



## Alle Jahre wieder: Der digitale Frühjahrsputz

Der Frühling naht mit großen Schritten. Morgens auf dem Weg zur Schule, Arbeit oder Studium ist es schon hell, die Temperaturen steigen. Traditionell lädt die Jahreszeit auch dazu ein, auszumisten, aufzuräumen und aufzuhübschen. Da die Digitalisierung längst auch im Zuhause Einzug gehalten hat, bietet sich so auch die perfekte Gelegenheit, den Frühjahrsputz auf die technischen Helfer auszuweiten.

### Dazu ein paar Tipps:

#### 1. PC & Laptop

Das E-Mail-Postfach läuft über? Der Festplattenspeicher geht zur Neige? Das Gerät braucht immer länger bei Starten? Größere Festplatten und Speicherriegel, neue Mainboards und Prozessoren können zwar helfen, aber einer-

seits geht das ins Geld und andererseits gibt es kostenlose Möglichkeiten, dem Rechner die alte Leistung zu entlocken.

#### **Installierte Apps und Anwendungen prüfen**

Nehmen Sie sich die Zeit, durch die installierten Softwares zu gehen und sich zu fragen, wann Sie diese das letzte Mal benutzt haben und ob Sie sie überhaupt noch benötigen. Ungenutzte

Apps (so wie etwa die vorinstallierten Windows Store Apps) belegen unnütz Speicherplatz und sollten gelöscht werden.

### **E-Mails ausmisten**

Wenn Sie ein E-Mail-Programm wie Microsoft Outlook / Mail oder Mozilla Thunderbird & Co. benutzen, werden entweder ganze Mails oder deren Anhänge auch lokal auf dem Computer gespeichert. Manche Anbieter kostenloser Mail-Dienste bieten zudem auch online nur ein begrenztes Kontingent an Speicherplatz an. Lassen Sie sich die Mails nach Zeit in umgekehrter Reihenfolge anzeigen, also die ältesten zuerst, und entscheiden Sie, ob nicht eventuell der ein oder andere Zahlungsbeleg von 2010 oder älter, oder die Einladung zur Gartenparty von 2012 mittlerweile gelöscht werden können.

### **Der Download Ordner**

Sie haben einen oder mehrere, zentrale Download Ordner, wo sämtliches aus dem Web hin gespeichert wird? Dann öffnen Sie diesen und schauen, ob alle Downloads, wie etwa Installationsdateien oder Konzerttickets für vergangene Veranstaltungen usw. noch benötigt werden. Falls nicht, löschen Sie die entsprechenden Dateien. So kommen schnell mehrere Gigabyte an freiem Festplattenspeicher zum Vorschein.

### **Bilder & Videos**

Viele Nutzer haben eine gute und lange Historie an Bildern und Videos auf dem „Familien PC“ abgelegt. Stellenweise sind hier auch alte Fotos von mobilen Geräten mit beinhaltet. Nicht jedes Foto oder Video wird dabei ewig gebraucht. Trennen Sie sich von Schnappschüssen mit geringer Qualität sofort und lagern Sie die anderen Dateien auf externe Speicher aus. Das können DVDs, ein Netzwerk- oder Cloudspeicherdienst sein (siehe Punkt 4).

### **Systemstart-Einträge prüfen**

Moderne Betriebssysteme bieten den Nutzern die Möglichkeit, die beim Systemstart automatisch mit geladenen Anwendungen anzuzeigen und zu bearbeiten. Schauen Sie beim

digitalen Frühjahrsputz auch hier vorbei. Adobe Acrobat, Spotify, Steam, iTunes und manches mehr starten auch, wenn Sie sie ganz normal aufrufen, verzögern aber den Systemstart teilweise spürbar.

### **Updates**

Das Betriebssystem, die Anwendungen und Apps sollten ebenfalls mit gepflegt und mit eventuell vorhandenen Updates versorgt werden. Das spart zwar nicht unbedingt Speicherplatz, schützt Sie aber vor dem Ausnutzen von Sicherheitslücken und Schaden, der durch Softwarefehler entsteht.

## **2. Smartphone & Tablet**

„Das E-Mail-Postfach läuft über? Der Speicher geht zur Neige? Das Gerät braucht immer länger bei Starten?“ Sie sehen schon, die Problematiken sind ganz ähnlich denen, die wir vom „klassischen“ Computer her kennen. Daher ähneln sich auch die Tipps:

### **Installierte Apps und Anwendungen prüfen**

Nehmen Sie sich die Zeit, durch die installierten Apps zu gehen und sich zu fragen, wann Sie diese das letzte Mal benutzt haben und ob Sie sie überhaupt noch benötigen. Ungenutzte Apps belegen unnütz Speicherplatz und sollten gelöscht werden.

### **E-Mails ausmisten**

Wenn Sie ein E-Mail-Programm wie Apple Mail oder Gmail benutzen, werden entweder ganze Mails oder deren Anhänge auch lokal auf dem Gerät gespeichert. Manche Anbieter kostenloser Mail-Dienste bieten zudem auch online nur ein begrenztes Kontingent an Speicherplatz an. Lassen Sie sich die Mails nach Zeit in umgekehrter Reihenfolge anzeigen, also die ältesten zuerst, und entscheiden Sie, ob nicht eventuell der ein oder andere Zahlungsbeleg von 2010 oder älter, oder die Einladung zur Gartenparty von 2012 mittlerweile gelöscht werden können.

### Der Download Ordner

Sie haben einen oder mehrere, zentrale Download Ordner, wo sämtliches aus dem Web hin gespeichert wird? Dann öffnen Sie diesen und schauen, ob alle Downloads, wie etwa Bilder, Videos oder Konzerttickets für vergangene Veranstaltungen usw. noch benötigt werden. Falls nicht, löschen Sie die entsprechenden Dateien. So kommen schnell mehrere Gigabyte an freiem Festplattenspeicher zum Vorschein.

### Bilder & Videos

Viele Nutzer haben eine gute und lange Historie an Bildern und Videos auf dem Smartphone oder Tablet abgelegt und wissen es teilweise gar nicht. Unter anderem die Speicherordner von WhatsApp & Co belegen mit Spaßvideos und Gruppenbildern unnötig viel Speicherplatz. Trennen Sie sich von Schnappschüssen mit geringer Qualität sofort und lagern Sie die anderen Dateien auf externe Speicher aus. Das können Netzwerk- oder Cloudspeicherdienste sein (siehe Punkt 4).

### Updates

Das Betriebssystem und die Apps sollten ebenfalls mit gepflegt und mit eventuell vorhandenen Updates versorgt werden. Das spart zwar nicht unbedingt Speicherplatz, schützt Sie aber vor dem Ausnutzen von Sicherheitslücken und Schaden, der durch Softwarefehler entsteht.

## 3. Heimnetzwerk

Wissen Sie eigentlich aus dem Kopf, wie viele Geräte sich aktuell in Ihrem heimischen (W)LAN befinden? Nein? Dann gehören Sie zum größten Teil der Anwender und es ist Zeit, sich einen Überblick zu verschaffen!

### Netzwerkverwaltung & -übersicht

Auch für Leser, die nicht die Funktion „Sicheres Heimnetzwerk“ der ESET Internet Security und Smart Security Premium nutzen können, gibt es eine einfache Möglichkeit, die Geräte des heimischen Netzwerks zu erkennen. Dazu

öffnen Sie die Weboberfläche Ihres Heimrouters im Browser. Die Standard-Adresse ist entweder „192.168.0.1“ oder bei den beliebten Fritz!Box Modellen von AVM „192.168.178.1“. Schauen Sie auf die Box oder in die Begleitdokumente nach den entsprechenden Anmeldedaten. Einmal eingeloggt, finden Sie einen Punkt „Netzwerkübersicht“. Dieser sollte eine Liste aller Smartphones, Smart TV, Streamingsticks (Chromecast, FireTV Stick & Co.), Tablets, Computer, Wasserkocher, Webcams, Netzwerkspeicher, digitaler Assistenten und vieler Geräte mehr anzeigen. Unter Umständen kann es vorkommen, dass Sie dabei unbekannte Geräte entdecken oder solche, die Sie eigentlich gar nicht mehr benutzen. Sperren Sie die unbekanntes gleich über die Weboberfläche des Routers und trennen Sie sich von nicht benutzten Geräten.

### Netzwerksegmentierung

In der Regel werden die meisten Nutzer alle Geräte in einem einzigen Netzwerk „halten“. Das birgt jedoch die Gefahr, dass Angreifer über Schwachstellen des smarten Wasserkochers oder anderer Geräte nicht nur Zugriff auf das Gerät, sondern auch auf die im Netzwerk gespeicherten Daten oder Kameras und Mikrofone erhalten. Abhilfe schafft hier eine strikte Trennung der Geräte. Eine gute, günstige und einfach zu realisierende Möglichkeit bietet die Nutzung des Gäste-Wlans. Geräte, die lediglich eine Internetverbindung für den korrekten Betrieb benötigen, können als „Gäste“ behandelt werden und dem entsprechenden, zweiten Netzwerk zugeordnet werden. Sollte eines der Geräte übernommen oder kompromittiert werden, bleiben Ihre privaten Daten und Bilder sicher.

### Updates

Prüfen Sie zudem, ob alle Geräte und vor allem der Router mit den neuesten Updates versorgt sind! Schwachstellen in der Firmware werden immer wieder von Cyberkriminellen ausgenutzt.

## 4. Backup & NAS

Backups, also die regelmäßige Sicherung von Dateien, Fotos, Videos & Co auf externe Speichermedien, lassen sich heutzutage kostengünstig realisieren. Netzwerkspeicher (Network Attached Storage – NAS) gibt es für unter 100 Euro mit mehreren Terrabyte Speicherplatz im Handel. Dazu kommen die Cloudspeicher-Angebote von Google Drive, Microsoft One Drive, Apple iCloud, Dropbox und vielen mehr, welche teilweise kostenlos sind.

### Stick, NAS oder die Cloud?

NAS und Cloudspeicher haben gegenüber USB-Stick und selbst gebrannter DVD den Vorteil, dass die Daten nahezu ausfallsicher gespeichert werden. Werden der Stick oder die DVD gestohlen oder erleiden physischen Schaden, sind die Daten darauf verloren. Fällt eine Platte im NAS aus, ist der Inhalt oft auf einer zweiten gespiegelt (RAID) – prüfen Sie, ob Ihr NAS über ein RAID verfügt. Daten, die in der Cloud abgelegt werden, sind mehrfach gespiegelt und gehen nur im äußerst unwahrscheinlichen Fall verloren. Außerdem kann man in den meisten Fällen von überall aus der Welt, außerhalb des Heimnetzwerks, auf die Daten zugreifen. Genau da liegt aber auch für sicherheitsbewusste Anwender das Problem: Die Daten sind außerhalb meines Netzwerks, ich muss mich als Anwender für den Schutz und Vertraulichkeit dieser Daten auf die Dienstbetreiber verlassen.

### Lokale Backups

Zu den lokalen Backup-Möglichkeiten zählen wir alle „daheim sichtbaren“ Medien, wie USB-Sticks, USB-Festplatten, CD/DVD, NAS usw. Diese sind leicht zu kontrollieren und gegebenenfalls zu verstecken, haben jedoch auch Nachteile. Bis auf das NAS haben wir keine oder kaum RAID-Funktionalitäten, also eine Ausfallsicherheit. Außerdem sollte darauf geachtet werden, dass die Sicherungsmedien nicht ständig mit dem Computer oder Smartphone (über das Netzwerk) verbunden sind. Fällt ein System einem Verschlüsselungstro-

janer zum Opfer, wird dieser versuchen, auch die Inhalte auf angeschlossenen Speichermedien zu „kidnappen“. Kreieren Sie also ein Ritual: Nach getaner Arbeit (Fotos erstellen/bearbeiten, Texte schreiben etc.) verbinden Sie das Speichermedium mit dem Computer oder Smartphone und sichern die neuen Daten. Danach trennen Sie das Backupmedium wieder. Sind die Speicherinhalte Updates von bereits vorhandenen Dateien, ersetzen Sie diese im Zielmedium. Zwingen Sie sich zudem, nur relevante Inhalte zu sichern. So sparen Sie nicht nur Speicherplatz, sondern auch das Aufräumen und „Durchforsten“ zu einem späteren Zeitpunkt.

### Backups in der Cloud

Die Speichermöglichkeiten in der Cloud sind teils kostenlos, nahezu ausfallsicher und dank plattformübergreifender Apps so gut wie überall nutzbar. Die gespeicherten Inhalte befinden sich aber auch außerhalb Ihres Kontrollbereiches. Sollten Strafverfolger, Regierungen oder Kriminelle Zugriff auf die Speicherserver irgendwo in der Welt erlangen, liegen Ihre Daten im schlimmsten Fall auf dem Präsentierteller. Da Sie ja nur wichtige, privat wertvolle Daten sichern, ist das unter Umständen ein großes Problem. Deaktivieren Sie eventuelle automatische Sicherungen Ihrer Smartphone-Bilder oder Dokumente. Kontrollieren Sie den Upload zu den Cloudspeicherdiensten darüber hinaus. Legen Sie bewusst Sicherungen in der Cloud an. Dazu gehört, dass die entsprechenden Daten mit einer zuverlässigen Verschlüsselung versehen sind, sodass nur Sie und von Ihnen autorisierte Personen und Apps diese lesen können.

## 5. Social Media & andere Webinhalte

Im Laufe der Zeit haben manche mehr als bereitwillig persönlichste Informationen mit der Welt geteilt. Ob bei Facebook oder dem bald nicht mehr existenten Google+, LinkedIn, XING und vielen sozialen Netzwerken mehr. Höchste Zeit, hier aufzuräumen!

## Postings in sozialen Netzwerken

Nicht wenige Nutzer sind bereits 10 Jahre bei Facebook und anderen Plattformen unterwegs. Teilweise gibt es einige nicht mehr (SchülerVZ), nicht mehr lange (Google+) andere nicht mehr in der bekannten Form (MySpace) oder werden einfach heutzutage ganz anders von uns benutzt (Facebook). Die „Erinnerungen“ bei Facebook etwa bieten eine gute Gelegenheit, alte Posts zu löschen oder deren Privatsphäre-Einstellungen anzupassen. Generell sollte man in sich gehen und überlegen, wo man was geteilt hat.

- Nutze ich MySpace, lastFm, knuddels, StudiVZ usw. überhaupt noch?
- Habe ich noch die Login-Daten bzw. die E-Mail-Adresse dazu noch?
- Kann ich das Konto nicht gleich löschen?

Das sind die Fragen, die es zuerst zu klären gilt. Anschließend prüft man bei noch verwendeten Plattformen, wie Facebook, Instagram, Twitter, YouTube usw., ob die Privatsphäre-Einstellungen noch meinen aktuellen Wünschen entsprechen, und ob Bilder oder ganze Alben, sowie einzelne Postings nicht vielleicht gelöscht werden können.

## Blogs und kostenlose Webseiten

Manche vergessen im Alltag den Blog, der zur Schul- oder Studienzeit angelegt wurde, – vielleicht sogar, bevor man für seine Inhalte YouTube, Facebook, Instagram und mehr entdeckt hat. Höchste Zeit, auch hier zu überlegen und zu prüfen, ob der Blog noch existiert und ob ich überhaupt noch möchte, dass die entsprechenden Inhalte und Seeleneinblicke aller Welt zur Verfügung stehen.

## 6. Passwörter & Zugänge

Nein, an dieser Stelle fordern wie Sie NICHT auf, alle Passwörter, die Sie benutzen, regelmäßig zu ändern. Studien und die eigene Erfahrung zeigen, dass dies allein nicht dafür sorgt, dass die Sicherheit steigt.

Stattdessen geben wir folgende Tipps:

## Passwortmanager

Passwortmanager sind gut, günstig und wertvoll. Teilweise sind sie, wie etwa in der ESET Smart Security Premium, als Feature in Security-Programmen enthalten. Gute Manager bieten nicht nur die Möglichkeit, plattformübergreifend mit entsprechenden Apps und Browser-Plugins, die gespeicherten Passwörter zu nutzen. Sie bieten auch die Möglichkeit, hochkomplexe Passwörter zu kreieren. Der Nutzer hat lediglich die Schwierigkeit, sich ein Master-Passwort zu merken. Das hilft, für jeden Anwendungszweck ein neues Passwort zu verwenden und niemals Logins wiederzuverwenden. Letzteres stellt die größte Gefahr durch Passwort-Diebstahl dar. Um sich das Master-Passwort leichter einzuprägen und die Sicherheit zu erhöhen, empfiehlt es sich, keine Abkürzungen oder einzelne Wörter, sondern lieber Passphrasen und ganze Sätze, inklusive aller Satz- und Leerzeichen zu verwenden. Auf diese Weise kommen schnell mehr als 40 Zeichen zusammen, was ein automatisches Durchprobieren durch Scripte erschwert. Allerdings sollte der Satz nicht im Zusammenhang mit dem Anmeldezweck stehen. Nutzen Sie deshalb NICHT „Ich melde mich am Passwortmanager an!“...

## E-Mail-Passwort

Ein Passwort, das Sie vielleicht doch ändern sollten, ist das Ihres E-Mail-Accounts, mit dem Sie sich bei Facebook, Amazon, eBay & Co. anmelden. Wird das Passwort auf einer Plattform gestohlen, probieren Kriminelle häufig automatisch die gleiche Kombination aus E-Mail-Adresse und gestohlenem Passwort als Login beim Mail-Provider. Haben sie Zugang zum Postfach, nutzen sie die die „Passwort vergessen“ Option anderer Plattform-Anbieter, um so Zugriff auf die anderen Dienste zu bekommen. Sofern möglich, aktivieren Sie zusätzlich die Option, dass Sie über alle Logins informiert werden und das Ändern von Passwörtern auf einem anderen Weg (zweite Mail-Adresse bei einem anderen Anbieter oder Push-Nachricht auf dem Smartphone) bestätigen müssen.

## 2-Faktor-Authentifizierung

Die 2-Faktor-Authentifizierung, oder auch „Anmeldung in zwei Schritten“ ist eine hervorragende Möglichkeit, trotz gestohlener, wieder verwendeter oder zu einfacher Passwörter, Kriminellen die Tür vor der Nase zuzuschlagen. Das grundlegende Prinzip dabei ist, dass zusätzlich zum Nutzernamen und Passwort ein weiterer Faktor, wie ein Einmal-Code per SMS oder App, biometrische Informationen, wie die Gesichtserkennung oder Fingerabdrücke oder Zertifikatsinformationen über USB-Sticks o.ä. zum Einsatz kommen.

Die meisten Dienste, wie Facebook, Twitter, Google und Apple bieten diese Möglichkeit zum zusätzlichen Schutz an. Leider ist die Funktion nicht automatisch aktiv. Prüfen Sie, ob Ihr Anbieter diese Optionen bietet, suchen Sie gezielt danach und aktivieren Sie sie. Ohne auch Zugriff auf Ihr Smartphone o.ä. zu haben, können Diebe so selbst mit korrekten Login-Daten nicht an Ihre Informationen gelangen und Ihr Social Media Profil, Ihren eBay Account und Ihre E-Mails für betrügerische Aktionen missbrauchen.

## FAZIT

Auch wenn es auf den ersten Blick viel erscheint, dass es zu beachten gilt: Es lässt sich alles an einem oder zwei Sonntagnachmittagen erledigen. Wer diese Zeit für den klassischen Frühjahrsputz zu Hause benötigt, kann auch gern abends ein paar Stunden damit verbringen. Klar ist jedoch, dass dies nur die wichtigsten Grundlagen für das sicherere Benutzen unseres digitalen Alltags sind.

In diesem Sinne – Enjoy Safer Technology!