet mehr Informationen mit, als er dies jemals in den eigenen vier Wänden tun würde. Und Millionen Menschen kommunizieren mehr im Internet als mit ihrem Partner. Diesen Zustand nutzen bestimmte Personen aus, und das aus den unterschiedlichsten Gründen. Der Hauptgrund aber ist stets Geld.

Ich sehe immer mehr Online-Dienste, die andere verleiten möchten, ihre Daten online zu übertragen. Sei es für E-Mail-Accounts, Social-Media, Umfragen, sogenannten kostenlosen digitalen Downloads, Musik-Foren, Wegfinder und tausende weitere Angebote fragwürdiger Webseiten. Audio, Video, Texte, Spielstände und vieles mehr sollen wir online konvertieren und auf Systeme Fremder hochladen. Es gibt kaum noch Programme für die Offline-Nutzung. Sind wir es erst einmal gewohnt, Daten ›ins Netz‹ zu speichern, dann gewöhnen wir uns immer mehr daran, stellen immer weniger Fragen und denken immer weniger darüber nach, weshalb das keine gute Idee ist.

Ist das Freiheit? Nein, es ist Abhängigkeit und das genaue Gegenteil!

Ist uns das Online-Verhalten so vertraut und intim geworden, dass wir das Gefühl haben, es sei unsere Familie?

Zum jetzigen Zeitpunkt sehen die wenigsten Menschen, dass sie meist den Feind vor sich haben: *den Wolf im digitalen Schafspelz*.

Geschäftliche sowie sehr intime Vertraulichkeiten werden in E-Mail-Konten gespeichert, von deren Betreibern mittlerweile jeder wissen sollte, dass diese die Inhalte einsehen und auswerten. Und zwar alles, den Text sowie Anhänge darin!

Sobald wir Fotos, Dokumente, Liebesbriefe … auf Systeme fremder Eigentümer speichern, haben noch weitere unbekannte Personen Zugriff darauf und wir sind nicht mehr Herr über unsere eigenen Daten! Auch wenn viele sagen, es sei ihnen egal, was ein anderer von ihnen weiß und sie hätten nichts zu verbergen , bin ich mir sicher, dass dies nur aus Mangel an Überlegung und Unwissenheit gesagt wird oder weil diesen Menschen noch nicht wissentlich etwas Schlimmes wegen Datenmissbrauchs geschehen ist!

Bei Privatpersonen ohne viel Kenntnis in der ›Informations-Technologie‹ kann für solche Aussagen noch ein kleines bisschen Verständnis aufgebracht werden, für Administratoren oder IT-Manager und Personen aus bestimmten Berufszweigen ist das jedoch mehr als unverantwortlich. Solche Personen sind einfach ausgedrückt *fehl am Platze.* Es geht dabei auch nicht nur um uns selbst, sondern auch um nachfolgende Generationen. Es geht um unsere Kinder und deren Kinder!

Wenn jeder wüsste, was wirklich mit all den Daten gemacht wird, mit den eigenen privaten Daten geschieht, würden die gleichen Personen solche inakzeptablen Aussagen nie wieder von sich geben. Durch das Mitmachen von so vielen bei diesem bösen Spiel werden etliche

kompromittiert, die immer wieder unfreiwillig dagegen ankämpfen müssen.

Generell gibt es gesunde und ungesunde Verhaltensregeln. Daten und Informationen über sich selbst und andere Personen im Internet zu hinterlassen, ist eine der schlechtesten überhaupt.

Mit diesem Buch möchte ich Menschen aufklären und warnen. Sie aufrütteln und dazu bewegen, etwas mehr nachzudenken, wenn es um Sicherheit und Datenschutz geht.

Dies ist der erste Guide mit dem Titel:

›Citizen – Somebody is watching you!‹

Diesen Titel wählte ich, weil es genau das ist, was mit Menschen geschieht: Sie werden von anderen zu bestimmten Zwecken beobachtet.

Außerdem bin ich der Meinung, dass Bürger beschützt werden müssen. Beschützt zum einen vor dem E-Commerce (hauptsächlich aus den USA), zum anderen vor Gesetzgebern, die ihre eigenen Bürger nicht genug schützen wollen oder können. Zum Dritten vor Personen, die sich anmaßen, die Welt planen zu können und die sich selbst zur Elite zählen, weil viele Menschen ihnen blind vertrauen. Genau das hat ihnen zu materiellem Reichtum verholfen, was wiederum Grund dafür ist, dass alle anderen Bürger nur eine Zahl auf ihrem Konto darstellen und als Schafe betrachtet werden, die man scheren und schlachten muss.

Nur wenige Menschen entmündigen und entmachten Millionen ihrer Mitmenschen und kaum jemand der Betroffenen begreift dies oder wehrt sich. Regierungen und Opfer unterstützen dies sogar durch viele ihrer Taten! Des Weiteren fördern diese Unternehmen die Cyber-Kriminalität durch die ein oder andere Weise. An erster Stelle aber dadurch, dass deren IT-Umgebungen und Systeme oft nicht

sicher vor Fremdzugriffen sind. Immer wieder gibt es darüber Berichte. Über hunderte Millionen gestohlener Datensätze oder Identitäten aufgrund eines Datenlecks oder fehlerhaft konfigurierter Dienste. Beispiele dazu finden Sie im Anhang und tonnenweise mehr lassen sich im Internet zu diesem Thema finden.

Ob es um die ›DSGVO‹ geht oder wie in den USA das ›CCPA Compliance‹ oder um die Rechte der Bürger in Amerika, Asien, Ozeanien oder Europa: Alle Bürger haben Rechte, die auch wahrgenommen werden sollten. Vor allem müssen diese aber bekannt sein! Ich lege Ihnen ans Herz, die Warnungen in diesem Buch ernst zu nehmen.

Jeder muss natürlich für sich selbst entscheiden, was er oder sie für seine bzw. ihre Privatsphäre bereit ist, zu tun und was nicht. Mir liegt es fern, für Sie zu entscheiden, so wie es die E-Commerce-Giganten täglich tun. Meine Hoffnung liegt auf der versteckten Vernunft derer, die sich nicht als Marionette von anderen benutzen lassen möchten. Dieses Buch ist als Ratgeber zu verstehen. Was Sie daraus machen, bleibt allein Ihnen überlassen.

An vielen Stellen finden Sie Beispiele, Tipps oder Gegenmaßnahmen zu bestimmten Dingen und Themen. Manche Textabschnitte sind als Gedankenreisen (wie ich es nenne) zu verstehen. Diese sind dann mit *GEDANKENREISE* gekennzeichnet. Ich möchte Ihnen im gewissen Sinne Angst einjagen, Sie aufwecken. Ich führe Ihnen verschiedene Szenarien vor Augen und nenne Dinge beim Namen.

Vielleicht gehören auch Sie zu denen, die stets sagen: *Ich habe nichts zu verbergen.* Dann hoffe ich, Sie durch diese Seiten umstimmen zu können und unser aller Sicherheit zu verbessern.

In diesem Sinne: informatives und wirkungsvolles Lesen!

Kapitel 1

Analyse Part 1 – Beweggründe

Fangen wir mit ein paar Fragen an!

Fragen wie diese sollte sich jeder stellen und dazu eine sinnvolle Antwort finden.

Wer, wie, was, wieso, weshalb, warum …?

Als Erstes müssen wir ein paar Dinge analysieren, um zu verstehen, was alles um unsere Daten herum geschieht.

Im Vordergrund und Drehpunkt steht der Mensch. Dann folgen Technik, Rechte und Pflichten, Gesetze.

Die Menschen sind natürlich der wichtigste Part von allem, denn um uns geht es schließlich.

Warum?

Die Frage nach dem Warum kann am schnellsten beantwortet werden: Geld, Profit, Macht und Manipulation.

Wer hat Daten von Ihnen?

Welche Person, öffentliche Einrichtung, welches Unternehmen, Amt …? Haben Sie persönliche Daten freiwillig weitergegeben oder sind die Besitzer über einen anderen Weg an Ihre Daten gekommen? Wenn ja, wurden Sie vorher darüber aufgeklärt?

Weshalb hat jemand Ihre Daten?

Muss er diese besitzen aufgrund von Gesetzen, weil Sie eingekauft haben, vielleicht einen Mitgliedsausweis anlegen ließen oder sind Ihre Daten dort ohne ersichtlichen Grund?

Bei geschäftlichen Aktivitäten ist es meist so, dass nur dann ein berechtigtes Speichern und Verarbeiten Ihrer personenbezogenen Daten erlaubt ist, wenn auch eine

geschäftliche Aktion getätigt wurde. Ist dies nicht der Fall, sind die meisten Unternehmen nicht berechtigt, Ihre personenbezogenen Daten zu besitzen oder gar zu verarbeiten.

Wie genau ist man an Ihre Daten gekommen?

Die letzte Frage ist eine der wichtigsten von all den vorangegangenen in diesem Abschnitt. Aus dem einfachen Grund, da sich die Lösung dahinter verbirgt, wie leicht oder schwer es für andere ist, an Ihre personenbezogenen Daten zu kommen. Haben Dritte Ihre Daten weitergegeben? Gibt es evtl. ein Leck in Form von Plaudertaschen oder Einbrüche bei Unternehmen? Sind Sie selbst die Plaudertasche? Haben Sie einen Virus auf Ihrem elektronischen Gerät? Oder geben Sie nur allzu bereitwillig Ihre Daten weiter, wenn jemand Sie danach fragt?

GEDANKENREISE Start

Durch Anhänge und Links aus E-Mails haben Sie Computerviren auf Ihrem Gerät. Diese Viren besitzen einen Mechanismus, an alle Kontakte in Ihrem Adressbuch eine Nachricht zu senden, um sich weiterzuverbreiten. Öffnet ein Empfänger eine dieser E-Mails und den darin befindlichen Link oder Anhang, installiert sich ein Virus (Programm), der weiteren Schaden anrichtet. Dieser Virus überträgt Daten und Informationen von Ihrem Datenträger an den Angreifer. Oder der Täter verschafft sich Zugriff auf Ihr Gerät via installiertem Tool und nimmt sich, was er kann. Das macht der Dieb, solange er nicht bemerkt wird, und das kann Jahre bedeuten!

Diebe in aller Welt haben jetzt Ihre vertraulichen Texte, privaten Fotos etc. und verkaufen diese weiter oder nutzen Ihre Daten auf verschiedenste Art und Weise, um sich damit zu bereichern.

Sie lassen Ihre elektronischen Geräte mit Internetverbindung Tag und Nacht an, sodass es Angreifer einfach haben, sich jederzeit mit Ihren Geräten zu verbinden. Smart-TV, Amazon-Türklingel, Smartphone, Tablet und unzählige weitere Wege ins Internet. Kriminelle wissen, in welcher Zeitzone Sie sich befinden und schlussfolgern daraus, wann Sie schlafen werden. Somit kann mitten in der Nacht die Datenquelle in aller Ruhe ausgeräumt werden. Durch Zugriff auf Ihr Notebook steuert dies der Feind, wie er möchte. Er aktiviert die Webkamera und inspiziert nun einen Großteil Ihres Heims samt Ihrer Aktivitäten. Das Notebook steht mit geöffnetem Display in Richtung Ihres Bettes. Ihr Feind kann Sie jetzt auf der anderen Seite der Leitung beim Schlafen oder anderem beobachten!

Sie als Betroffener haben keine Ahnung von diesen Vorgängen, keinen geeigneten Schutz noch die benötigte Erfahrung, um sich vor derartigen Aktivitäten zu schützen. Sie denken sich nichts dabei, wenn Sie E-Mails mit Links von Freunden bekommen, was auch der Grund ist, weshalb Sie diese Links anklicken. Der Einbrecher hat sich jetzt bei Ihnen festgefressen und kommt immer wieder, solange Sie nichts dagegen unternehmen. Nachdem Ihre Geräte von Viren infiziert wurden, bauen diese wiederkehrend Verbindungen zu den Systemen der Angreifer auf. Das Stehlen Ihrer Daten findet auf diese Weise über einen langen Zeitraum hinaus statt.

Ihrem unfreiwilligen Kommunikationspartner geben Sie so im Laufe der Zeit viele intime und vertrauliche Informationen, Fotos, Dokumente und Passwörter. Daten über Ihre Kinder, Ihre finanzielle Situation, was Sie demnächst tun werden, wohin und wann Sie in den Urlaub fahren wollen in Form von Terminkalender, Tabellen, Buchungsbestätigungen etc.

Diebe, die es nicht allzu weit zu Ihrem Zuhause haben, entscheiden sich, Ihrem Heim einen Besuch abzustatten.

Alles kein Problem für den Feind, denn er kennt sich bestens mit Ihren Gewohnheiten, Ihren Finanzen und allem Übrigen über Sie aus!

GEDANKENREISE ENDE

Utopie? Nein, ganz und gar nicht. Solche Dinge passieren täglich!

Das kann über Wochen, Monate und Jahre so weitergehen.

Es gibt auch Schadsoftware, die Ihre Tastatureingaben protokollieren und übertragen. Aber nicht nur diese protokollieren Tastatureingaben, auch Facebook und andere Dienste tun oder taten dies.

Kurz zusammengefasst:

Privatpersonen untereinander sind oft der Schwachpunkt in Bezug auf Sicherheit von eigenen und Daten anderer Personen sowie im Umgang mit Elektronik und dem Internet!

Ihr Verhalten sollte in Ihrem Job nicht anders sein als im privaten Bereich, was die freizügige Herausgabe von persönlichen und vertraulichen Informationen angeht. Ebenso die Absicherung Ihrer elektronischen Umgebung vor Diebstahl und Einsicht. Auf Ihrer Arbeitsstelle müssen Sie diverse Unterlagen gegenzeichnen, die von Ihnen als Arbeitnehmer oft nicht richtig durchgelesen oder verstanden werden. In diesen Unterlagen geht es nicht selten um Ihre personenbezogenen Daten und um Ihre Unterschrift zum Einverständnis der bedingungslosen Verarbeitung. Oftmals stehen Texte in solchen Dokumenten, die Sie als Eigentümer Ihrer persönlichen Daten völlig Ihres Eigentums entheben!

Bevor Sie solche Dokumente unterzeichnen, sollten Sie sich diese genauestens durchlesen, verstehen und des

Weiteren immer eine Kopie davon für sich beanspruchen. Je nachdem, wie Sie auf Ihre privaten Informationen achten und um sie besorgt sind, kann das dazu führen, dass vieles davon in die Öffentlichkeit gerät, ohne dass Sie (der ursprüngliche Eigentümer) etwas davon wissen oder ahnen.

Genau wie Privatpersonen möchten auch Unternehmen (vor allen anderen) nicht, dass Geschäftsgeheimnisse an die Öffentlichkeit geraten. Das ist zwar paradox, da die meisten Firmen viele Daten in einer Cloud speichern und damit genau das Gegenteil erreichen, aber so ist es.

Noch schlimmer ist es, wenn jemand Daten von anderen Personen verkauft!

Es ist bei Weitem keine Seltenheit, dass Mitarbeiter bei Versicherungen, Krankenkassen oder andernorts (einmal von Google und Co. abgesehen) Daten von Kunden verkaufen (eigene Erfahrung!). Aber es gibt auch Einbrüche in Gesundheitssysteme, in IT-Datenzentren, bei Hotelketten, bei denen große Mengen an Kundendaten gestohlen werden. Online versteht sich!

Kaum jemand macht sich die Mühe, zu Fuß irgendwo hinzugehen, um dort einzubrechen und an Daten zu gelangen, da es über den elektronischen Weg viel einfacher ist. Nicht zuletzt, weil viele IT-Umgebungen schlecht gewartet und nicht ausreichend vor Angriffen geschützt sind.

Wie auch die Antwort ausfallen mag, wer, wie, was …, einerseits ist der Grund immer mangelndes Wissen und Vertrauen an falscher Stelle durch den ursprünglichen Datenbesitzer und auf der anderen Seite steht fast immer der Profit!

Sollten Sie selbst einen Virus (oder auch mehrere) auf Ihrem elektronischen Gerät haben, ist es an der Zeit, sich um einen guten Schutz zu kümmern. Kaufen Sie nicht gleich das Erstbeste, sondern erkundigen Sie sich zunächst darüber und holen Sie auch über den Hersteller Informationen ein.

Genauso wie das andere schon seit Langem mit Ihnen machen, das machen Sie jetzt mit dem Hersteller der Virensoftware. Im Gegensatz zu ihm sind Sie eine Privatperson. Der Hersteller des Virenprogramms betreibt ein Unternehmen, das Profit machen möchte und deshalb etwas verkauft. Das ist ein sehr großer Unterschied!

Antiviren-Software überträgt ebenfalls Daten ins ›Netz‹. Zudem sammeln die Hersteller dieser Software Informationen von dessen Nutzern. Teils um die korrekte Arbeitsweise seines Programms zu überprüfen, teils um Informationen über nutzende Kunden zu sammeln.

Ein Antiviren-Programm zu installieren reicht aber nicht aus, um sich vor Schädlingen aus dem Internet zu schützen! (Dazu folgt demnächst ein separater Guide.)

Um die eigentliche Frage, wie es dazu kommt, dass Sie Viren auf Ihrem Gerät haben, zu beantworten, muss die Quelle gefunden werden!

Bekommen Sie Viren über ›Social-Media-Plattformen‹ wie Facebook-Kontakte? Per E-Mail? USB-Stick? …? Von jemandem, den Sie persönlich kennen oder einem Fremden? Vielleicht haben Sie kürzlich E-Mails von einem neuen Kontakt bekommen, in denen sich ›Links‹ befanden, auf die Sie geklickt haben, um etwas zu ›downloaden‹ wie zum Beispiel Fotos. Zumindest glaubten Sie, dass dahinter Fotos zum Downloaden seien, in Wirklichkeit aber war es ein Virus.

Was auch immer der Grund war, der Ihnen den Virus beschert hat. Das herauszufinden ist sehr wichtig für Ihre Sicherheit, Privatsphäre und Lernkurve zur Erweiterung Ihres Horizonts.

So gut wie jede installierte Software auf Ihren elektronischen Geräten sendet Daten an den Hersteller, sobald eine Internetverbindung besteht, und das öfter als Sie glauben. Zu unterscheiden gilt dabei, welches der eingesetzten Programme Daten senden muss, damit es ordentlich funktionieren kann, und welches dies tut, ohne dass es notwendig oder gar angebracht wäre. Ein

Unternehmen, das Daten zur Auswertung seiner Software kombiniert, um dieses zu verbessern, benötigt keine personenbezogenen Daten des Nutzers!

Für die Entwicklung von Software ist es hilfreich, viele unterschiedliche Kombinationen von Hard- und Software-Installationen auszuwerten:

- Ist die Funktion gewährleistet?
- Werden Fehlermeldungen generiert?
- Welches Betriebssystem wird genutzt?

Mehr dazu ist überflüssig und sollte von Ihnen der Kategorie ›Datensammler‹ zugeordnet und somit aussortiert werden.

Immer wenn Ihre Daten in fremde Hände geraten, ist die Wahrscheinlichkeit sehr hoch, dass diese missbraucht und/oder verkauft werden, ohne dass Sie etwas davon erfahren. Um herauszufinden, wer Ihre Daten verarbeitet, müssen Sie nur wissen, wer diese besitzt. Jeder, der Daten von Ihnen speichert, wird diese mit 99%iger Wahrscheinlichkeit auch verarbeiten und irgendwie zu Geld machen wollen. Elektronische Güter, die wir anderen freiwillig übergeben, erkennen wir meist nicht als ›Wert‹ an. Daten haben aber immer einen ›Wert‹, welcher für jeden einen anderen Zahlenstand besitzt.

Bestellen Sie etwas im Internet und übermitteln dabei Ihre Adresse, Telefonnummer, Kreditkartennummer und andere Informationen zu Ihrer Person, dann machen Sie das aus freien Stücken, außer jemand hält Ihnen in dem Moment eine Pistole an den Kopf und zwingt Sie dazu (Scherz am Rande).

Meistens haben diese Shops und Märkte im Internet AGB (allgemeine Geschäftsbedingungen) und weitere Schriften, um Ihnen von vornherein die Entscheidung der Selbstbestimmung, was mit Ihren Daten weiterhin getan werden darf, zu nehmen. Die wenigsten Bürger haben die Muse, sich bei einer Bestellung und vor einem Einkauf all diese Dokumente durchzulesen. Das macht es ›Datensammlern‹ leicht, dieses wertvolle Gut anderer zu bekommen, weiterzuverarbeiten und bei Bedarf zu verkaufen. Zumal sie davon viel und ohne großen Aufwand bei Ihren getätigten Käufen erhalten.

Wie sieht es bei öffentlichen Einrichtungen und Ämtern aus?

Diese sind ein weiterer Quell und Anlaufpunkt für Datenpools. Immer wenn Sie in eine Bibliothek, zum Rathaus, zur Fahrzeug-Zulassungsstelle etc. gehen und Informationen über sich in Form von Übertragung Ihrer Adresse, Telefonnummer, Ihres Geburtsdatums und weiterer personenbezogener Angaben preisgeben, geben Sie Privatsphäre von sich an Dritte weiter. Meist an völlig Fremde!

Darüber hinaus wissen weder Sie noch die Person in der jeweiligen Örtlichkeit, wohin all die eingegeben Informationen über Sie und weitere Millionen von Bürgern gesichert und kopiert werden. Personen, deren Aufgabe es ist, den ganzen Tag an einem Arbeitsplatz über einen Computer Daten einzugeben, egal um welche Art von Daten es sich hierbei handelt, kennen meist nicht die weiteren Mechanismen zur Verarbeitung im Hintergrund!

Diese Angestellten machen einfach nur ihren Job, ohne sich Gedanken darüber zu machen, ob die dahinter befindlichen Systeme schlecht gewartet sind oder überhaupt richtig funktionieren.

Der Rechner wird sich im ›Falle eines Falles‹ schon bemerkbar machen. Das passiert leider oft nicht oder zumindest bekommt es derjenige, der die Daten Tag für Tag

eingibt, nicht mit. Jedes Ding hat seine Ansprechpartner und niemand will sich in seine Arbeitsbereiche hineinreden lassen oder gar einen Rat annehmen.

Mitarbeiter der IT-Abteilung kommen oft arrogant und eingebildet daher. Ja, manchmal von ›oben herab‹.

Wieder einmal will am elektronischen Gerät etwas nicht so recht funktionieren. Den IT-Fachmann bittet man aber nicht gern um Hilfe und traut sich selbst nicht so recht etwas zu sagen, um nicht wie ein Trottel beäugt zu werden.

In vielen Unternehmen fühlen und benehmen sich Administratoren, Software-Entwickler, User-Help-Desk, User-Support und wie sie sich alle nennen mögen, als wären sie die Krone im Unternehmen und unersetzbar.

Der eigentliche Sinn solcher Abteilungen ist es, Service zu leisten!

Die Mitarbeiter in einem Unternehmen sind sozusagen Kunden der IT-Abteilungen. Diese wiederum nutzen elektronische Geräte, Software und IT-Prozesse, welche von den Unternehmen eingeführt wurden. Personen, die in IT-Abteilungen arbeiten, sind somit auch Vermittler zwischen den Unternehmenszielen und der eingesetzten Technik. Das ordnungsgemäße Funktionieren eines Unternehmens hängt in großem Maße von reibungslosen Abläufen mit der Technik und den dahinterstehenden Mitarbeitern ab! Was umso mehr verwundert, dass IT-Abteilungen oftmals als eigenständiger Teil im Unternehmen selbst behandelt werden. Diese Sonderbehandlung innerhalb einer gesamten Struktur ist schlichtweg falsch!

Dafür gibt es viele Gründe:

- Als besonders deklarierte Teile einer gesamt agierenden Struktur verlieren Mitarbeiter den Bezug zur

Wertschätzung.

- Eingebildete Personen verlieren das Verständnis zu dem Service, den sie zu leisten haben.
- IT-Abteilungen und innerhalb derer arbeitende Personen neigen dazu, Unmut zu verbreiten.
- Personen mit zu vielen Freiräumen innerhalb einer solchen Struktur sind nicht kontrollierbar (in Bezug auf deren Arbeit).
- Mitarbeiter in separat geführten Abteilungen werden oftmals schlecht geschult, ohne dass die Geschäftsführung etwas davon bemerkt.
- Manager und Führungsebenen kümmern sich zu wenig um diese Bereiche.

Es gibt sehr viele weitere negative Seiteneffekte, welche entstehen können, wenn einzelne Bereiche eines Ganzen in den ›Himmel‹ gehoben werden oder zu wenig Beachtung erhalten. Eines haben diese Punkte gemeinsam, sie schaden dem Unternehmen und letztendlich allen Mitarbeitern!

An dieser Stelle möchte ich Ihnen das Konzept ›CWR-Framework‹ nahelegen, das Sie auf https://artdesign88.com erhalten können. Es enthält außer der einzigartigen Sicht auf Taten auch digitale Dateien, um Ihnen das Verständnis in Bezug auf Qualität in Firmen und im privaten Bereich näher zu bringen.

Die Aufführung solcher Punkte soll verdeutlichen, wie Beweggründe entstehen und welche es gibt. Bei dem vorangegangenen Beispiel geht es um Personen, Mitarbeiter, Bürger, die sich durch spezielle Gegebenheiten so oder so verhalten. Dieses Auftreten wirkt sich auf gewisse Weise negativ auf die Technik und die dahinter

wirkenden Prozesse aus (aber nicht nur). Personen der IT-Abteilungen, die der Meinung sind, dass alles um das Thema Datenverarbeitung nur sie selbst etwas angehen würde und sonst niemanden, stellen oft einen großen Schwachpunkt im Unternehmen dar. Nur weil sich jemand Administrator oder Teamleiter der IT-Abteilung nennen darf, sollte das kein Grund sein, auf Sicherheit, Datenschutz und Privatsphäre verzichten zu müssen.

Wechseln wir die Orte des Geschehens.

Wenn Sie in einem Hotel übernachten und Ihre Kreditkarte und den Personalausweis kopieren lassen (aus Perspektive der Sicherheit eine Katastrophe), geben Sie sehr vertrauliche Dokumente und ein Stück Ihrer Sicherheit und Privatsphäre an völlig Fremde weiter. Von der Sicherheit des Speicherplatzes einmal abgesehen.

Ausweise, Pässe und Kreditkarten durch Dritte kopieren zu lassen, ist etwas, das Sie auf jeden Fall vermeiden sollten!

Gehen Sie zum Autoservice, ist das nichts anderes. Kreditkarteninformationen (Achtung, den Verification-Code könnte sich jemand ebenfalls kopieren, ohne dass Sie es merken), Adresse, Telefonnummer, Geburtsdatum, E-Mail-Adresse, Auskünfte über Ihre Gewohnheiten und Ihr Auto etc. Einiges davon, gerade Details zu Gewohnheiten und Vorlieben einer Person, ist im Marketing sehr begehrt und bei allen, die etwas verkaufen wollen. Bei Google werden E-Mails ausgewertet, um gezielt Marketing betreiben zu können. Google sammelt über verschiedene Dienste auf Millionen von Webseiten Informationen zu deren Besuchern, ohne dass die meisten Besucher dieser Webseiten davon wissen. Google beliefert damit Hunderttausende seiner Kunden wie die zuvor genannten Webseiten-Betreiber mit Informationen über Sie und andere, damit diese wiederum Sie und die anderen manipulieren können.

GEDANKENREISE START

Sie stehen an der Kasse und zahlen mit Kreditkarte. Um Sie herum ebenso Einkäufer, die jetzt gespannt auf die Eingabe Ihres Kreditkarten-PIN-Codes warten. Fast jeder der Zuschauer blickt Ihnen magisch auf die Finger bei der Eingabe des Codes zu Ihrer Kreditkarte. Da Sie in Gedanken sind und auch nichts Schlimmes erwarten, fällt Ihnen das nicht weiter auf. Sie zahlen und gehen in Richtung Ausgang. Auf dem Weg nach draußen rempelt Sie jemand an und stiehlt Ihre Tasche und Ihre Geldbörse. Das Abhandenkommen der Tasche bemerken Sie schnell, aber nicht so schnell die Gefahr durch das Verlorengehen der Kreditkarte. Sie realisieren erst nach und nach, dass der Dieb außer physikalischen Dingen nun auch Digitales von Ihnen besitzt.

Wie dem auch sei, der Dieb hat jetzt den ›PIN-Code‹, den er bei Ihrer Eingabe an der Kasse mitverfolgt hat, und die dazugehörige ›Kreditkarte‹ von Ihnen.

Das Erste, was er machen wird, sich so schnell wie möglich zum nächsten Geldautomaten bewegen, um so viel Ihres Geldes abzuheben wie nur möglich. Da Ihnen nicht gleich bewusst wird, dass jemand den ›PIN-Code‹ ihrer ›Kreditkarte‹ haben könnte, schenken Sie diesem speziellen Umstand anfangs keine Beachtung. Sie melden den Diebstahl der Tasche. Bis Sie Ihre Kreditkarte sperren lassen, vergehen eventuell einige Stunden, vielleicht auch 1–2 Tage.

In dieser Zeit kann der Dieb ohne Schwierigkeiten 20 oder mehr Geldautomaten ansteuern und vielleicht sogar all Ihr Geld plündern.

Sollten Sie kein bestimmtes Limit zur täglichen Abhebung eingerichtet haben, kann es passieren, dass Ihr ganzes Konto leer geräumt wird.

GEDANKENREISE ENDE

Sich bei der Eingabe von ›PIN-Codes‹ auf die Finger schauen zu lassen, kann unzählige Male gut gehen, aber einmal ist