Empfehlungen zur Erhöhung der Datensicherheit für private Computer

zusammengefasst von Kurt Kimmel

Nach dem kürzlich versuchten Hackerangriff auf Internet Router eines großen Telekommunikations- Anbieters ist sicher bei vielen Bürgerinnen und Bürgern wieder einmal das beklemmende Gefühl entstanden, dass womöglich der eigene PC auch schon von einem dieser Hackerangriffe betroffen war oder einmal betroffen sein wird. In der Tat, die Wahrscheinlichkeit, dass es jemand auch auf Ihren PC und die darauf liegenden Daten bzw. auf Ihre Identität im Netz abgesehen hat, liegt in der Tat bei nahezu 100%. Denn jeder, der seine Email-ID zum Online Shopping, in sozialen Netzwerken oder einfach zum Austausch von Nachrichten per Email verwendet hat, ist im Netz bekannt, seine Email Adresse wurde ausspioniert und womöglich schon in Datenbanken von Gruppen mit kriminellen Absichten abgespeichert.

Diese E-Mail Adressen sind dann die Eintrittskarte zum Versenden von Massen-Emails, auch Spam Mails genannt, die wiederum Links mit den dann gefährlichen, ausführbaren Programm Codes enthalten, die Ihren PC weiter ausspionieren können, oder, noch schlimmer, Ihre Daten darauf vielleicht verschlüsseln und sie ohne den zugehörigen Schlüssel – und dem damit verbundenen Erpressen von Geldzahlungen, von Ihnen nicht mehr gelesen werden können. Ist ihr PC erst einmal von Schadsoftware befallen, können Kriminelle Ihre Zugänge zu Online Shops ausspionieren und dann z.B. Waren in Ihrem Namen und auf Ihre Kosten bestellen oder ggf. auch Transaktionen beim Online-Banking manipulieren.

Es gibt vielfältige Möglichkeiten, wie dubiose und kriminelle Gruppen Ihren PC attackieren können, an dieser Stelle können nur einige Beispiele genannt werden. Auch gibt es keinen ultimativen Schutz vor solchen Angriffen, aber jeder kann einiges dafür tun, dass es potentielle Angreifer aus dem Netz zumindest deutlich schwerer haben. Deshalb möchten wir Ihnen hier noch einmal die wichtigsten Maßnahmen aufzeigen, wie sie auch von vielen Fachleuten und der Polizei empfohlen werden:

1) Benutzen Sie immer ein aktuelles Betriebssystem für Ihren Computer, also z.B. die aktuelle Version von Windows 7 oder Windows 10. Aktivieren Sie automatische Updates, nur so können vorhandene Lücken im System vom Hersteller nach Bekanntwerden geschlossen werden. Benutzen Sie also keine alten Versionen mehr, wie z.B. Windows XP! Dies wird nicht mehr vom Hersteller gewartet, bestehende, bisher unbekannte Sicherheitslücken werden daher nicht mehr geschlossen. Auch ist es wichtig die sonstigen Zusatzprogramme wie z.B. den Adobe Flash Player oder Ihren Internet Browser wie z.B. den Internet Explorer, Mozilla Firefox oder Google Chrome immer aktuell zu halten.
2) Verwenden Sie nicht den Administrator User im Windows zum täglichen Gebrauch. Erstellen Sie stattdessen einen zweiten Benutzer mit einem eigenen (natürlich anderen) Passwort als der Administrator) in ihrem Windows System, der eben nur normale Nutzerrechte hat, eben keine Administrator Rechte. Würde ein Virus oder eine manipulierte

Software Änderungen an Ihrem Betriebssystem vornehmen wollen, so müssten Sie das Administrator Passwort manuell eingeben. Werden Sie von Windows zur Eingabe des Administrator Passwortes aufgefordert, so sollte sie das äußerst misstrauisch werden lassen. Im Zweifelsfall lieber ablehnen und einen gesamten Scan ihrer Festplatte durch Ihr (ständig aktualisiertes) Virenschutzprogramm vornehmen lassen.

3) Kaufen Sie sich eine gute Sicherheitssoftware, wie z.B. Norton Security, Avira oder Kaspersky Internet Security und aktivieren sie den automatischen Update mindestens einmal die Woche, wer viel am PC Online arbeitet, besser täglich. Nur ein aktuelles Sicherheitsprogramm bietet auch maximalen Schutz. Kostenlose Versionen hingegen hinken meistens hinterher und schützen meist nicht umfassend. Scheuen Sie nicht die Kosten dafür! Es ist wirklich wichtig!
4) Denken Sie über die Nutzung eines Password Managers nach. Dies ist eine Software, die alle ihre Passwörter sicher, weil verschlüsselt auf Ihrem PC abspeichert. Sie müssen sich nur noch ein „Master-Passwort" merken. Eine solche Software ist z.B. der Password Manager von der Firmen Steganos oder Kaspersky. Sie kostet nur wenige Euro im Jahr und helfen Ihnen komplexere Passwörter, die man sich nicht so einfach merken kann, zu benutzen.
5) Verwenden Sie starke Passwörter und nicht „123456", „Test", die Namen ihrer Liebsten oder Wörter, die in einem Lexikon zu finden sind. Ein moderner Computer knackt solche einfachen Passwörter innerhalb Sekunden. Verwenden Sie auch Groß- und Kleinbuchstaben, Sonderzeichen (z.B. !+_)$), ein Passwort sollte aus mindestens 10, besser aus noch mehr Zeichen bestehen! Oder, wenn Sie einen Password Manager besitzen, lassen Sie sich von diesem Programm sehr sichere Passwörter generieren. Ändern Sie auch in regelmäßigen Abständen Ihre Passwörter. Wie kürzlich wieder aus der Presse zu lesen war, werden auch immer wieder die Internet Betreiber oder Mail Anbieter angegriffen und Online-Konten gestohlen. Wer regelmäßig seine Passwörter ändert, kann ein Missbrauch z.B. seines Email Kontos entgegenwirken.
6) Öffnen sie NIE Dateien dubioser Absender, auch keine darin befindliche PDF oder sonstige Dateien. Diese Dateien können Hacker-Software enthalten, sobald einmal angeklickt, installiert sich diese auf Ihrem Computer. Klicken Sie auch nicht auf Links in Emails, die sie nicht kennen. Löschen Sie am besten alle dubiosen Emails aus ihrem Postfach und vertrauen Sie nur Absendern, die Sie kennen. Bedenken Sie, dass Sie Rechnungen und sonstige wichtige Informationen in den aller seltensten Fällen von für Sie unbekannten Personen erhalten.
7) Verwenden Sie mehrere Email Adressen. Alle Email Provider bieten sogenannte Alias oder Wegwerf- Adressen, die Phantasienamen enthalten können, sodass man anhand der Email Adresse erst einmal nicht auf ihren tatsächlichen Namen schließen kann. Verwenden Sie für Online Bestellungen oder für soziale Netzwerke diese Wegwerfadressen. Wechseln Sie durchaus mal diese Adressen indem sie sich einfach eine neue generieren und die alte löschen. Ihre Haupt-Email-Adresse verwenden Sie nur für die persönliche Kommunikation mit Ihnen bekannten Personen. Am ratsam ist es, bei einem anderen Anbieter eine weitere Email Adresse für rein persönliche Mails zu nutzen. Manche Email Anbieter blockieren auch

bei Verdacht ihre Adresse und können Sie dann über ihre zweite Email Adresse darüber benachrichtigen.

8) Informieren Sie sich regelmäßig beim Bundesamt für Sicherheit in der Informationstechnologie (BSI). www.bsi.de Dort finden Sie viele weitere „Bürger-Informationen“ unter www.bsi-fuer-buerger.de zur sicheren Einrichtung Ihres Computers und Smartphone. Lesen Sie die Empfehlungen!
9) Erstellen Sie regelmäßige Sicherungen (Backups), z.B. auf eine externe Festplatte (einfach per USB Anschluss) oder vielleicht auch bei Ihrem (seriösen) Internet Anbieter, als Backup in die Cloud! Die externe Festplatte sollte nach der Sicherung wieder vom Computer getrennt werden. Das Sichern auf eine externe Festplatte ist einfach und ermöglicht das Wiederherstellen ihrer Daten, sollte ihr Computer doch einmal von Schadprogrammen befallen worden sein.

Das Arbeiten mit dem Computer ist heutzutage kaum noch aus dem täglichen Leben wegzudenken. Beachten Sie aber bitte immer, dass mit der Nutzung der benötigten Software auch Kosten verbunden sind, es „kostenlose“ Angebote nicht geben kann, denn niemand arbeitet für umsonst. Auch das beliebte „googeln“ ist z.B. nicht für Sie „kostenlos“ – die Anbieter von Suchmaschinen erstellen Nutzerprofile von Ihnen und vertreiben die daraus gewonnenen Erkenntnisse weiter. KAUFEN Sie sich also die benötigte Software, insbesondere die Sicherheitssoftware. Diese kosten oft im Jahr nicht mehr als eine Tankfüllung. Das sollte es Ihnen wert sein.

Die hier aufgeführten Ratschläge sind sicher nicht vollständig, dafür ist die Materie zu vielfältig und komplex geworden. Wenn Sie die wenigen Punkte aber befolgen, wird es deutlich schwerer sein, an Ihre Daten oder an Ihre Identität heranzukommen oder Ihren Computer mit Schadprogrammen zu infizieren. Alle hier aufgeführten Tipps und Vorschläge erfolgen natürlich ohne Gewähr, letztendlich sind Sie selbst für die Sicherheit Ihres Computers verantwortlich. Im Zweifelsfall fragen Sie einen Experten oder lassen Sie sich unterstützen.

Bleiben Sie vorsichtig!

Ihr CDU Ortsverband Meckenheim/Pfalz