7 Tipps für sicheres Arbeiten am PC

Computer und Internet sind in unserem Alltagsleben fest verankert. Viele Menschen nutzen E-Mails, Konferenzen und Online-Banking-Apps. Doch diese Technologien bieten auch Angreifern die Möglichkeit, leichter an persönliche Daten, wie z. B. Bankinformationen, zu gelangen. Das Risiko, Opfer eines Cyber-Angriffs zu werden, ist groß. Deshalb ist es wichtig, dass Sie Ihren PC entsprechend schützen und sich an gewisse Grundregeln halten.

Diese Tipps sind vor allem für Einsteiger wichtig, die mit dieser Materie noch nicht so vertraut sind. Es gibt viele Schutzmethoden, die Sie anwenden können. Diejenigen, die wir hier aufgezählt haben, sind am wichtigsten:

1. Updates kontrollieren
2. Programme mit bedacht installieren
3. Berechtigungen einrichten
4. sichere Passwörter erstellen
5. Datensicherung durchführen
6. Internet mit Vorsicht nutzen
7. E-Mails mit Vorsicht nutzen

Updates kontrollieren

Mit Updates werden in regelmäßigen Abständen Softwareaktualisierungen von Betriebssystem und einigen Microsoft-Programmen durchgeführt. Die wichtigen Updates enthalten in erster Linie wichtige sicherheitskritische Nachbesserungen, sogenannte Patches, oder mitunter auch Lösungen für Programmfehler.

Seit Windows 10 geschieht dies mehr oder weniger ohne weiteres zutun. Es kann jedoch vorkommen, dass es ein Problem mit dem Update-Dienst gibt und es dadurch zu einem Update-Stau kommt. Wird dieser nicht bemerkt, steigt das Risiko durch Sicherheitslücken, die nicht zeitnah geschlossen werden.

Deshalb sollte gelegentlich unter Einstellungen / Updates und Sicherheit, kontrolliert werden, ob Windows auf dem aktuellen Stand ist. Hier könnte auch ein Funktionsupdate angezeigt werden. Funktionsupdates erweitern quartalsweise das Betriebssystem um weitere Funktionen und werden nicht automatisch installiert.

Mit einem Funktionsupdate ändert sich die interne Versionsnummer von Windows 10. Jede Version wird nur 18 Monate mit Sicherheitsupdates versorgt. Deshalb ist es wichtig, dass Funktionsupdates heruntergeladen und installiert werden.

Programme mit bedacht installieren

Vielleicht haben Sie sich auch schon gewundert, weshalb nach der Installation einer Software immer wieder mal Popups auftauchen. Wenn Sie Programme installieren möchten, dann verwenden Sie nur Installationsdateien aus vertrauenswürdigen Quellen. Wenn Ihnen für die Installation ein Express-Modus und ein Benutzerdefinierter-Modus angeboten wird, verwenden Sie den Benutzerdefinierten-Modus. Hier sehen Sie genau was voreingestellt installiert werden soll und können durch Abwählen verhindern, dass Ihnen zusätzliche Software untergejubelt wird, die Sie auf keinen Fall installieren möchten. Wie wichtig die Frage der Wahl der Software ist, sieht man übrigens In größeren Unternehmen, hier muss vor dem Einsatz einer Software, diese von einem IT-Sicherheitsbeauftragten freigegeben werden.

Benutzer mit Standard-Berechtigungen einrichten

Wenn Sie als Privatanwender einen Rechner mit einem neu installiertem Windows 10 vor sich haben, dann hat ihr Profil das dabei angelegt wurde, administrative Rechte. Mit diesen Rechten könnten Sie alles an Ihrem System verändern. Schadsoftware könnte das dann übrigens auch. Um das Sicherheitsniveau eines Rechners zu erhöhen, ist es deshalb wichtig, dass Sie nach der Einrichtung eines Rechners, einen neuen Benutzer erstellen, der nur Standardrechte hat. Mit diesem Nutzer sollten Sie sich dann zum arbeiten anmelden.

Passwörter sicher genug erstellen

Ich erlebe es leider immer wieder, dass es sich manche Anwender mit den Passwörtern allzu leicht macht und für viele Zugänge immer das Selbe verwendet wird. Auch die Auswahl des Kennwort selbst lässt zu wünschen übrig. Lautet Ihr Kennwort etwa auch 123456, password, qwertz , asdfg oder abc123? oder hängt es auf einem Notizzettel am Bildschirm?

Hacker haben Werkzeuge, mit denen sie sich vollautomatisch Zugang verschaffen können, in dem sie alle gängigen Kombinationen aus einem Wörterbuch häufig verwendeter Kennwörter durchprobieren. Bei der Wahl Ihres Kennwortes, sollten Sie sich daher mindestens an die folgenden Empfehlungen orientieren.

- keine Namen von Familienmitgliedern
- mindesten 8, besser 12 Zeichen, je länger, desto besser
- Groß- und Kleinbuchstaben verwenden
- Ziffern und Zeichen verwenden (!?%&+-)

Damit Sie sich ein so erstelltes Passwort selbst leicht merken können, verwenden Sie eine Eselsbrücke, mit den Anfangsbuchstaben der Worte aus einem Satz, z.B.:
Ich **h**abe **m**eine **F**rau **i**m **W**inter 1998 **i**n **U**lm **g**eheiratet.

und wandeln Sie zusätzlich den Buchstaben “i” in “1” und das “u” in “&” um.
Ihr Kennwort lautet also: 1hmF1W19981&g

Sie können aber auch einen Passwort-Generator verwenden und sich die Kennwörter in einem Passwort-Manager speichern. Das Masterpasswort zu diesem Manager sollte dann natürlich ein aufwendiges Kennwort sein.

Desweiteren können Sie das Sicherheitsniveau eines Zugangs mit einem zweiten Sicherheitsfaktor erheblich erhöhen. Wenn ein Dienst eine solche Zwei-Faktor-Authentifizierung (2FA) anbietet, sollten Sie ihn also unbedingt benutzen. Das kann ein in Fingerabdruck, ein Code per E-Mail oder SMS, oder ein Code einer Authenticator-App sein.

Datensicherung durchführen

Datensicherung dürfte wohl der Wichtigste aller Punkte sein und dennoch gerät er bei einigen Endanwendern und kleinen Unternehmen immer wieder aus dem Fokus. In manchen Fällen reicht es schon aus, wenn man sich seine eigenen Dateien auf ein USB-Stick kopiert. Vorausgesetzt man wiederholt es regelmäßig, wenn neue Daten dazugekommen sind, oder sich geändert haben. Einfacher ist es jedoch, wenn man eine externe Festplatte an den USB-Anschluss des Rechners bzw. MACs anschließt. Beim MAC regelt das die Time Maschine nach Bestätigung sofort ohne weiteres zutun vorbildlich. Bei einem Windows 10 Rechner muss man dafür einen Assistenten bemühen, den man in der Systemsteuerung unter System und Sicherheit unter dem Punkt Sichern und Wiederherstellen findet. Die Sicherung auf eine externe Festplatte macht nur Sinn, wenn es im Privatbereich um einen einzelnen Rechner geht. Geht es um ein kleines Unternehmen, mit mehreren Rechnern, werden die Daten sinnvollerweise zentral von einem sog. Netzwerkspeicher (NAS) gesichert, bzw. liegen die Daten gleich im Netzwerk und nicht auf den jeweiligen Rechnern. In größeren Unternehmen werden die Mitarbeiter deshalb auch immer darauf hingewiesen, dass sie wichtige Daten nicht auf ihrem Desktop ablegen sollen, sondern direkt auf dem Netzlaufwerk, welches dann gesichert wird.

Internet mit Vorsicht nutzen

Auch im Internet sollten Sie stets darauf achten, was in anklicken und skeptisch sein wenn Ihnen eingeredet wird, Ihr Rechner sei gefährdet und nur mit diesem Virenscanner wieder geschützt, den sie gratis bekommen, wenn Sie hier klicken. Damit bewirken Sie meistens das Gegenteil. Solche Meldungen sollten Sie ignorieren. Windows 10 ist von Haus aus mit einem hervorragenden Virenscanner ausgestattet. In größeren Unternehmen wird hingegen ein zusätzlicher Virenscanner eingesetzt um die Geräte zentral verwalten zu können um mehr Kontrolle über den Datenverkehr zu haben.

Seien Sie sparsam beim Umgang mit Ihren persönlichen Daten. Geben Sie Ihre Daten nur auf Seiten ein, von denen Sie absolut sicher sind, dass es sich um eine

seriöse Seite handelt, bzw, um die Seite handelt von der Sie glauben, dass sie es auch ist. Ebenso kann es sinnvoll sein, wenn Sie sich für bestimmte Kategorien von Anmeldungen eine eigens dafür vorgesehene Email-Adresse erstellen. Mit Gmail-Adressen ist das z.B. relativ einfach. Nehmen wir an, Sie haben eine Gmail-Adresse nach dem Muster vorname.nachname@gmail.com, wenn Sie sich für einen Newsletter anmelden wollen, geben Sie als E-Mail-Adresse in diesem Fall einfach vorname.nachname+newsletter@gmail.com an. Somit lassen Sich im Email-Client wesentlich leichter Filter-Regeln erstellen.

E-Mails mit Vorsicht nutzen

Das ursprüngliche Format der E-Mail, ist das Textformat also einfach nur reiner Text, ohne Formatierungen. Im Laufe der Zeit hat sich das geändert und E-Mails wurden formatiert. Bei den später, meist für Werbung eingeführten HTML-Mails, hat man als Mail im Prinzip eine kleine Miniwebseite. Die Gefahr dabei ist Programmcode und Phishing, der sich dahinter verbergen kann.

So lässt sich einiges hinter der Oberfläche verschleiern und man kann leicht auf eine andere Seite gelenkt werden, als eigentlich angezeigt wird. Der Grund ist klar. Hier soll z.B in einer gefälschten Mail von einer Bank, dazu aufgefordert werden, PIN und TAN einzugeben. Doch keine Bank würde das in einer E-Mail von Ihnen verlangen.

Also, niemals derartigen Aufforderungen folgen und auf jeden Fall auch keine E-Mail-Anhänge öffnen, von Absendern die Sie nicht kennen. Trotzdem sollte man auch bei suspekten Anhängen von Freunden und Bekannten vorsichtig sein, da sie selbst unfreiwillig und unwissend Malware im Anhang bei der Versendung von E-Mails verbreiten können. Im Zweifelsfall löschen oder beim Absender nachfragen.

Suspekt sollte es Ihnen auch erscheinen, wenn Sie Rechnungen erhalten, die Fehler in der Rechtschreibung oder Grammatik enthalten und zudem als Word-Dokument und nicht als PDF versendet werden. Oft werden solche Mails automatisch ins Deutsche übersetzt, wodurch grammatikalischer Unsinn entsteht. Das sollte Ihnen gleich ein Zeichen dafür sein, das es mit dieser E-Mail nichts Gutes auf sich haben kann.

Fazit

Hundertprozentige Sicherheit gibt es nicht. Der unsicherste Faktor bleibt der Mensch. Wer alles glaubt, was er liest und allen Handlungsaufforderungen unbedacht, oder im Klickreflex nachgeht, wird irgendwann sein blaues Wunder erleben. Darauf sind Autoren von Schadsoftware spezialisiert.

Auch wer nach Möglichkeiten sucht, eine sonst teure Software irgendwo kostenlos zu bekommen, fällt oft auf Seiten rein, die es genau darauf ausgelegt haben. Auf solchen Seiten ist besondere Vorsicht geboten. Nichts gibt’s ohne Hintergedanken

wirklich umsonst. Da soll gelockt werden und schon hat man eine Seuche auf dem Rechner. Also, nichts zu schnell anklicken und kostenlosen Angeboten erstmal skeptisch gegenüberstehen und im Zweifel nach Kritik zu einem Thema googlen. Da kann man schon mal gewarnt sein, was da auf einen zugekommen wäre.

Ich hoffe die Tipps konnten Ihnen etwas behilflich sein und Sie konnten davon vielleicht auch etwas umsetzen oder Ihnen wenigstens zu denken geben. Es ersetzt auf keinen Fall eine persönliche Beratung, die auf die individuellen Umstände Rücksicht nehmen kann.

Falls Sie weitere Fragen haben, scheuen Sie nicht, mich zu kontaktieren.

Ich wünsche Ihnen noch eine schöne und sichere Zeit

Ihr
Marco Uras