CAW 15.05.2019

- Aktuelles zu Windows 10 Frühjahr (1903) Update

- Digitaler Nachlass (Wiederholung)

- WLAN Probleme beheben

- Tipps und Tricks

- Beantwortung der Fragen

Vorbereitung für Update 1903

Alle vorbereitenden Updates müssen eingespielt sein / installierte Windows 10 Version muss aktuell sein.

Falls erforderlich / möglich aufräumen, das Mai Update benötigt 32 GByte Speicher für die Installation

(Datenträgerbereinigung, Speicheroptimierung, Systemsteuerung)

Backup erstellen, falls nicht permanent

(Einstellung – Update und Sicherheit – Sicherung) oder z.B. Paragon Backup & Recovery

Hinweis von Microsoft: Installation kann unter Umständen abbrechen wenn ein Datenträger per USB angeschlossen ist. Hintergrund ist, dass bei einem Neustart nach dem Update ggf. andere Laufwerksbuchstaben zugeordnet werden.
Ziehen Sie also vor dem Update USB-Sticks und externe Festplatten ab.

Digitaler Nachlass

Digitale Vorsorge – so gehen Sie vor

Aufbereiten:
Verschaffen Sie sich regelmäßig einen Überblick über Ihre Onlineaktivitäten. Listen Sie für jedes Konto die Zugangsdaten und Passwörter auf. Dann können Erben oder andere Vertrauenspersonen darauf zugreifen. Diese können etwa auf einem USB-Stick abgespeichert werden, der an einem sicheren Ort hinterlegt ist, oder in Passwortmanagern aufgelistet werden. Die Auflistung sollte regelmäßig aktualisiert werden.

Löschen:
Daten, die niemandem in die Hände fallen sollen, löschen Sie am besten von Zeit zu Zeit. Das können E-Mails oder Fotos sein.

Digitaler Nachlass

Testament:
Wer festhalten will, welche seiner Daten gelöscht und welche vererbt werden sollen, kann das in einem Testament regeln. Er kann auch eine Vertrauensperson zum digitalen Nachlassverwalter bestimmen und dies in einer Vollmacht festhalten.

Handgeschrieben:
Formulieren Sie alle Regeln zu Ihrem digitalen Nachlass persönlich von Hand. Auch für den digitalen Nachlass gilt: Nur ein hand-schriftliches und unterschriebenes Testament ist rechtswirksam.

Digitaler Nachlass

Informationen, die wir im Internet, aber auch auf Festplatten, USB-Sticks und Speicherkarten hinterlassen, gehören im Todesfall zur Erbschaft – genauer: zum digitalen Nachlass.

Der umfasst nicht nur gespeicherte Daten, sondern auch online geschlossene Verträge – ob mit Versandhändler, Reiseanbieter oder Auktionsplattformen.
Rechte und Pflichten gehen auf den Erben über.
Dieser muss den Mantel bezahlen, die Kreuzfahrt stornieren oder die ersteigerte Designer-Uhr abnehmen.
Die wenigsten Verträge enden mit dem Tod.
Auch Nutzerkonten bei sozialen Netzwerken und Versandhändlern bleiben erst einmal bestehen.

Digitaler Nachlass

Ohne Passwort kein Zugriff

Ohne Passwörter und andere Zugangsdaten wie Nutzernamen ist es schwierig, den digitalen Nachlass zu ordnen und die Pflichten des Verstorbenen zu erfüllen.
Kennt der Erbe ein Passwort nicht, kann er das dazugehörige Nutzerkonto nicht aufrufen und löschen.
Er muss sich an den Diensteanbieter, etwa den E-Mail-Provider, wenden. Die sind nach dem aktuellen Urteil des Bundesgerichtshof dazu verpflichtet, den Erben Zugang zu dem Konto zu gewähren.

Digitaler Nachlass

Google-Account: Den Kontoinaktivität-Manager nutzen

Wer einen E-Mail-Account bei Google hat, für den empfiehlt sich dessen Kontoinaktivität-Manager:
Der Nutzer kann bis zu zehn Personen benennen, die benachrichtigt werden, wenn er auf das Konto in einer von ihm festgelegten Wartefrist zwischen 3 und 18 Monaten nicht zugegriffen hat.
Die benannten Personen bekommen dann drei Monate Zeit, die relevanten Inhalte herunterzuladen.

Zur Schritt für Schritt Anleitung >Bei Google vorsorgen.

Digitaler Nachlass

Facebook-Konto

Nach dem Tod des Konto-Besitzers versetzt Facebook den Account in den "Gedenkzustand". Andere haben so keinen Zugriff auf das Konto. Facebook bietet in den "Einstellungen" die Möglichkeit, einen Nachlasskontakt zu bestimmen. Dieser muss selbst ein Facebook-Konto besitzen.

Achtung: Laut Allgemeiner Geschäftsbedingungen von Facebook ist es nicht erlaubt, sich in das Konto einer anderen Person einzuloggen. Zudem ist der Zugriff auf fremde Daten (also bspw. von Chat-Partnern des Verstorbenen) laut §202a StGB (http://dejure.org/gesetze/StGB/202a.html) möglicherweise strafbar. Ist der Weg über den Login in das Konto des Verstorbenen unumgänglich, z.B. wenn es um die Sicherstellung wichtiger Daten geht, sollten sich Hinterbliebene auf jeden Fall rechtlichen Rat einholen.

Twitter-Account

Angehörige von verstorbenen Twitter-Nutzern haben die Möglichkeit, den Account löschen zu lassen. Dazu müssen sie einen Löschantrag einreichen und entsprechende Dokumente bereitstellen, wie beispielsweise Personalausweis und Sterbeurkunde. Log-in-Informationen erhalten die Angehörigen laut Twitter aber nicht.

Digitaler Nachlass

Amazon Konto löschen

https://www.amazon.de/gp/help/customer/contact-us

EBAY Konto löschen

https://www.ebay.de/help/Account/changing-account-settings/ihr-ebaykonto-schlieen?id=4199

Alle Gebühren wurden bezahlt und Ihr eBay-Konto ist ausgeglichen.

Es laufen keine Gebote auf einen Artikel.

Falls Sie die Zahlungsabwicklung für Verkäufer nutzen, stehen keine Auszahlungen aus, die noch auf Ihr Bankkonto überwiesen werden müssen oder noch nicht abgewickelt wurden.

Digitaler Nachlass Zusammenfassung

Welche Daten/Accounts/Online-Mitgliedschaften etc. gibt es?

Wie lauten die jeweiligen Zugangsdaten?

Was soll mit dem jeweiligen Account/den jeweiligen Daten geschehen (Erhaltung/Löschung/Archivierung/Übertragung der Daten an eine andere Person)?

Wer soll sich darum kümmern?

Digitale Alternative zum analogen Dokument

Ebenso können sie alle Daten auch in einem Passwort-Manager speichern. Wichtig: Master-Passwort des Passwort-Managers und Zugang zu deinem Laptop/Smartphone/etc. analog sichern und z. B. deinem Testament beilegen.

WLAN Probleme beheben

Wenn Internet Anbieter und Streaming Dienst keine Probleme melden, ist oft eine schlechte WLAN Verbindung die Ursache für ruckelnde Bilder beim Streaming oder langsames Laden von Internet Inhalten.

Ein Grund kann ein veralteter Router sein (Übertragungsstandard „802.11g“)

Weitere Ursachen sind Funknetze in der Nachbarschaft, Signale können überlappen oder funken auf demselben Kanal. Dadurch wird die Datenübertragung im eigenen WLAN gedrosselt.

Auch DECT Telefone, Babyphone, etc. können den Funk stören

WLAN Probleme beheben

Wie lassen sich die Probleme beheben?

1. Der Router sollte wenn immer möglich zentral aufgestellt werden

2. Der Router sollte so hoch wie möglich aufgehängt werden

3. Nicht stehen sollte das Gerät in einer Ecke, hinter dicken Mauern oder Schränken.

Um den optimalen Standort zu finden, gibt es kostenlose Analysetools wie z.B. Wi-Fi Analyser, Fritz-WLAN-App oder Heatmapper.

Mittels dieser Tools auf Smartphone oder Laptop kann der beste Standort ermittelt werden.

WLAN Probleme beheben

4. Die Zahl der Geräte gleichzeitig im WLAN sollte so gering wie möglich gehalten werden.

5. Stationäre Geräte wie PC, TV oder Spielekonsole sollte per LAN angeschlossen werden.

6. Wechsel in das 5 GHz-Netz
(geringere Störanfälligkeit, höherer Datendurchsatz)

Allerdings unterstützen ältere Geräte diesen Standard nicht, finden somit auch kein WLAN.

Wer sicher sein will, setzt auf einen Router mit simultaner Dual Band Funktion, es wird in beiden Netzen gleichzeitig gefunkt.

WLAN Probleme beheben

7. Änderung des WLAN Kanals im Router, aktuelle Router finden den besten Kanal allerdings selbstständig und wechseln entsprechend automatisch.

Anmerkung: Änderungen im Router sind bedenkenlos möglich, sollte das WLAN dann nicht mehr funktionieren, lassen sich die Änderungen durch zurücksetzen des Routers zurücknehmen.

Ist die Reichweite auf Grund der örtlichen Gegebenheiten zu gering, lässt sich durch Einsatz eines **Repeaters** die Reichweite vergrößern.
Zu beachten ist, dass der Repeater zum Router passt.
Beispiel: Router funkt im „G“ Standard, dann ist Geld zum Fenster hinausgeworfen wenn ein Repeater mit „AC“ Standard gekauft wird.

Praktisch ist auch die Möglichkeit, größere Entfernungen durch Einsatz von **Powerline** zu überbrücken. **Voraussetzung: ein Stromnetz, ein Sicherungskasten.**

WLAN Standards

WLAN-Standard	Frequenzband	max. Bandbreite	Reichweite indoor
IEEE 802.11a	5 GHz	54 Mbits/s	35 Meter
IEEE 802.11b	2,4 GHz	11 Mbits/s	38 Meter
IEEE 802.11g	2,4 GHz	54 Mbit/s	38 Meter
IEEE 802.11n	2,4 und 5 GHz	600 Mbit/s	70 Meter (Wi-Fi 4)
IEEE 802.11ac	5 GHz	1300 Mbit/s	35 Meter (Wi-Fi 5)

Der neue Standard IEEE 802.11 AX (Wi-Fi 6)

Microsoft Konto in der Praxis

www.microsoft.com

E-Mail und Passwort

Tipps und Tricks

Man darf jetzt USB-Sticks einfach rausziehen !!

Bisher war es unter Windows Gesetz, dass man einen USB-Stick oder ein anderes angeschlossenes USB-Gerät nicht einfach abstöpselt, sondern vorher in der Taskleiste das entsprechende Symbol ansteuert und "Hardware sicher entfernen und Medium auswerfen" klickt. Tat man dies nicht, war theoretisch ein Datenverlust möglich, worauf das Betriebssystem bei Regelverstößen mit einer entsprechenden Meldung empört hinwies. Das ist jetzt vorbei, seit dem Oktober-Update darf man ein Gerät einfach abziehen, ohne einen Datenverlust oder eine Rüge zu riskieren. Nur wusste das bisher kaum jemand.

Nach dem Oktober Update ist die Standard-Einstellung "Schnelles Entfernen" . Das bedeutet, dass keine Daten zwischengespeichert werden (Cache), um die Systemleistung zu verbessern. Früher war die "Bessere Leistung" voreingestellt.

Tipps und Tricks

Das alte Prozedere stammt noch aus einer Zeit, als Medien noch nicht so schnell beschrieben wurden und man nicht sicher sein konnte, dass der Schreibvorgang beendet ist, wenn man sie vom USB-Eingang entfernte. USB-Sticks und andere moderne Medien sind aber viel schneller und die Gefahr, Daten zu verlieren, wenn man sie nach einem beendeten Kopiervorgang sofort abzieht, ist gering. Das ist auch ein Grund, weshalb sich ohnehin schon kaum noch jemand an die Regel gehalten hat.

Unter Umständen ist es aber besser, den alten Standard wiederherzustellen, beispielsweise wenn man Backups erstellt oder sehr wichtige Dateien kopiert. Außerdem kann - wie der Name schon sagt - "Bessere Leistung" einen schnelleren Schreibvorgang gewähren.

Um die Standard-Einstellung zu ändern, klickt man mit der rechten Maustaste unten links auf das Windows-Symbol und wählt dann Datenträgerverwaltung aus. Dort macht man einen rechten Mausklick auf den Datenträger und geht zu den Eigenschaften, wo man unter Richtlinien die Entfernungsrichtlinie bestimmen kann.

Emotet noch gefährlicher
Trojaner fälscht E-Mails nahezu perfekt

Von Meier, Antje <compromised.account@extern.tld>

Betreff **RE: AW: Angemieteter Parkplatz Musterstraße**

An Mueller, Bertram <Bertram.Mueller@musterfirma.de>

anbei findest du den Überweisungsbeleg, das Geld sollte also bald bei dir auf dem Konto sein.
Ebenfalls anbei der Scan der Vereinbarung.bitte Anhang beachten.

http://musterfirma.de/doc/B-3256-UV5323/Musterfirma_0451742669_April_09_2019.doc

http://super-plus.pl/css/oo6a-atf3y-frzom/

Mit freundlichen Grüßen,
Meier, Antje
antje.meier@musterfirma.de

Sehr geehrte Frau Meier,

vielen Dank für die schnelle Bearbeitung.
Den Schlüssel für die Tiefgarage gebe ich dann in der Hausmeisterei zurück, nehme ich an.

Viele Grüße
Bertram Müller

Von Emotet zuvor auf infiziertem System ausgespähte authentische E-Mail

-----Ursprüngliche Nachricht-----
Von: Meier, Antje
Gesendet: Donnerstag, 28. Juni 2018 13:48
An: Müller, Bertram
Betreff: AW: Angemieteter Parkplatz Musterstraße

Sehr geehrter Herr Müller,

hiermit bestätige ich Ihnen den Eingang Ihrer Kündigung vom 28.06.2018.
Die Kündigungsbestätigung und den Stellplatzvertrag für den Stellplatz Nr. 42 erhalten Sie in den nächsten Tagen.

Mit freundlichen Grüßen
Im Auftrag

Antje Meier

Beschreibung Trojaner

Ein Trojaner ist kein Virus, sondern ein destruktives Programm, das wie eine echte Anwendung aussieht. Im Gegensatz zu Viren replizieren sich Trojaner nicht selbst, können jedoch ebenso großen Schaden anrichten. Trojaner öffnen zudem eine Hintertür auf Ihrem Computer, über die bösartige Benutzer oder Programme Zugang zu Ihrem System erhalten und vertrauliche oder persönliche Informationen stehlen können.

Trojaner werden danach klassifiziert, wie sie Systeme infizieren und welche Schäden sie verursachen. Es gibt sieben Haupttypen von Trojanern:

- Trojaner, die Fernzugriff ermöglichen
- Trojaner, die Daten senden
- Destruktive Trojaner
- Proxy-Trojaner
- FTP-Trojaner
- Trojaner, die Security-Software deaktivieren
- Trojaner, die Denial-of-Service-Angriffe ausführen