excubits.com
Einfach. Sicher. Excubits.

PC-Sicherheit in 7 Schritten

Schritt 1: Weniger ist mehr.

Jedes zusätzlich angeschlossene Gerät und jedes installierte Programm vergrößern die Möglichkeiten, Ihren Computer zu hacken. **Überlegen Sie genau, ob Sie ein neues Programm brauchen**. Prüfen Sie, ob Ihre bereits installierten Programme nicht das können, was Sie suchen. So hat Windows zum Beispiel im Mediaplayer eine Funktion, um CDs zu kopieren oder zu brennen. Auch Fotos lassen sich mittlerweile mit dem internen Fotoprogramm gut bearbeiten. Weitere Vorteile der Programm-Sparsamkeit: Sie sparen Geld, haben mehr Platz auf der Festplatte, verbringen weniger Zeit mit Updates der vielen Programme und haben einen Computer, der schneller arbeitet.

Schritt 2: Nur legal ist sicher.

Installieren Sie nur Programme aus legalen Quellen, am besten direkt vom Hersteller. Programme sind wie neues Zubehör fürs Auto. Hand auf´s Herz: Würden Sie geschenkte Bremsbeläge im Hinterhof von dubiosen Mechanikern einbauen lassen? Genau! Eher nicht. Machen Sie es deswegen auch nicht bei Ihrem Computer. Sie wollen, dass Ihre Programme richtig funktionieren und keine Schadfunktionen besitzen, die Hacker in vermeintlich kostenlose Programme einbauen.

Schritt 3: Aktualisieren, aktualisieren, aktualisieren.

Programme haben Fehler. Diese bieten leider Schlupflöcher für Hacker. Siehe Schritt 1: Weniger Programme bedeutet mehr Sicherheit. Weil ein Computer ohne Programme sinnlos ist, brauchen Sie natürlich bestimmte Programme. Und diese Programme sollten Sie regelmäßig aktualisieren, also updaten. Solche Updates zu suchen und zu installieren macht wenig Spaß. Doch auch Zähneputzen ist langweilig. Trotzdem machen wir es. Und damit Sie auch morgen noch sicher am PC arbeiten können, sollten Sie regelmäßig Updates suchen und installieren. Sie könnten sich zum Beispiel immer am 1. jeden Monats um die Updates kümmern. Tragen Sie sich diesen Tag fest in den Kalender ein und sehen Sie diese Zeit nicht vergeudet. Denken Sie daran, dass Sie sich auch regelmäßig die Zähne putzen, die Haustür abschließen, sich im Auto anschnallen. Auch Updates gehören in diese Aufzählung der Dinge, die Ihr (Berufs-) Leben sicherer machen.

Schritt 4: Schutz- und Sicherheitsprogramme nutzen.

Sie sollten ein **Antivirenprogramm** nutzen. Die Betonung liegt dabei auf „ein". Denken Sie an Schritt 1: Weniger ist mehr. Dies gilt auch für Antivirenprogramme. Windows verfügt bereits automatisch über ein

solides Antivirenprogramm: Der Microsoft Defender. Auch die Experten der renommierten Fachzeitschrift c't raten dazu, den Defender zu benutzen. Egal welches Antivirenprogramm Sie benutzen, sollten Sie es regelmäßig aktualisieren. Führen Sie auch regelmäßig eine Prüfung Ihres Computers durch. Lassen Sie das Antivirenprogramm einmal im Monat nach Bedrohungen auf Ihrem Computer suchen.

Weitere **Schadcode-Scanner**: Der heise-Verlag veröffentlicht mehrmals im Jahr ein Sonderheft mit dem Prüfprogramm desinfec't. Auf der Seite botfrei.de finden Sie einen kostenlosen Schadcode-Scanner, der in einem gemeinsamen Projekt des Bundesamtes für Sicherheit in der Informationstechnik (BSI), des eco-Verbands und mit Unterstützung des Innenministeriums und Antiviren-Unternehmen entstanden ist.
Beide Programme können Sie ab und zu neben Ihrem (einzigen) Virenscanner für eine vollständige Prüfung Ihres Computers nutzen.

Wir empfehlen zudem auch ein Programm zur Ausführungskontrolle: Application-Whitelisting. Mit diesem legen Sie fest, welche Programme auf Ihrem Computer gestartet werden dürfen. So können Sie verhindern, dass Schadprogramme (Viren, Trojaner, Keylogger) auf Ihrem Rechner starten. Unser Produkt Türsteher ist die perfekte Ergänzung zum Antivirenprogramm. Auch die Experten vom BSI empfehlen, Application-Whitelisting einzusetzen.

Schritt 5: Schalten Sie Ihr Gehirn ein.

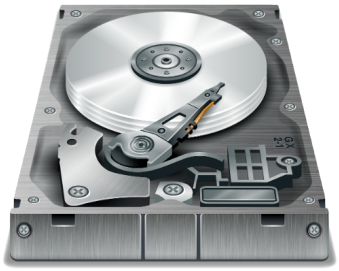
Die allermeisten Menschen fangen sich durch einen E-Mailanhang einen Virus, Trojaner oder Ransomware ein. Dabei können Sie diese Gefahr stark reduzieren, indem Sie „nur" Ihren Verstand nutzen:

- Haben Sie wirklich etwas bestellt?
- Kennen Sie den Absender?
- Erwarten Sie eine Bewerbung?
- Werden Sie stark unter Druck gesetzt?
- Sollen Sie in der E-Mail etwas anklicken, um zum Beispiel zu erfahren, wie viel Geld die Kollegin nach der Gehaltserhöhung bekommt?

Jede E-Mail, die von der Norm abweicht, die Ihnen irgendwie seltsam vorkommt oder deren Inhalte zu gut sind, um wahr zu sein, Sie unter

Druck setzt oder Sie womöglich sogar erpresst, sollten Sie mit Vorsicht betrachten. Rufen Sie lieber die gewohnte Webseite auf, um nachzusehen, ob Ihr Paket auf dem richtigen Weg ist. Banken, Dienstleister, Onlineversandhändler, Webbetreiber **fragen niemals in E-Mails nach Passwörtern**. Nehmen Sie sich Zeit, um über die nächsten Schritte nachzudenken. Fragen Sie beim Absender nach, ob er Ihnen wirklich eine E-Mail mit Anhang oder Link gesendet hat. Der Absender einer E-Mail lässt sich leicht fälschen. Die vermeintliche E-Mail Ihres Kollegen oder der Freundin kann gefälscht sein! Eile verführt oft zu schlechten Entscheidungen. Seien Sie misstrauisch und vorsichtig.

Schritt 6: Goldmünzen im Tresor sind wie Sicherheitskopien auf externen Festplatten.



Legen Sie Sicherheitskopien Ihrer persönlichen Daten an, am besten einmal in der Woche. Speichern Sie die Sicherheitskopien auf externen Datenträgern, wie Festplatten oder USB-Sticks. Ganz wichtig: Sind Ihre Daten als Sicherheitskopie auf der Festplatte, dann trennen Sie die Festplatte oder den USB-Stick vom Computer. Legen Sie die Sicherheitskopie an einen sicheren Ort, zum Beispiel in einen Schrank. Und wenn Sie sehr viel Wert auf Sicherheit legen, dann sollten Sie die kopierten Daten auf der Festplatte auch noch verschlüsseln, zum Beispiel mit VeraCrypt. **Es gilt der Satz: Kein Backup. Kein Mitleid.** Soll heißen: Wir leben im Jahr 2020, Sicherheitskopien sind elementar wichtig und wer das immer noch nicht weiß, ist selbst schuld!

Schritt 7: Bitte nicht füttern!

Beim Fleischer oder beim Bäcker fragen die Verkäufer immer, bevor sie dem Kind ein Stückchen Wurst oder ein Bonbon geben dürfen. Auch Pferdebesitzer schreiben in großen Lettern „Bitte nicht füttern" auf den Zaun der Koppel. Auch Sie als Besitzer eines Computers sollten sehr genau darauf achten, was in Ihren PC gesteckt wird und wer das macht. Jede CD, jeder USB-Stick, jede Festplatte kann sehr schnell Viren, Trojaner, Keylogger oder sonst etwas auf Ihrem PC transportieren. Sie sollten Ihren PC auch nicht unbeaufsichtigt lassen auf Messen, im Zug oder bei einer Konferenz. Sollen wir es wirklich noch einmal schreiben? Ja: Stecken Sie niemals auf der Straße, in der Bahn oder im Bus gefundene USB-Sticks in Ihren PC! Oder geben Sie Ihrem Kind ein Bonbon, das sie auf der Straße gefunden haben?

Schritt 7,5: Müssen wir wirklich noch etwas zu Passwörtern sagen?

Nutzen Sie ein Passwort nicht mehrmals. Ein Passwort pro Zugang. Nehmen Sie keine Passwörter wie 12345, Maria, Jesus, Passwort, qwertz oder ähnlich. Ein gutes Passwort könnte zum Beispiel aus den Anfangsbuchstaben eines Satzes entstehen: **MHh3sO,wn?** (**M**ein **H**und **h**at **3 s**chiefe **O**hren**, w**as **n**un**?**) So haben Sie Sonderzeichen, wie Komma und Fragezeichen, eine Zahl, Groß- und Kleinschreibung vereint. Perfekt ist, wenn Sie gar keinen Hund haben oder er auch nur ordnungsgemäß zwei Ohren hat. Sie können sich gute Passwörter auch aufschreiben. Lassen Sie den Zettel mit dem Passwort aber nicht in der Nähe des Computers liegen. Auch nicht unter der Tastatur. Für Fortgeschrittene und sehr sicherheitsbewusste Menschen helfen Passwort-Manager, z. B. keepass. Mit Passwort-Manager verwalten Sie Passwörter, außerdem helfen Sie Ihnen dabei, lange und sichere Passwörter zu erstellen.

Sieben ist eine schöne Zahl, deswegen haben wir diese gewählt. Für mehr Schutz gibt es immer auch noch mehr Schritte. Gerne unterstützen wir Sie bei einer Sensibilisierungsveranstaltung in Ihrem Unternehmen/Behörde.

Wenn Sie Fragen dazu haben oder uns Anregungen geben wollen, sprechen Sie uns gerne an.

Bildnachweis
https://pixabay.com/users/200degrees-2051452/
https://pixabay.com/users/OpenClipart-Vectors-30363/
https://pixabay.com/users/geralt-9301/