IT SICHERHEIT LEICHT GEMACHT

8 TIPPS FÜR EINE SICHERE DIGITALE ZUKUNFT

PETER'S IT
SICHERHEIT FÜR JEDERMANN

PETER DAVIDA

Inhaltsverzeichnis

Vorwort

Bei meinem Job als IT Sicherheits-Berater und Techniker, durfte/musste ich die letzten knapp 10 Jahre bei den unterschiedlichsten Firmen und Branchen vieles sehen und lernen. Es waren viele prägende Erlebnisse dabei, welche mich immer wieder zum Nachdenken angeregt haben. Ich frage mich auch noch nach so vielen Jahren:

„Hätte das wirklich passieren müssen?“

„Wieso unternimmt niemand etwas dagegen?“

„Gibt es wirklich noch immer Leute, die auf so etwas hereinfallen?“

Auch auf der Straße, im Restaurant, im Flugzeug oder an praktisch allen Orten, an denen ich mich in meiner Freizeit aufhalte, beobachte ich immer wieder, wie unachtsam die Kinder, Jugendliche und vor allem die Erwachsenen mit den neuen Medien umgehen.

Die meisten Vorfälle, welche ich bearbeitet habe, wurden vom Benutzer selber ausgelöst. Der Grund war praktisch immer gleich, entweder Unwissenheit oder Unaufmerksamkeit.

Mit diesem E-Book habe ich mir das Ziel gesetzt, ganz normale sowie nicht IT-affine Benutzer mit meinem Wissen über IT Sicherheit zu unterstützen und Denkanstöße zu verschiedensten Themen zu geben.

Eine 100%ige Sicherheit kann höchstwahrscheinlich nie erreicht werden, jedoch wäre es sehr fahrlässig, sich nicht mit diesem sehr wichtigen Thema zu befassen.

Jeder ist für seine eigene Sicherheit zuständig. Einen kleinen Überblick, wie so etwas in der Realität aussehen kann und was die wichtigsten Aspekte eurer persönlichen Sicherheit sind, findet ihr in diesem E-Book.

Weiter solltet ihr Lösungsmöglichkeiten erkennen und diese praktisch umsetzen. Mit den folgenden Methoden bringt ihr euer digitales Leben auf einen Top Stand!

Was mir ganz besonders am Herzen liegt, ist, dass ihr folgende Punkte versteht:

1. Um was geht es hier überhaupt?
2. Welche Risiken/Bedrohungen und Sicherheitslücken gibt es?
3. Welche Konsequenzen können für mich entstehen?
4. Was kann ich dagegen tun?
5. Wie kann ich ein gesundes Bewusstsein für IT Sicherheit aufbauen?

Und jetzt rein ins Vergnügen, es gibt viel zu tun!

Ich wünsche euch viel Freude beim Lesen und vor allem viele neue Erkenntnisse.

Peter Davida

1. Passwörter

1.1 Warum sind Passwörter so wichtig?

Mindestlänge, Groß- und Kleinschreibung, Sonderzeichen, Nummern – wer blickt hierbei noch durch? Und kann man überhaupt darauf vertrauen, dass Onlinekriminelle die Passwörter nicht doch herausfinden? Die Realität zeigt, dass Passwörter immer noch der größte Risikofaktor in der IT Sicherheit sind. Das Erraten bzw. das automatische Errechnen der Passwörter ist in vielen Fällen sehr einfach. Passwörter wie „123456“, „abc123“ oder auch die Benennung nach der entsprechenden Webseite sind sehr beliebt. Es scheint, als ob die Benutzer die Wichtigkeit dahingehend noch nicht erkannt hat.

Bei Registrierungen auf Webseiten sind Passwortrichtlinien, wie z.B. mindestens einen Großbuchstaben (A-Z), mindestens einen Kleinbuchstaben (a-z), mindestens eine Ziffer (0-9), mindestens ein Sonderzeichen sowie eine Mindestlänge von zehn Zeichen mittlerweile sehr beliebt. Aufgrund der Komplexität der Passwörter, kommt es jedoch oft vor, dass Nutzer nun das gleiche Passwort für mehrere Seiten benutzen. Weiter werden oft Passwörter wie z.B. „Hallo1234!“ erstellt. Dieses Passwort würde zwar den Anforderungen entsprechen, doch stellt es insgesamt durch seine Einfachheit und

aufgrund der häufigen Benutzung von anderen Usern, ein nicht besonders starkes und dadurch kein sicheres Passwort dar. Ein Computer eines durchschnittlichen Benutzers benötigt ca. 9 Sekunden, um alle Kombinationen eines 6-stelliges Passworts, welches nur aus Groß- und Kleinbuchstaben besteht durchzuprobieren.

Jedoch finde ich es nicht fair, die komplette Verantwortung nur den Nutzern zuzuschieben. Klar ist es die persönliche Verantwortung und sollte auch im persönlichen Interesse aller liegen, aber wer kann sich heute schon bei den unendlich vielen Logins komplexe und einzigartige Passwörter merken und dann auch noch schnell parat haben? Das grenzt schon an einer gedanklichen Höchstleistung. Und wer hat schon Lust und Zeit, sich damit auseinanderzusetzen?

Eine schnelle Lösung ist hierbei natürlich das gleiche Passwort für mehrere Konten zu verwenden. Das Problem hierbei ist jedoch, dass es Kriminellen immer wieder gelingt, sich in Datenbanken einzuhacken und Millionen von Zugangsdaten zu stehlen. Mit einer Technik namens „Credential Stuffing“ werden diese Zugangsdaten dann automatisch auf verschiedenen anderen Plattformen ausprobiert. So ist das Einloggen in E-Mail-Konten, Zahlungsdiensten, Sozialen Netzwerken usw. möglich.

Auch bei anspruchsvollen Passwörtern besteht weiterhin das Risiko für einen Passwortklau.

1.2 Tipps für eure Passwortwahl

Eure 12 Top Tipps:

1. Benutzt verschiedene Passwörter für unterschiedliche Logins.
2. Bildet Zahlen- und Buchstabenkombination, welche nicht in der Abfolge „1234…“ oder „abcd...“ aufgebaut sind.
3. Je länger die Passwörter, desto besser – sichere Passwörter starten mit mind. 10 Zeichen.
4. Benutzt Klein- und Großbuchstaben, Zahlen und Sonderzeichen.
5. Alternativ können auch lange Sätze wie „IchSpieleseit23JahrenTennis!“ benutzt werden.
6. Teilt eure Passwörter nicht mit anderen Personen oder kommuniziert sie online in E-Mails etc.
7. Vermeidet das Speichern der Passwörter im Browser, besonders, wenn ihr euch auf fremden Geräten einloggt.
8. Falls ihr Geräte benutzt, welche nicht euch gehören, achtet darauf, dass ihr am Ende der Nutzung auf jeden Fall wieder ausgeloggt seid.

9. Wenn ihr WLAN-Verbindungen in z.B. Cafés, Flughäfen und anderen öffentlichen Plätzen nutzt, loggt euch nur im Notfall in wichtige Accounts wie z.B. Bank-App oder E-Mail Accounts ein.
10. Falls ihr Bedenken habt, dass eines eurer Passwörter geknackt und gestohlen wurde, ändert dieses auf dem schnellsten Weg, um weitere Versuche durch Dritte auszuschließen.
11. Aktualisiert und wechselt eure Passwörter in regelmäßigen Abständen.
12. Verwendet einen Passwortmanager.

1.3 Persönlicher Assistent gewünscht? –> der Passwortmanager

Die Technologie ist doch schon so weit fortgeschritten – warum gibt es nicht auch eine einfache Lösung, welche bei der Passwortwahl unterstützt?

Diese Lösung gibt es. Man nennt sie den Passwortmanager!

Euer persönlicher Assistent – der Passwortmanager hilft euch dabei….

1. eine Vielzahl von Passwörtern effektiv zu verwalten,
2. sichere Passwörter zu erstellen,
3. einen Überblick und Kontrolle zu behalten

… und darüber hinaus die Gefahr durch einen Passwortklau zu minimieren!

Man kann sich den Passwortmanager wie einen Tresor vorstellen, welcher eure Passwörter aufbewahrt. Dieser ist mit einem Master-Passwort verschlossen. Wenn ihr den Manager öffnet, könnt ihr eure gespeicherten Passwörter rauskopieren und für die jeweilige Plattform nutzen.

Falls ihr Passwörter erstellen möchtet, könnt ihr dies direkt durch den Passwortmanager tun. Mit einem „Browser-Plug-In“ ist es möglich, dass ihr euren Browser mit dem Passwortmanager verbindet. Sobald ihr dann ein neues Konto erstellt, könnt ihr ganz einfach eine zufällige und sichere Zeichenabfolge durch den Assistenten generieren lassen, welcher das neue Passwort automatisch im Tresor speichert.

Beim Einloggen in die entsprechenden Plattformen braucht ihr nur noch das Master-Passwort eingeben und das gewünschte Passwort wird bereitgestellt.

Bezüglich der Wahl für den Passwortmanager gibt es Online- oder Offlinelösungen. Der Vorteil der Onlinelösungen besteht darin, dass Passwörter von überall abgerufen werden können. Offlinelösungen bieten teilweise eine höhere Sicherheit, da die Passwörter nicht online in einer Cloud gespeichert werden, welche ebenfalls gehackt werden könnte.

2. Multi-Faktor-Authentifizierung

2.1 Schon mal gehört, aber um was geht es hier?

Der erste Schritt mit dem perfekten Passwort ist somit getan. Lasst uns jetzt noch einen weiteren Schritt in Richtung „perfekte“ Sicherheit gehen. Immer öfters hört man von der „Zwei-Faktor Authentifizierung“, welche aber leider noch immer auf zu wenigen Plattformen vorausgesetzt wird.

Dabei handelt es sich um zwei Faktoren, welche man auch als Identifikationsmerkmale bezeichnen kann. Ein Merkmal dabei ist etwas das „man weiß“ und das andere etwas das „man hat“. Für eine fremde Person ist es sehr schwierig, beide Merkmale zu besitzen. Der Dieb würde den physischen Gegenstand sowie das Wissen benötigen, um sich entsprechend in euer persönliches Territorium einzuhacken um euch dann Daten zu stehlen.

2.2 Welche Faktoren sind das genau?

Faktoren, um eine Authentifizierung durchzuführen:

„Man weiß“- Faktor

Darunter fällt Wissen, wie z.B. ein Passwort oder PIN. Dies ist der am häufigsten genutzte Faktor, auch „Ein-Faktor-Authentifizierung“ genannt. Hier wird lediglich Wissen abgefragt, welches nur dem Anwender bekannt sein sollte. Wie bereits erwähnt, spielt hier auf jeden Fall die Wahl eines starken Passworts die wichtigste Rolle.

„Man hat“-Faktor

Dies sind physische Besitzobjekte wie Token, Schlüssel, Magnetkarte oder Mobiltelefon, welche in eurem Besitz sind. Wenn ihr euch mit eurem Konto anmelden oder einen Dienst nutzen möchtet, wäre hierbei dieser Gegenstand mitzuführen, um den entsprechenden zweiten Faktor zu bestätigen. Eure Sicherheit nimmt durch die Bestätigung dieses zweiten Faktors erheblich zu.

„Physisches Merkmal“-Faktor

Die Entwicklung geht dahin, dass mittlerweile ein dritter Faktor angefragt wird, was auch Multi-Faktor-Authentifizierung genannt wird. Dabei handelt es sich um ein Merkmal, welches unverwechselbar mit eurer Identität verknüpft ist, wie z.B. biometrische Informationen, darunter Fingerabdruck, Muster der Iris oder auch Stimme. Besonders wichtig ist hierbei, dass Systeme genutzt werden, welche diese Merkmale eindeutig erkennen, wie z.B. Scanner für Fingerabdruck, Augen-Iris und mittlerweile auch Stimmerkennungssysteme. Genau dieser Faktor wäre zusätzlich zum „Wissen-“ und „Haben-Faktor“ zu belegen.

2.3 Und in der Praxis?

Vielleicht ist es euch gar nicht bewusst, aber ihr benutzt die Zwei-Faktor-Authentifizierung schon seit langer Zeit auf vielen Wegen. Ein Beispiel ist die Nutzung eurer EC-Karte, wenn ihr bezahlt oder Geld am Automaten abhebt. Faktor 1 wäre hierbei euer Wissen über euren persönlichen PIN und Faktor 2 eure Karte, welche ihr vorlegt. Am Ende braucht ihr beides, um die „Zwei-Faktor-Authentifizierung“ durchzuführen.

Besonders im Online-Banking könnt ihr mit diesem Verfahren eure Sicherheit erhöhen. Hierbei benutzt ihr euren Usernamen und das Passwort sowie einen USB-Token oder eine TAN, welche ihr per SMS erhaltet oder mit eurem TAN-Generator erstellt. Falls ihr

die „Zwei-Faktor-Authentifizierung“ auf eurem Paypal-Konto aktiviert habt, könnt ihr auch hier euer Passwort sowie ein TAN via SMS/APP zur „Zwei-Faktor-Authentifizierung“ nutzen.

Die Sicherheit wäre erst gefährdet, wenn ihr physisch sowie digital bestohlen werdet. Das Verfahren der „Zwei-Faktor-Authentifizierung“ hat sich also schon lange etabliert und dient daher auch den wichtigsten Angelegenheiten wie z.B. euren Finanzen etc.

2.4 Wo ist diese Sicherheit besonders gefragt?

Generell ist es immer ratsam, eine „Zwei-Faktor-Authentifizierung“ zu aktivieren, falls diese angeboten wird. Dies wäre besonders bei der Nutzung von Online-Banking oder Zahlungsdienstleistern wie z.B. Paypal zu befürworten. Da es hier um euer Geld geht, ist die Erhöhung der Sicherheit durch einen zweiten Faktor auf jeden Fall angebracht. Des Weiteren empfehle ich, dieses Verfahren zu nutzen, wenn ihr irgendwo online einkauft. Mittlerweile bietet euch zum Beispiel Amazon diesen Service an.

Darüber hinaus ist euer E-Mail-Konto eine der wichtigsten Adressen, wenn es um Sicherheit geht. Da ihr auf fast jeder Plattform das Passwort mit eurer E-Mail-Adresse zurücksetzen könnt, ist es besonders wichtig, euer E-Mail-Postfach zu schützen. Es gibt inzwischen E-Mail-Provider, welche die „Zwei-Faktor-Authentifizierung“ anbieten, daher würde ich euch empfehlen, einen Blick darauf zu werfen und ernsthaft zu überlegen, diesen Anbietern euer Vertrauen zu schenken.

3. Backups

3.1 Warum Backups unsere „Helden“ sind

Kennt ihr diese Schreckensmomente?

„Ihr seid auf der Suche nach einer wichtigen Info aus einer alten Steuererklärung. Da ihr so gut organisiert seid, wisst ihr genau, in welchem Ordner auf eurem Rechner sich diese Daten befinden. Doch obwohl alles sauber abgelegt ist, müsst ihr feststellen, dass der Zugriff nicht mehr möglich ist. Euer Rechner zeigt beim Starten aus heiterem Himmel die Fehlermeldung <Festplatte defekt> an.“

Oder....

„Ein wichtiger Geschäftstermin steht bevor und ihr bemerkt 20 Minuten vor dem Vortrag, dass beim Kopieren eurer Präsentation ein Fehler aufgetreten und die Datei auf unerklärliche Weise verschwunden ist.“

Schlimmer geht immer...

„Ihr seid auf dem Heimweg von eurer Traumreise – vielleicht sogar von den Flitterwochen. Als ihr zu Hause ankommt, stellt ihr fest, dass euer Smartphone verschwunden ist. Letzte Erinnerung an das Gerät: Imbiss Flughafen Dubai. Wie stehen wohl die Chancen, das Gerät wieder zu bekommen? Alle Urlaubsbilder sind weg und ebenfalls die Fotos aus einem kompletten Lebensabschnitt – von den persönlichen Daten gar nicht erst zu sprechen.“

Durch die genannten Beispiele wird klar, dass die Notwendigkeit von Sicherheitskopien auf externe Datenträger in ganz vielen Fällen unterschätzt wird. Man hört immer wieder „Ach das passiert mir nicht“ – und wenn doch, ist es bereits zu spät. Die gute Nachricht für euch: In der IT-Welt gibt es unzählige und einfache Möglichkeiten, damit Fälle wie oben erwähnt nicht zum Totalverlust der Daten führen. Ein Datenverlust kann unter anderem aufgrund von Hackerangriffen, defekter Hardware, fehlerhaften Betriebssystemen oder auch durch Diebstahl entstehen.

Mit dem Helden namens „Backup“ an unserer Seite lässt es sich viel besser schlafen.

3.2 Formen der Sicherung

Offline

Eine Offline-Sicherung könnt ihr z.B. ganz einfach durchführen, indem ihr eine externe Festplatte per USB-Kabel an euren Rechner anschließt. Hinsichtlich der Speichergröße für Festplatten gibt es mittlerweile Modelle in allen Größen und Formen. Sie ermöglichen euch, ein großes Volumen an Daten wie z.B. die persönlichen Musik- und Video-Sammlungen zu speichern.

Online

Weiter gibt es heutzutage auch die Möglichkeit, eure Backups online bei verschiedensten Anbietern durchzuführen. Google mit Google Drive, Apple mit der iCloud oder auch Amazon mit S3 bieten euch hierfür diverse Möglichkeiten, eure Daten online zu speichern oder auch zu archivieren.

3.3 Online vs. Offline? Was ist besser?

Es wäre anmaßend von mir, hier zu entscheiden, was besser oder schlechter ist. Es gibt verschiedene Faktoren, welche bei der Entscheidung miteinbezogen werden sollten. Im folgenden Abschnitt versuche ich euch die Fakten so neutral wie möglich aufzulisten.

Vorab möchte ich erwähnen, dass die Komplexität einer Konfiguration der Offline- oder Online-Sicherung gleich hoch beziehungsweise tief ist. Mit der geeigneten Software ist es mit beiden Varianten möglich, die Daten regelmäßig und automatisch zu sichern.

Offline

Eine Offline-Sicherung wird, wie bereits erwähnt, auf ein externes Gerät wie z.B. einer Festplatte gemacht. Dieses Gerät muss für die Sicherung sowie für eine Wiederherstellung von verlorenen Daten immer verfügbar und angeschlossen sein.

- Die Kosten für eine Festplatte sind sehr überschaubar.
- Sobald die Festplatte voll ist, wird eine neue benötigt.
- Ein Feuer oder auch ein handelsüblicher Hammer können die Festplatte problemlos zerstören.
- Hacker haben, sofern die Festplatte nicht angeschlossen ist, keinen Zugang auf die Daten.
- Festplatten haben eine durchschnittliche Lebensdauer von 10 Jahren.
- Eine Internetverbindung wird für die Sicherung nicht benötigt.

Online

Für eine Online-Sicherung wird ein guter Anbieter benötigt. Einige jedoch nicht abschließende Beispiele wurden bereits erwähnt.

- Die Daten sind immer und von überall zugänglich.
- Hacker könnten bei unzureichender Absicherung oder bei einem schlechten Anbieter Zugang zu den Daten erhalten.
- Ein Onlinespeicher ist sehr günstig und fast unendlich verfügbar.
- Die Lebensdauer von Onlinedaten ist unlimitiert.
- Eine Internetverbindung ist für die Sicherung immer zwingend notwendig.

3.4 Euer Masterplan – Anzahl der Kopien und Zeitabstände

Zwei Kopien, um auf Nummer sicher zu gehen

Empfehlenswert ist es, zwei weitere Kopien zusätzlich zu euren Originaldaten zu erstellen. Die erste Sicherung wäre eine komplette Kopie eures Gerätes auf eine Festplatte. Bei einer solchen Komplettsicherung werden sehr viele Daten kopiert, welche kaum gebraucht werden. Diese Sicherung ist für den Fall, dass euer Laptop, Smartphone oder Computer aus heiterem Himmel den Geist aufgibt.

Bei der zweiten Sicherung werden nur die wichtigen Daten wie Dokumente, Bilder, Videos oder sonstige Daten gespeichert, welche immer wieder benutzt und geändert werden. Idealerweise befindet sich diese Sicherung online, damit auch auf Reisen darauf zugegriffen werden kann.

Die Vorgehensweise kann natürlich auf jegliche Bedürfnisse und Art der Geräte angepasst werden.

Zeitplan

Hinsichtlich des Zeitplans kommt es ganz individuell auf eure Datenproduktion an. Auf das oben beschriebene Szenario bezogen, wäre eine zweiwöchentliche Offlinesicherung des Gerätes und eine tägliche Onlinesicherung der einzelnen Daten zu empfehlen.

Da die Sicherung ein automatischer Prozess ist bzw. im Offlinefall nur die Festplatte angehängt werden muss, kann mit dem Zeitplan auch gespielt und die richtigen Abstände erörtert werden.

4. Updates

4.1 Der Wurm „Conficker“

Was hat der „Conficker“-Wurm mit Updates zu tun? Für alle, die noch nie von diesem Computerwurm gehört haben: Er ist ein sehr prominentes Beispiel für die Ausnutzung von Sicherheitslücken. Im Jahr 2009 sind durch diesen Wurm Millionen von Rechnern infiziert worden, obwohl es im Oktober 2008 bereits ein Sicherheitsupdate von Microsoft gab. Im Nachhinein betrachtet, hätte durch die aktive Durchführung des entsprechenden Updates ein Schaden bei Millionen von Benutzern vermieden werden können.

Klar, man weiß nie, was in Zukunft passiert und so eine Updateanfrage kann echt nervig sein. Daher stellt das „Wegklicken“ für viele die schnellste und üblichste Lösung dar. Anhand des Beispiels lässt sich jedoch erkennen, dass es manchmal vielleicht doch Sinn macht, dem Update eine Chance zu geben. Denn einfacher lässt sich eure IT-Sicherheit nicht erhöhen – besonders dann, wenn unsere schöne und saubere Datenwelt durch hartnäckige, eklige Fälle, wie z.B. Würmer bedroht wird.

4.2 Lösungen für diese lästigen Schwachstellen

Eine zeitnahe und regelmäßige Durchführung von Updates hat viele Vorteile.

Sicherheitslücken im Betriebssystem oder in der Software werden geschlossen, Fehler werden behoben und neue Funktionen werden aktiviert. Das Betriebssystem selbst sowie auch Standardprogramme, wie z.B. Antivirus, Adobe Reader, Office oder Java untersuchen regelmäßig, ob es neue Updates gibt und zeigen euch diese meist durch eine Benachrichtigung auf dem Bildschirm an. Für Standardbenutzer, welche sich nicht mit dem Thema auseinandersetzen wollen, besteht die Möglichkeit, die Updates vom System automatisch installieren zu lassen.

Und mal ehrlich, neben den Sicherheitsfunktionen, wer möchte nicht auf dem neuesten Stand sein und auch in Zukunft die Vorzüge eines modernen Systems nutzen?

4.3 So könnt ihr eure Updates auf einfachsten Weg durchführen

Eigentlich ist das Thema „Updates“ überhaupt keine Raketenwissenschaft für Benutzer, da die wirkliche Herausforderung bei den Herstellern liegt. Sobald diese herausfinden, dass es Probleme oder Fehler in der Software oder Hardware gibt, werden Updates dazu entwickelt und euch zur Verfügung gestellt. Auch wenn neue Viren oder Schädlinge unterwegs sind, wird vorgesorgt, indem entsprechende Updates bereitgestellt werden. Das einzige was ihr dann wirklich tun müsst, ist, die Hilfe anzunehmen, die Updates zu akzeptieren und auszuführen. Auch wenn dies einen Moment in Anspruch nimmt und ihr vielleicht den Rechner neu starten müsst, lohnt sich die investierte Zeit auf jeden Fall.

5. Firewall & Antiviren-Software

Unsere geliebten Geräte sollten nicht nur aufgeräumt, gesichert und auf dem aktuellsten Stand sein, sondern auch gesund. Eine kleine Aufmerksamkeit mit großer Wirkung sind die Firewall und eine Antiviren-Software. Mit geringem Aufwand lassen sich die „Reinigungshilfe“ und eine Art Türsteher auf den Geräten aktivieren.

5.1 Antiviren-Software

Malware wie Viren, Würmer, Ransomware und wie sie alle heißen, lieben es, einen möglichst großen Schaden anzurichten. Szenarien wie das Klauen eurer Daten, die Zerstörung eurer Geräte, die Erpressung von Lösegeld oder Spionage eurer Aktivität sind nur einige Beispiele. Aufgrund der großen Verbreitung sind Windows-Rechner etwas stärker und häufiger damit konfrontiert als Linux und macOS. Trotz der weitverbreiteten Meinung, dass vor allem macOS keine Malware bekommen kann (was im Übrigen der Kategorie „gefährliches Halbwissen“ zuzuordnen ist), ist es auf jeden Fall zu empfehlen, dass ihr auch auf weniger anfälligen Systemen eine Antiviren-

Software installiert. Dabei sollte man Mobiltelefone, wie vor allem aber nicht ausschließlich Android Geräte, nicht vergessen.

Sobald ihr die Antiviren-Software installiert und konfiguriert habt, läuft der Schutz im Hintergrund mit. Die mittlerweile sehr intelligente Software weiß ganz genau, was sie tut und ihr als normale Benutzer habt praktisch keinen Aufwand mehr.

Das Programm überprüft jeweils neue Dateien, die zum Beispiel über Datenträger, E-Mail oder Downloads auf eurem Rechner ankommen. Darüber hinaus werden regelmäßig die Daten überprüft, welche bereits gespeichert sind. Die Überprüfung verläuft wie folgt: Der, benennen wir es „Fingerabdruck“ eurer Datei, wird in einer Datenbank mit dem Fingerabdruck des Schadprogrammes abgeglichen.

Sollte es irgendwelche Auffälligkeiten oder Übereinstimmungen geben, werdet ihr informiert. Hierbei seht ihr auch, wie wichtig es ist, immer die neueste Antiviren-Software zu nutzen und die Updates zu installieren. Nur so kann gewährleistet werden, dass die Software über die neuesten Versionen von Schädlingen Bescheid weiß und entsprechende „Fingerabdrücke“ dazu speichert.

In früheren Zeiten war es Voraussetzung, die regelmäßigen Scans manuell für einzelne Teile wie Festplatte, Laufwerke etc. durchzuführen. Der heutige Stand der Technik ermöglicht es, dass ihr nur noch die „Auto-Protect-Funktion“ einschalten müsst, damit die Überprüfung automatisch im Hintergrund durchgeführt wird. Ein wöchentlicher vollständiger Scan ist aufgrund der höheren Scan-„Aggressivität“ trotzdem zu empfehlen. Funde teilt euch das Programm sofort mit der entsprechenden Gegenmaßnahme mit.

5.2 Die Firewall - „Du kommst hier nicht rein!“

Die Firewall ist euer persönlicher Türsteher, welche den Zugang zu eurem PC überprüft. Nur erwünschte und angeforderte Verbindungen werden zugelassen. Angriffe und unerwünschte Zugriffe werden abgewehrt.

Eine Firewall ist auf jedem modernen Betriebssystem wie Windows 10 oder macOS X bereits vorab installiert und komplett auf das System abgestimmt.

Geräte mit Internetverbindung wie z.B. euer Haus, Auto oder Kühlschrank, sind dem sogenannten „Internet der Dinge“ zuzuordnen. Sollten solche Geräte in eurem Netz angeschlossen sein, ist eine Hardware-Firewall nach dem Internetanschluss dringend zu empfehlen. Da die Details dieses Themas den Rahmen des E-Books sprengen würden, möchte ich nicht weiter darauf eingehen. Bei Fragen könnt ihr mich gerne jederzeit kontaktieren.

5.3 Nicht nachlässig werden

Mit der Aktivierung von Firewall und Antiviren-Software ist ein guter Grad an Grundschutz für eure Geräte gegeben. Ein Grundschutz ist und bleibt jedoch „nur“ ein Grundschutz. Man darf nie vergessen, dass es sehr viele Sicherheitslücken gibt, von denen niemand weiß und welche die Kriminellen meistens zuerst finden. Die Hersteller geben zwar ihr Bestes, finden aber viele Schwachstellen erst nachdem sie jemand ausgenutzt und eine geschädigte Person dies gemeldet hat.

Beim Surfen durchs Internet sollten trotz toller installierter Sicherheitsprogramme, nicht alle Links angeklickt, E-Mails von fremdem Absender geöffnet und unbekannte Programme installiert werden. Behaltet immer eine gesunde Skepsis bei.

6. Festplattenverschlüsselung

6.1 Wie wäre es mit einem Bodyguard für eure Daten?

In der heutigen Zeit, im Trend zur Mobilität und Flexibilität ist es bereits selbstverständlich geworden, mit Laptop, Notebook oder Tablet unterwegs zu sein. Mit diesem Trend gehen auch einige Gefahren einher.

In den letzten Kapiteln dieses E-Books, haben wir dafür gesorgt, dass eure Daten vor Gefahren direkt aus dem Internet geschützt sind. Jetzt kommt natürlich die Frage auf, wie ihr die Daten unterwegs vor Verlust oder Diebstahl schützen könnt. Manchmal kann es ganz schnell gehen: Ihr seid nur einmal kurz am Bahnhof oder Flughafen mit den Gedanken woanders und super schnell ist euer Gerät in die Hände eines Fremden geraten.

Was nun? Können die Daten direkt vom Laptop oder Mobiltelefon ausgelesen werden? Auch wenn euer Gerät mit einem Passwort geschützt ist, wissen wir, dass dies nur ein bedingter Schutz ist. Eure Festplatte wird ganz einfach ausgebaut und an das Gerät des Diebes angeschlossen. Der Passwortschutz greift nun nicht mehr richtig oder kann umgangen werden. Der Dieb kann jetzt freudig auf eure Daten zugreifen und damit

machen was er will. Wenn es ganz schlecht läuft, stehlen die Langfinger sogar eure Zugangsdaten für Internetseiten, Online-Banking und was ihr sonst noch alles auf dem Gerät installiert habt.

Die Lösung für dieses Problem darf ich euch jetzt vorstellen: Der „Data-Bodyguard“, genannt Festplattenverschlüsselung. Die Festplattenverschlüsselung verschlüsselt, wie der Name schon sagt, die komplette Festplatte. Sehr vereinfacht kann man sich diese Verschlüsselung wie eine Geheimschrift von Kindern vorstellen, die nicht wollen, dass der Lehrer versteht, wovon sie in ihren geheimen Briefchen sprechen.

Aus...

Hallo ich bin Peter, 30 Jahre alt und komme aus Liechtenstein.

wird mit der Caesar-Verschlüsselung...

Ohssv pjo ipu Wlaly, 30 Qhoyl hsa buk rvttl hbz Spljoaluzalpu.

Solange das Gegenüber den Entschlüsselungsschlüssel nicht weiß, wird die Nachricht für immer geheim bleiben.

6.2 Verschlüsselungsprogramme

Auch wenn wir unsere Geräte nicht an uns ketten können, um einen Diebstahl zu vermeiden, gibt es zumindest Mittel und Wege, welche die Daten für Diebe unbrauchbar machen. Windows hat z.B. mit BitLocker und MacOS mit FileVault eine gute und bereits vorab eingebaute Lösung gefunden. Diese Programme anonymisieren quasi auf Knopfdruck komplett alle Daten oder falls gewünscht, nur einzelne Ordner auf dem Gerät. Der große Vorteil an den vorinstallierten Verschlüsselungsprogrammen ist, dass die Verschlüsselung transparent erfolgt. Dies bedeutet, dass ihr ganz normal mit euren Daten arbeiten könnt. Auch wenn eure Festplatte aus dem Gerät entfernt wird, bleiben die Daten weiterhin verschlüsselt und der Dieb stößt nur auf ein Wirrwarr aus Buchstaben und Ziffern. Weitere, nicht vorab installierte Lösungen für ältere Windows- oder auch Linux-Systeme stelle ich euch im folgenden Abschnitt vor.

TrueCrypt/VeraCrypt

TrueCrypt hat unterschiedlichste Assistenten bereits eingebaut, welche es euch ermöglichen, die Festplatte teilweise oder auch das komplette Betriebssystem zu verriegeln. Bei der Suche wird euch wahrscheinlich auch die Software mit ähnlichem Namen – VeraCrypt, über den Weg laufen. VeraCrypt ist nach der Beendigung des TrueCrypt-Projekts entstanden. Obwohl in TrueCrypt einige Sicherheitslücken geschlossen wurden, schwören die hartgesottenen TrueCrypt-Fans noch immer auf das

Original. Beide Varianten bieten eine umfangreiche Verschlüsselung für eure Daten auf der Festplatte.

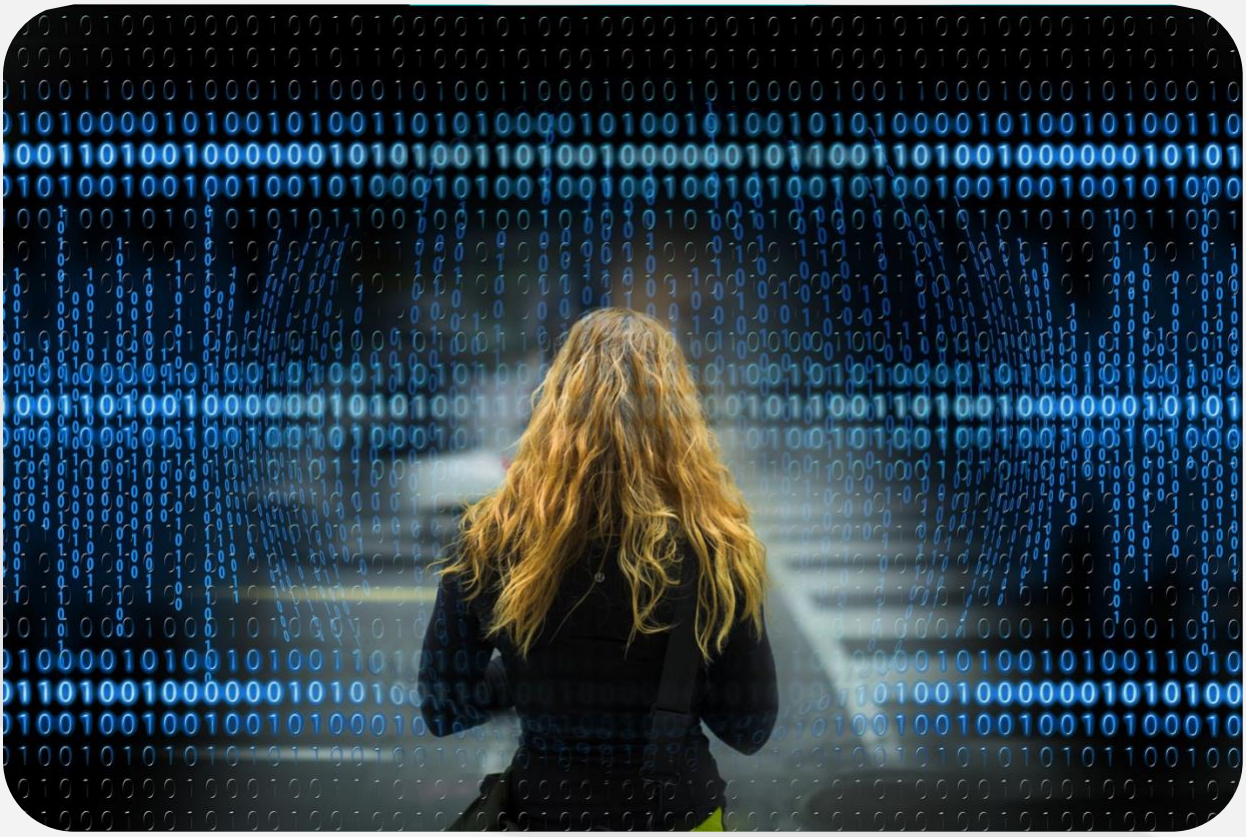
TPM (Trusted Platform Module)

TPM hat zu viele verschiedene Anwendungsfälle, um diese genauer auszuführen. Vereinfacht ist TPM ein Chip, der direkt auf der Hauptplatine eines Rechners platziert wird und Softwares wie BitLocker und Co. bei der Verschlüsselung direkt von der Hardware aus unterstützt.

Grundsätzlich ist es für alle möglich, selber eine Festplattenverschlüsselung durchzuführen. Bei sehr kritischen Systemen wie z.B. zentrale Server in einer Firma ist eine Beratung durch einen Fachmann noch immer zu bevorzugen.

Falls ihr schon direkt beginnen möchtet, eure Festplattenverschlüsselung einzurichten, wäre diesbezüglich nochmals hervorzuheben, dass ihr unbedingt auf ein sehr starkes Passwort achten solltet.

7. Privatsphäre & Personenbezogene Daten



7.1 Ich habe nichts zu verbergen

Edward Snowden der US-amerikanische Whistleblower und ehemaliger CIA-Mitarbeiter kontert diese Aussage in seinem Buch „Permanent Record“ wie folgt:

„Zu behaupten, dass uns unsere Privatsphäre egal ist, weil wir nichts zu verbergen haben, ist letztlich dasselbe, als würden wir behaupten, dass uns die freie Meinungsäußerung egal ist, weil wir nichts zu sagen haben. Oder dass uns die Freiheit der Presse egal ist, weil wir nicht gerne lesen. Oder dass uns die Religionsfreiheit egal ist, weil wir nicht an Gott glauben. Oder dass uns das Recht auf friedliche Versammlung egal ist, weil wir träge und antisozial sind und an Agoraphobie leiden. Nur weil uns die eine oder andere Freiheit heute nicht wichtig ist, heißt das nicht, dass sie uns oder unserem Nachbarn morgen auch noch unwichtig sein muss, oder den vielen prinzipientreuen Dissidenten, denen ich auf meinem Handy folgte, während sie an verschiedenen Orten demonstrierten in der Hoffnung, nur ein Bruchteil der Freiheiten zu erlangen, die mein Land so eifrig zu beschneiden suchte.“

7.2 Der Mensch besteht aus Daten

Laut der Datenschutz-Grundverordnung (DSGVO), welche seit Mitte 2018 in der ganzen EU aktiv ist, sind personenbezogene Daten all jene Informationen, die sich auf eine natürliche Person beziehen oder zumindest beziehbar sind und so Rückschlüsse auf deren Persönlichkeit erlauben. Zusätzlich ermöglichen sie Einblicke in die physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität. Beispiele dafür sind allgemeine Personendaten, wie Namen und Alter, Bankdaten, physische Merkmale wie Geschlecht, Hautfarbe oder Kleidergröße, Besitzmerkmale wie Fahrzeug- und Immobilieneigentum, Kfz-Kennzeichen und vieles mehr.

Einige unter euch fragen sich jetzt bestimmt, wieso man diese Daten schützen muss oder was das Thema mit IT-Sicherheit zu tun hat.

Eure Daten spielen bei der Nutzung von Anwendungen eine sehr wichtige Rolle. Unternehmen wie Google, Facebook und Konsorten, verdienen viel Geld damit, Daten zu nutzen, welche von euch (un-)freiwillig mit ihnen geteilt wurden. Dies reicht von personalisierter Werbung oder im schlimmsten Fall bis zur Manipulation von euch bei diversen Themen wie Politik, Kleidungskauf etc.

Der Missbrauch von Daten kann auch strafrechtliche Konsequenzen haben, sobald Kriminelle eure Bankdaten erhalten und sich Zugriff auf euer Vermögen ergaunern.

7.3 Sei ein Daten-Minimalist!

Eine gesunde Prise Skepsis sollte mittlerweile jeder von euch in sich tragen. Natürlich möchtet ihr euch auch nicht nur darauf verlassen, dass sich Unternehmen und Regierungen an Gesetze halten und ihre technischen Sicherheitsmaßnahmen den Angriffen trotzen.

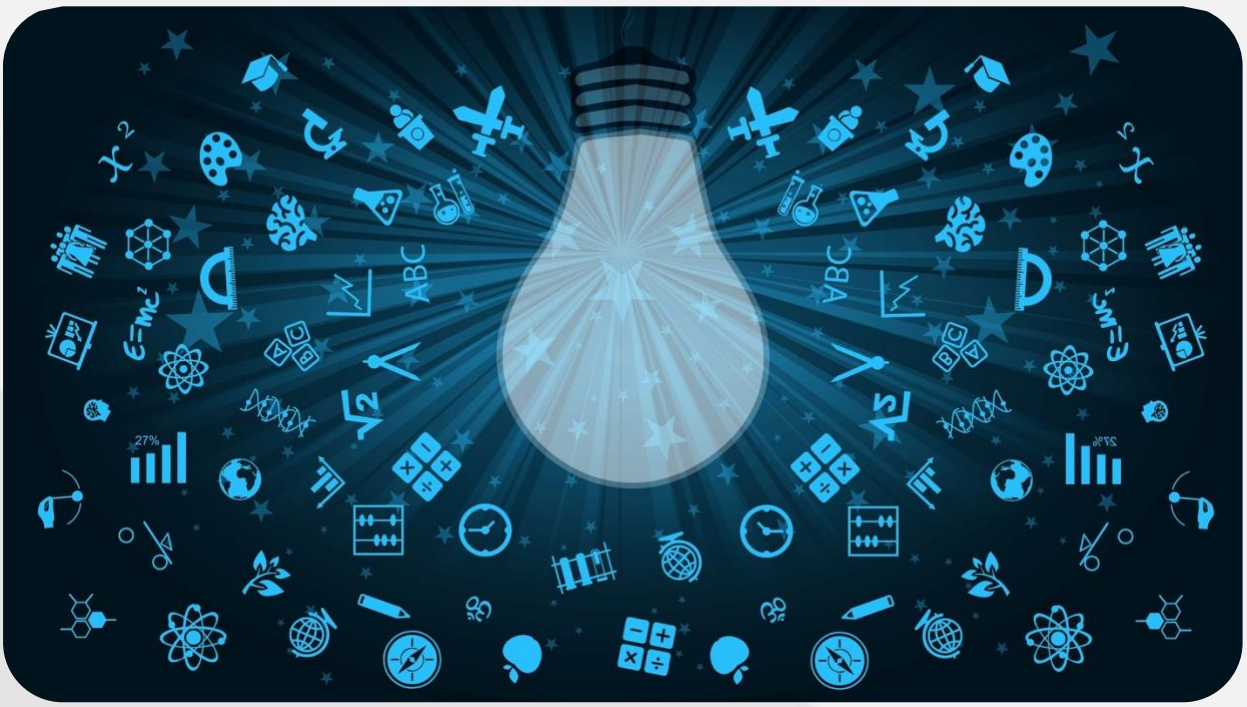
Wir alle sind auch hier selbst in der Pflicht und müssen Eigenverantwortung übernehmen. Fragt euch bei der Registrierung auf Internetseiten zweimal, ob z.B. die Informationen zu eurer politischen Einstellung oder Religion beim Kauf von Schuhen wirklich benötigt werden oder ob ihr dadurch womöglich beim nächsten Wahlkampf auf euch maßgeschneiderte Werbung bekommen werdet.

7.4 Keine Lust mehr auf Daten verteilt in der EU?

Nach Artikel 19 und 34 der DSGVO hat jeder das Recht bei Unternehmen und Behörden in der EU, Auskunft, Berichtigung oder Löschung seiner Daten zu beantragen.

Einige Unternehmen sind sich dessen noch immer nicht bewusst und stellen sich im schlimmsten Falle quer. Mit einem kleinen Hinweis auf die gesetzliche Lage sollte der Fall dann aber erledigt sein.

8. Sicherheitsbewusstsein (Awareness)



8.1 Lernen und up-to-date bleiben – Wissen ist Macht!

In der IT-Welt ist die Entwicklung so rasant, dass es eine große Herausforderung ist, beim Thema Sicherheit immer auf dem neuesten Stand zu bleiben.

Auch wenn Maschinen uns sehr bei der Sicherung unserer Geräte und Daten unterstützen, sind es nichtdestotrotz nur die Instrumente, welche von uns Menschen bedient werden. Das heißt, wir entscheiden, auf welche E-Mail-Anhänge wir klicken, welche Webseiten wir besuchen, welche Passwörter wir verwenden, ob wir Updates installieren, ein Backup durchführen oder wie wir unsere Geräte schützen. All diese Entscheidungen treffen wir nach bestem Wissen und Gewissen.

Um diese Aufgaben durchführen oder gar optimieren zu können, ist es natürlich erst einmal nötig, Wissen darüber zu erlangen. Erst wenn das Verständnis mit dem Umgang von IT-Systemen vorhanden ist, kann auch den Risiken und Bedrohungen entgegengewirkt werden. Daher gilt nach wie vor: Wissen ist Macht!

8.2 Moderne Unternehmen als Beispiel

Viele Unternehmen wissen, dass der Mensch noch immer das wichtigste Glied in einem Unternehmen ist. Dies bedeutet jedoch auch, dass der Mensch intern das größte Risiko darstellt. Leichtsinniges Verhalten oder Unwissenheit der Mitarbeiter/innen, welche keine Rücksicht auf Sicherheitsthemen nehmen oder es sogar als übertriebener Unfug ansehen, können eine Unternehmung ganz schnell Opfer von unzähligen Angriffen und Datenverlusten machen.

Daher führen Unternehmen, welche sich der Gefahren bewusst sind und sich der Sicherheit von Mitarbeiter/innen und Kunden verschrieben haben, sogenannte „Security Awareness Trainings“ durch. Das Ziel dieser Trainings ist es, alle Mitarbeiter/innen auf ein vertretbares Sicherheitsniveau anzuheben.

8.3 Zukunft?

Wer nicht von solchen Sicherheitstrainings profitieren kann oder sie als schlecht und lückenhaft ansieht, muss auf Alternativen ausweichen.

Events oder ein privater Sicherheitscoach sind eine sehr gute Möglichkeit, sich auf den neusten Stand zu bringen. Wer sich das Geld jedoch sparen möchte, findet im Internet diverse Blogs, die sehr leicht verständlich und angenehm zu lesen sind und regelmäßig über einfache Sicherheitsmaßnahmen aufklären. Personen, die sich lieber über Videos und Kurse weiterbilden, sind mit Youtube und Udemy sehr gut versorgt. Natürlich gilt auch hier – nicht alles was man im Internet sieht und hört, stimmt auch zu 100%.

Wichtig ist mir vor allem, dass ihr Vertrauen zu neuen Technologien aufbaut und die IT-Sicherheit so im Hinterkopf verankert habt, dass ihr gar nicht mehr bewusst darüber nachdenken müsst. Der Mensch als zentrales Glied in der Digitalisierung macht den Unterschied. Es hängt von jedem Einzelnen ab, ob neue Technologien angenommen und benutzt oder sie als Bedrohung der Menschheit angeschaut werden.

Fakt ist, dass sich die Welt mit, aber auch ohne euch weiterdreht und nicht einfacher wird. Meiner Meinung nach sollte jeder versuchen, so gut es geht am Ball zu bleiben und sich auf die Vorteile zu konzentrieren, welche die neuen Technologien bieten.

Aktuelle Informationen findet ihr auf meinem Blog „Peter's IT Sicherheit für jedermann" unter www.itsicherheit.li oder bei meinen privaten Schulungen und Vorträgen. Eine Kontaktaufnahme bezüglich eurer Fragen und auch eventuelles Interesse an einer Kooperation ist jederzeit über E-Mail, Instagram, Facebook oder Whatsapp möglich.

Herzlichen Dank für euer Interesse an diesem E-Book!

Ich freue mich, von euch zu hören.

© Autor Peter Davida 2020
2. Auflage
Alle Rechte vorbehalten.
Nachdruck, auch auszugsweise, verboten.
Kein Teil dieses Werkes darf ohne schriftlich Genehmigung des Autors in irgendeiner Form reproduziert, vervielfältigt oder verbreitet werden.
Kontakt: Davida Online / Schellenbergstrasse 25 / 9491 Ruggell / Fürstentum Liechtenstein
Inhaber: Peter Davida
Covergestaltung: Cebooker

Über den Autor

Peter Davida ist ein 31jähriger IT Sicherheitsspezialist aus Liechtenstein.

Als Chief Information Security Officer bei einem schnell wachsenden Scaleup Unternehmen in der Schweiz und auch als selbstständiger IT Trainer & Consultant, liebt er es, seine lebenslange Liebe zur Technologie mit seiner Leidenschaft zur Sicherheit zu verbinden.

Seine inzwischen 16jährige IT-Erfahrung, hilft ihm, die grosse Bedeutung von IT- und Datensicherheit sowohl an Privatpersonen als auch Organisationen zu bringen.

Ein großes Ziel von ihm ist, dass alle Menschen verstehen, dass Datensicherheit sowohl für den Einzelnen als auch für die Organisationen von entscheidender Bedeutung ist.