

KOSTENLOS – Zur Mitnahme

Neuigkeiten und Informationen aus der IT

# Newsletter

Ausgabe Q3/2018

Themen dieser Ausgabe:

WPA3 Verschlüsselungsstandard beschlossen



Trend zu bewusstem Online- und Offlineleben



## Smartwatches und ihre Apps

Ist eine Spionage und ein Datenklau mittels Smartwatches möglich?



Top 10 Apps in Österreich

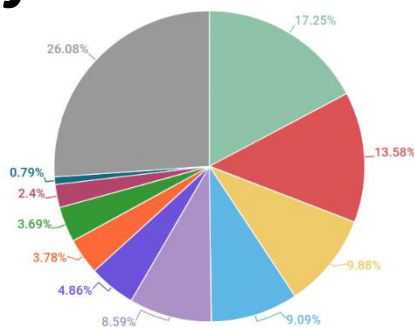


### Microsoft:

Windows 10 Update Historie und Office 2019



## Kaspersky Labs: Surfverhalten der Kids



● Video ● Online-Übersetzer ● Kommunikationsmedien im Internet ● Computerspiele  
● Inhalt für Erwachsene ● Bildung ● Musik ● Sport ● Einkäufe ● Anime ● Andere

Aktualisieren & Updates auf Ihren Geräten



Kaspersky Labs:  
„Krypto-Miner erfüllen unsere Prophezeiung“





## City PC EDV-Handel und Dienstleistung OG

Langgasse 29, A-8490 Bad Radkersburg

Tel.: (0043) 3476 / 40 397, www.citypc.at, office@citypc.at

Firmenbuchnr.: FN 328518 s, UID-Nr.: ATU65095899, Steuernr.: 228/6465

### Impressum

Herausgeber und Redakteur:

#### City PC EDV-Handel und Dienstleistung OG

Langgasse 29

A-8490 Bad Radkersburg

Tel.: 0043 (0) 3476 / 403 97

Fax: 0043 (0) 3476 / 403 97

Web: [www.citypc.at](http://www.citypc.at)

E-Mail: [office@citypc.at](mailto:office@citypc.at)

UID-Nr.: ATU65095899

Steuernr.: 228/6465

FB-Nr.: FN328518 s

Erfüllungsort und Gerichtsstand Bad Radkersburg

Dieser Newsletter dient hauptsächlich Informationszwecken. Druckfehler & Änderungen vorbehalten. Bilder müssen nicht den tatsächlichen Produkten entsprechen. Quellen der jeweiligen Artikel und Informationen finden Sie direkt bei den Artikeln. Falls angegeben verstehen sich alle Preise inkl. der österreichischen Mehrwertsteuer und ohne Versandgebühren (außer anders angegeben). Wir übernehmen keine Haftung für die Richtigkeit der jeweiligen Beiträge und Informationen.



### Öffnungszeiten

*Montag bis Donnerstag:*

8 bis 12:30 und 13:30 bis 17 Uhr

*Freitag:* 8 bis 12:30 Uhr

*Ihr EDV-Profi in der Region!*



#### Termindetails:

13.07. *RosenROT*

20.07. *KUNSTGenuss*

27.07. *WeisseNACHT*

03.08. *RegionERLEBEN*

10.08. *StreetFASHION*

17.08. *AtemLOS*

24.08. *WeinTRACHT*

31.08. *ModeHERBST*

07.09. *AltstadtFLOHMARKT*

## Trend zu bewusstem Online- und Offlineleben

Wie Google und Apple bereits auf Konferenzen angekündigt haben, hat nun auch Facebook bestätigt, eine Funktion in der Android-App einbauen zu wollen, die den Nutzern aufzeigen soll, wie lange sie die App genutzt haben.

Der Trend geht klar dazu, Apps bewusster zu benutzen, um so einen besseren Ausgleich zwischen Online- und Offlineleben zu bieten.

So hat Facebook vor, in der App dem Nutzer anzuzeigen wie viel Minuten er am Tag die Anwendung verwendet hat. Ebenfalls soll es eine Einstellungsmöglichkeit geben, wie lange die App genutzt werden soll und mittels Benachrichtigungsfunktion, soll der Anwender über den Ablauf erinnert werden.

Beim kommenden „Android P“, arbeitet Google sogar daran, stärker zwischen Arbeit und Privat zu unterscheiden. So sollen Apps, die mit einem Arbeitskonto genutzt werden, nach Feierabend ausgegraut werden.

Auch Instagram möchte, wie Facebook, ein Erinnerungs- und Nutzungssystem integrieren.

Quelle: golem.de

## Fake-News in Sozialen Medien

Wir alle kennen das Synonym Fake-News und obwohl fast jeder bei dem Wort darüber lacht, ist gerade in sozialen Medien, wie Facebook, Twitter und Co., die Welle der Falschmeldungen ein verheerendes Problem.

Dank der sozialen Medien, sind wir immer wieder top informiert, kennen die neuesten Katzenvideos und wissen was unsere Freunde machen. Auch die Flut an Werbungen, Angeboten und neuesten Nachrichten aus aller Welt, werden uns ganz einfach präsentiert. Aber sind diese News immer wahr? Wussten Sie zum Beispiel das eine Meerjungfrau (also ein wirklich, wirklich echte Meerjungfrau) gesichtet wurde? Nein? Tja auf Facebook wurde das berichtet, also muss es auch wahr sein, oder?

Nicht alles ist schlecht an sozialen Medien und das wissen wir alle. Aber welche News und Informationen sind wahr. Welche Artikel sind Fakt und welche Fake? Das herauszufinden ist für normale Anwender und Nutzer schwer.

Aus diesem Grund wurde 2011 ein Verein gegründet der diesen „Fake-News“ zu Leibe rückt: „Mimikama“.

Sie haben sich zum Ziel gesetzt, Meldungen und News, die Teils von Nutzern eingesendet und hinterfragt werden, ordentlich zu recherchieren und Falschmeldungen zu identifizieren. Der Verein möchte ein Zeichen des Schutzes von Internetnutzern setzen. Sie stehen klar dafür, Falschmeldungen zu entlarven, verdrehte Inhalte klarzustellen und auf Nutzerprobleme zu reagieren.

Alle Informationen zu Mimikama, aktuelle Falschmeldungen und News, finden Sie auf [www.mimikama.at](http://www.mimikama.at).

## Anonymes Ausdrucken bei Farblaserdruckern

Gewusst? Wenn Sie einen Farblaserdrucker nutzen, sind Ihre Ausdrücke nicht anonym. Soll heißen, dass der Drucker ein Muster aus kaum sichtbaren gelben Punkten hinzufügt, mit dem man auslesen kann, welcher Druckertyp es ist. Seriennummer, sowie Erstellungsdatum und Uhrzeit des Ausdrucks sind ebenfalls ersichtlich.

Das Deutsche Forschungsinstitut für Künstliche Intelligenz (kurz DFKI) und die Electronic Frontier Foundation (kurz EFF) haben dies im Jahr 2005 entdeckt.

Nun aber haben Dresdner Informatiker ein Verfahren entwickelt, die dieses Muster mit weiteren Punkten ausfüllen soll, um so eine Identifikation unmöglich zu machen.

Wie soll es funktionieren und warum wurde dieses Verfahren entwickelt?



Foto: Microsoft Bilder

Im Zuge Ihrer Diplomarbeit, untersuchten Sie über 1200 Seiten, die von über 140 Druckern, von knapp 20 Herstellern gedruckt wurden.

Nach der Analyse, die zudem noch weitere Druckeridentifikationscode aufzeigte, entwickelten Sie ein Verfahren, um die Identifikationspunkte zu erfassen. Im nächsten Schritt versuchten Sie diese zu umgehen. Resultat war nun, dass Sie weitere Punkte willkürlich hinzufügen, weglassen oder komplett ausfüllen konnten.

Laut Angaben der Informatiker, fanden Sie es wichtig die Menschen über die vorhanden Codes und die damit mögliche Überwachung aufzuklären. „Den wenigsten sei bewusst, dass Sie auch mit analogen Geräten überwacht werden könnten.“

Warum sind die Ausdrücke identifizierbar gemacht worden? Dazu äußerten sich die Druckerhersteller nicht. Ein eventueller Grund könnte zur Strafverfolgung sein.

Quelle: golem.de

## WPA3 Verschlüsselungsstandard

Der aktuelle Verschlüsselungsstandard WPA2 (engl. Wi-Fi Protected Access 2) wurde vor 14 Jahre eingeführt. Im Laufe dieser Zeit, haben sich einige Sicherheitslücken angesammelt und die Verschlüsselungstechnik ist nicht mehr aktuell.

So hat die Wi-Fi Alliance, die ein Zusammenschluss von verschiedenen Geräteherstellern ist, einen neuen Verschlüsselungsstandard verabschiedet, den WPA3. In diesem Verschlüsselungsstandard für drahtlose Netzwerke (kurz WLAN), sollen einige Macken ausgebessert und neue Standards eingeführt worden sein.

Zum Beispiel sollen Offline-Passwort-Angriffe unterbunden werden. Gemeint ist damit, dass bei WPA2 ein Offline-Wörterbuchangriff auf schwache Passwörter möglich war/ist. Mit dem WPA3 soll das nicht mehr möglich sein, da ein Angreifer mit dem Netz verbunden sein muss und jedes Passwort einzeln schicken muss, was ein Ausprobieren von Millionen von Passwörtern bedeutet und daher die Aktion nicht mehr rentabel macht.

Unterstützt soll auch der Diffie-Hellmann-Schlüsselaustausch „Forward Secrecy“ werden. „Wi-Fi Easy Connect“ soll möglich sein, genau so wie die sogenannte „opportunistische Verschlüsselung“.



Foto: Wi-Fi Alliance

*Diffie-Hellmann-Schlüsselaustausch Perfect Forward Secrecy (PFS):*

Einfach erklärt, sind dass zwei Kommunikationspartner, die die gleiche Verschlüsselung nutzen, der aber nicht über die Leitung mitversendet wird. Vorteil selbst wenn die Kommunikation abgefangen wird, kann diese, selbst wenn der Angreifer den Schlüssel besitzt, nicht ausgelesen werden.

*Wi-Fi Easy Connect:*

Ist eine Technologie, die IoT-Geräte sicher mit einem WLAN-Netz verbindet. Dies soll mit Hilfe eines QR-Code am Gerät und einer gescannten App funktionieren.

*Opportunistische Verschlüsselung:*

Dies ist eine Verschlüsselungsmöglichkeit, die in Netzen eingesetzt werden kann, die keine Authentifizierung vorgesehen haben und dadurch trotzdem eine verschlüsselte Verbindung aufbauen. (Hinweis: diese Verschlüsselung bietet keinen aktiven Schutz gegen Angreifer.)

Die ersten Geräte mit WPA3 werden voraussichtlich erst 2019 erwartet.

Quelle und Foto: golem.de



# Kaspersky Labs: Surfverhalten der Kids

Das Unternehmen Kaspersky Lab hat mit Hilfe der Module Kindersicherung und Kaspersky Safe Kids das Surfverhalten der jungen Nutzer untersucht und analysiert.

Das anonymisierte Verfahren analysiert, wie sich die Kinder an die digitale Welt anpassen und wofür sie sich interessieren.

## Wie werden diese Daten gesammelt?

In den verschiedenen Modulen zum Kinderschutz, gibt es gesamt 14 Kategorien. In diesen können von den Eltern selbst ausgewählt werden, welche blockiert werden oder welche nicht. Unter diesen Kategorien sind u.a. Inhalte für Erwachsene, Gewalt, Obszönitäten, Alkohol, Tabak usw.

Wird von den jungen Nutzern eine Webseite aufgerufen, die in eine dieser Kategorien fällt, übermittelt das Modul diese Daten an das Kaspersky Security Network. Die übermittelten Daten beinhalten jedoch keine Benutzerdaten und wurden nur von Computern mit den Betriebssystemen Windows und MacOS gesammelt, jedoch nicht über mobile Geräte.

Laut dem Artikel von Kaspersky Labs spiegelt sich das Interesse am besten an den Suchanfragen in den Suchmaschinen ab. So wurden die Daten die zwischen November 2017 und Mai 2018 eingegangen sind genauer analysiert und in folgende Kategorien unterteilt:

- Computerspiele
- Musik
- Videos
- Anime
- Shopping
- Pornografie und Erotik
- Kommunikation im Netz
- Bildung
- Sport
- Übersetzer
- Sonstiges

Die Analyse ergab folgendes Weltweites Ranking:

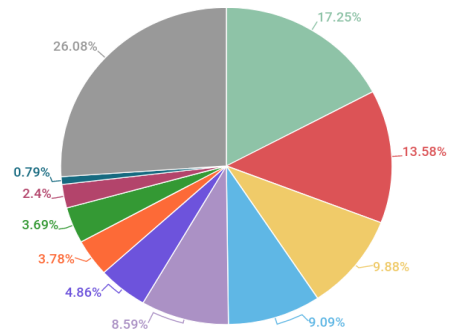
Platz 1: Video (17,25%)

Platz 2: Übersetzung von Texten (13,59%)

Platz 3: Kommunikation im Internet (9,88%)

Video beinhaltet jede Art von Videoinhalten, Streaming-Dienste, Video-Blogs, Serien und Filme. Kommunikation im

Internet sind sowohl soziale Medien, wie auch Messenger und E-Mail-Dienste.



● Video
 ● Online-Übersetzer
 ● Kommunikationsmedien im Internet
 ● Computerspiele
 ● Inhalt für Erwachsene
 ● Bildung
 ● Musik
 ● Sport
 ● Einkäufe
 ● Anime
 ● Andere

Foto: Kaspersky Labs

**KASPERSKY**

Sieht man sich die Regionalen Unterschiede an, erkennt man aber durchaus Abweichungen zum Weltweiten Trend.

Es gibt sowohl Unterschiede in Bezug auf Länder als auch auf Sprache. So wurde folgender Trend für Westeuropa (u.a. Österreich, Deutschland, Frankreich, Schweiz, usw.) ermittelt:

Platz 1: Kommunikationsmedien im Internet (37,44%)

Platz 2: Software, Audio, Video (27,36%)

Platz 3: Alkohol, Tabak, Betäubungsmittel (12,13%)

Auf dem letzten Platz dieses Rankings findet man mit 1,18% die Kategorie Inhalte für Erwachsene.

Sieht man sich die Statistiken genauer an und vergleicht diese mit den Erhebungen der letzten Jahre, kann man klar erkennen, dass junge Nutzer aktuell lieber Streamen (z.B. Netflix) als nach Computerspielen zu suchen. Ebenso gibt es einen Abwärtstrend in der Kategorie Alkohol, Tabak, Betäubungsmittel.

Kommunikationsmedien im Internet wie Facebook, Twitter und Co. werden vermehrt über mobile Geräte genutzt.

Positiv anzumerken ist aber noch, dass es einen Aufwärtstrend im Bereich der Bildung gibt.

Abschließend hält Kaspersky Labs fest, dass Kinder ihre Interessen so gut wie gar nicht vor den Eltern verbergen und das Internet nicht nur rein für Unterhaltung nutzen, sondern auch zum Lernen verwenden.

## Kaspersky Labs:

### „Krypto-Miner erfüllen unsere Prophezeiung“



Das Unternehmen Kaspersky Labs. warnt regelmäßig vor neuen Gefahren und Bedrohungen aus und im Internet und stellen auch hin und wieder Vorhersagen an, welche neuen Gefahren sich entwickeln können.

So haben Sie im November 2017 folgende Prognose abgegeben: „Nächstes Jahr (2018) werden Malware-Entwickler vermutlich von Ransomware auf bösartige Web-Miner umsteigen.“

Nun haben wir die erste Hälfte des Jahre 2018 hinter uns gebracht und müssen zugeben, Kaspersky Labs. hatte recht. Die sogenannten Krypto-Miner haben Ransomware vom Thron gestoßen.

#### Krypto-Miner, was oder wer ist das?

Krypto-Miner befallen Nutzer- (also Private-) und Unternehmenscomputer und nutzen deren Leistung (Hardware-Ressourcen) um Krypto-Währungen zu generieren und in die eigene Tasche zu stecken. Kurz gesagt: Nutzt ein anderer Ihren Computer/Laptop um damit „Geld“ zu verdienen ohne das sie was davon haben.

#### Welche Anzeichen und Symptome gibt es?

Im Endeffekt handeln Krypto-Miner im verborgenen. Es gibt

natürlich Anzeichen auf Ihrem Gerät, wie:

- Die Systemantwort wird langsamer; der Speicher, Prozessor und die Grafikkarten sind damit beschäftigt, die Krypto-Mining-Arbeitsschritte zu vervollständigen.
- Die Batterie wird wesentlich kürzer halten als vorher und die Geräte könnten sich erhitzen.
- Falls der Nutzer einen Datentarif verwendet, wird er die Skyrocket-Datennutzung sehen.

Die Gefahr durch Krypto-Miner sollte nicht so leicht abgetan werden. So ist in den Jahren 2017 und 2018 die Gesamtzahl von Krypto-Miner-Vorfälle von 1,9 Millionen auf 2,7 Millionen (also von 3% auf 4%) angestiegen.

Betroffen können sowohl Desktop-Computer (PC), Laptop/Netbook, Smartphone und Tablet sein und das nicht nur mit Windows-Betriebssystemen.

#### Welche Schutzmöglichkeiten gibt es?

Immer die gleichen, ist leider die Antwort: keine unbekanntes E-Mail-Anhänge und Links öffnen, kein Installieren von Software aus dem Internet von unbekanntes Quellen und Virenschutzprogramme (aber bitte keine Kostenlosen!).

Quelle: <https://www.kaspersky.de/blog/cryptominers-almost-double/17094/>

## Smartwatches und ihre Apps

Ende Juni 2018 haben wir bei Kaspersky Labs. angefragt ob es aktuell eine Sicherheitssoftware für Smartwatches gibt bzw. ob Kaspersky Labs Berichte darüber vorliegen wie die Sicherheitslage rund um Smartwatches und die dazugehörigen Apps ist.

Laut der Pressemitteilung von Kaspersky Labs, die uns übermittelt wurde ist sowohl Spionage als auch Datenklau möglich. Heißt Wearables (also Computer der während der Anwendung am Körper des Benutzers befestigt oder in die Kleidung integriert sind) kann als Spionage-Tool eingesetzt werden, indem heimlich Daten zu Beschleunigung und Ausrichtung des Nutzers gesammelt werden. Die Folge ist, so laut Kaspersky Labs.: „Es lassen sich einzigartige Datensätze der Nutzer zur Überwachung erstellen – inkl. der Eingabe sensibler Informationen.“

Experten von Kaspersky Labs. haben mit Hilfe einer einfachen Applikation Smart-Watches unterschiedlicher Anbieter untersucht, um herauszufinden welche Nutzerinformationen an unbefugte Dritte zur Verfügung gestellt wurden. Mit Hilfe von mathematischen Algorithmen, die der Rechenleistung des Smart-Wearables zur Verfügung standen, konnten Verhaltensmuster sowie Zeiträume, wann und wo Nutzer sich bewegten und wie lange sie damit arbeiteten, ermittelt werden.

Zudem konnten auch noch sensiblere Nutzerdaten ausgelesen werden, wie Passworteingabe am Computer (Genauigkeit von 96 %), PIN-Code Eingabe am Geldautomaten (Genauigkeit 87 %), Entsperrung des Mobiltelefons (Genauigkeit 64 %).

Resultat: Einzigartige Verhaltensmuster des jeweiligen Nutzers am Gerät wurden sichtbar. Dritte könnten über eine E-Mail-Adresse, die bei der Registrierung in der App angefordert wurde, oder über den aktivierten Zugriff auf die Anmeldeinformationen des Android-Kontos die dahinterstehende Identität sowie die Gewohnheiten ermitteln. Darüber hinaus könnten Cyberkriminelle die empfangenen Signale entschlüsseln, Opfern auflauern oder Skimmer an ihren bevorzugten Geldautomaten installieren.

Da in den Jahren 2015 bis 2017 der Umsatz mit Smart-Watches um 92,3 % auf 325 Millionen Euro und bei Fitness-Trackern um 77,1 % auf 142,74 Millionen gestiegen ist, sind auch die potentiellen Opfer gestiegen.

Es wird daher zu besonderer Aufmerksamkeit geraten und schützen Sie Ihr Endgerät auf dem Sie die (Originale) Wearable-App vom Hersteller installiert haben, ebenso mit einer Sicherheitssoftware wie Ihren PC oder Laptop! Und aktualisieren Sie die App wirklich regelmäßig.

Quelle: Kaspersky Labs.

# Windows 10 Update Historie



29. Juli 2015 Windows 10 wurde veröffentlicht.

Seither hat es einen Marktanteil von 42,8% (Stand: 01/2018) unter den Windows-Betriebssystemen. Neben einigen Features wurden auch die automatischen Updates eingeführt. Und ja wir alle haben uns das ein oder andere Mal gefragt: „Jetzt schon wieder ein Update?“ Mittlerweile stehen wir vor dem 7ten Versionsupdate, dass für Herbst 2018 geplant ist, aus diesem Grund wollen wir mal einen Blick auf die bereits erschienen werfen:

Version	Build	Name (Codename)	Erscheinungsdatum (Supportende)	Bemerkungen und wichtige Änderungen
1507	10240	Release to Manufacturing (RTM) (Threshold 1)	29. Juli 2015 (9. Mai 2017)	Erste RTM-Version von Windows 10. Nach Meinung einiger Autoren der Fachpresse ist Windows mit diesem Build allerdings noch nicht ganz fertig. Um Windows 10 gratis aktivieren zu können, musste man aus einem bereits aktivierten Windows 7 oder 8/8.1 heraus ein Upgrade durchführen. Der Support für die RTM Version wurde am 9. Mai 2017 eingestellt.
1511	10586	November Update (Threshold 2)	12. November 2015 (10. Oktober 2017)	Hauptsächlich Detailverbesserungen, wie vereinheitlichte Optik vieler weiterer Kontextmenüs. Erstmals konnte man Windows 10 bei einer Neuinstallation innerhalb des von Microsoft angegebenen Zeitraums direkt mit einem Produktschlüssel von Windows 7 oder 8/8.1 gratis aktivieren.
1607	14393	Anniversary Update (Redstone 1)	2. August 2016 (10. April 2018)	Das „Anniversary Update“ für Windows 10 beinhaltet unter anderem die folgenden Neuerungen und Änderungen: <ul style="list-style-type: none"> <li>• Verbesserte Unterstützung von Eingabestiften mit <i>Windows Ink</i>.</li> <li>• Überarbeitetes Startmenü.</li> <li>• Cortana versteht mehr Befehle, ist tiefer im System integriert und funktioniert auch auf gesperrtem Bildschirm.</li> <li>• Edge Browser unterstützt Erweiterungen und das Anheften von Tabs.</li> <li>• Windows Defender mit „Offline“-Modus, der ausgeführt werden kann, noch bevor das Betriebssystem geladen wird.</li> <li>• Einige Gruppenrichtlinienobjekte verlieren unter Windows 10 Pro ihre Wirkung.</li> <li>• Das Windows Subsystem for Linux, eine Kompatibilitätsschicht zum Ausführen von Linux-Programmdateien. Dies ist vor allem für Software-Entwickler gedacht und kann ab dieser Version als experimentelle Funktion aktiviert werden.</li> <li>• In der 32-Bit-Version sind die Systemanforderungen bei Neugeräten von 1 auf 2 GB Arbeitsspeicher gestiegen. Die Build-Nummern von Desktop- und Mobil-Version wurden zwischenzeitlich angeglichen, dadurch gab es einen größeren Sprung bei der Build-Nummer.</li> </ul>
1703	15063	Creators Update (Redstone 2)	6. April 2017 (9. Oktober 2018)	Das „Creators Update“ wurde am 6. April zur manuellen Installation veröffentlicht. Die Verteilung per Windows Update startete am 11. April. Die Aktualisierung enthält unter zahlreichen Detailverbesserungen insbesondere die folgenden Änderungen und Neuerungen: <ul style="list-style-type: none"> <li>• Die Datenschutzoptionen sind ausführlicher und transparenter erklärt.</li> </ul>

				<ul style="list-style-type: none"> <li>• <i>Paint 3D</i> ermöglicht es, einfache dreidimensionale Zeichnungen anzufertigen.</li> <li>• Der <i>Nachtmodus</i> ändert die Farbtemperatur der Bildschirmausgabe abhängig von der Tageszeit.</li> <li>• Ein <i>Spielmodus</i> soll die Leistung in Computerspielen durch Freigabe von Ressourcen verbessern.</li> <li>• Verbesserte Darstellung älterer Anwendungen bei der Bildschirmskalierung.</li> </ul>
1709	16299	Fall Creators Update (Redstone 3)	17. Oktober 2017 (9. April 2019)	<p>Die am 17. Oktober 2017 erschienene Aktualisierung beinhaltet folgende Neuerungen:</p> <ul style="list-style-type: none"> <li>• OneDrive-Funktion „Dateien bei Bedarf“: In der Cloud gespeicherte Dateien werden nur bei Bedarf heruntergeladen.</li> <li>• Überwacher Ordnerzugriff: Nur Programme, denen die entsprechende Erlaubnis erteilt wurde, dürfen in persönliche Ordner schreiben.</li> <li>• Microsoft Edge kann Inhaltsverzeichnisse von PDF-Dateien anzeigen und Formulardaten ausfüllen.</li> </ul>
1803	17134	April 2018 Update (Redstone 4)	30. April 2018 (12. November 2019)	<p>Die Aktualisierung enthält folgende Neuerungen:</p> <ul style="list-style-type: none"> <li>• Verbesserte Personenleiste</li> <li>• Neue Timeline-Funktion</li> <li>• Verbesserungen beim Update-Prozess</li> <li>• Unterstützung des Bildformats HEIF ohne Zusatzprogramme</li> <li>• Fluent Design in den Einstellungen und einigen vorinstallierten Apps</li> </ul>
1809	–	(Redstone 5)	Herbst 2018	Die nächste große Aktualisierung für Windows 10, die im Herbst 2018 erscheinen soll.

Anmerkung: Die Versionen 1507 bis 1607 sind ältere Versionen die nicht mehr unterstützt werden, 1703 bis 1709 sind ebenfalls ältere Versionen werden aber noch unterstützt, die Version 1803 ist die aktuelle und die Version 1809 ist die zukünftige.

Quelle: wikipedia.org

# Microsoft Office 2019



Mit ein „bissel mehr“ gibt sich Microsoft anscheinend nicht zu frieden. So soll im Herbst 2018 nicht nur ein neues Versionsupdate für Windows 10 kommen, sondern auch das neue Microsoft Office 2019.

Die von Microsoft selbst genannte „ewige“ Version (weil man dafür nur einmal bezahlen muss und es dann für immer besitzt oder solange es auf dem Windows-Betriebssystemen nutzbar ist), soll z.B. neue und verbesserte Farbfunktionen beinhalten, Drucksensitivität und Neigungseffekte, leistungsfähigere Datenanalysen (wie neue Formeln, Diagramme und Power BI-Integration), sowie ausgefeilte Präsentationsfunktionen wie Morph und Zoom.

Basieren wird Office 2019 auf Office 365. Zudem wird es auch Funktionen daraus enthalten.

Angekündigt wurde das neue Office im Jahr 2017 bei der Microsoft Ignite Tech Conference. Wobei darauf hingewiesen werden sollte, dass nur eine Vorschau und nicht die Endversion angekündigt wurde.

Was aber schon fixiert ist, ist die Laufzeit vom neuen Office: so wird es einen 5 Jahre grundlegenden Support und einen 2 Jahre erweiterten Support geben. Diese Laufzeit ist an die Support-Phase vom Office 2016 ausgerichtet.

Übersicht Microsoft Office-Versionen seit dem Jahr 2000:

- Office 2001 11. Oktober 2000 (Win / MacOS)
- Office XP 31. Mai 2001 (Win)
- Office v.X 19. November 2001 (MacOS)
- Office 2003 17. November 2003 (Win)
- Office 2004 11. Mai 2004 (MacOS)
- Office 2007 30. Januar 2007 (Win)
- Office 2008 15. Januar 2008 (MacOS)
- Office 2010 15. Juni 2010 (Win)
- Office 2011 26. Oktober 2010 (MacOS)
- Office 365 28. Juni 2011 (Win)
- Office 2013 29. Januar 2013 (Win)
- Office 2016 09. Juli 2015 (MacOS)
- Office 2016 22. September 2015 (Win)
- Office 2019 voraussichtlich Herbst 2018

Quellen: Microsoft.com, Wikipedia.org



## Top 10 Apps in Österreich

Wir alle haben sie, wir alle nutzen sie. Hier sind die beliebtesten Android, Windows und Apple Apps der Österreicher(innen):

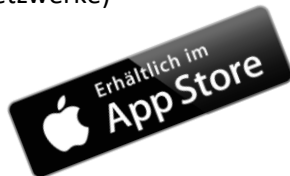
### Android Play-Store:

- Platz 10: Wish – Smart Shoppen & Sparen (Shooping)
- Platz 9: Love Balls (Spiele)
- Platz 8: Sling Drift (Spiele)
- Platz 7: Kick the Buddy (Spiele)
- Platz 6: WhatsApp Messenger (Soziale Netzwerke)
- Platz 5: Rise Up (Spiele)
- Platz 4: Poly Artbook – Puzzle Game (Spiele)
- Platz 3: Tomb of the Mask (Spiele)
- Platz 2: Helix Jump (Spiele)
- Platz 1: Youtube Music (Musik und Audio)**



### Apple iTunes:

- Platz 10: Spotify Music (Musik)
- Platz 9: Love Balls (Games)
- Platz 8: Poly Artbook – puzzle (Spiele)
- Platz 7: Snapchat (Foto und Video)
- Platz 6: Google Maps – GPS (Navigation)
- Platz 5: Instagram (Foto und Video)
- Platz 4: H&M App (Shopping)
- Platz 3: Pokémon Quest (Spiele)
- Platz 2: WhatsApp (Soziale Netzwerke)
- Platz 1: Helix Jump (Spiele)**



### Windows Store:

- Platz 10: Messenger (Soziale Netzwerke)
- Platz 9: iTunes (Music, Video)
- Platz 8: theChive UWP (Soziale Netzwerke)
- Platz 7: Facebook (Soziale Netzwerke)
- Platz 6: Microsoft Sticky Notes (Office)
- Platz 5: CBS Sports Scores, News, State (News)
- Platz 4: Instagram (Soziale Netzwerke)
- Platz 3: WhatsApp Desktop (Soziale Netzwerke)
- Platz 2: Spotify Music (Musik)
- Platz 1: Netflix (Streaming)**



Stand Juli 2018. Quellen und Fotos Google PlayStore, Windows Store, Apple iTunes Store

## Aktualisieren & Updates auf Ihren Geräten

Aus der Erfahrung mit Kunden und Anwendern wissen wir, dass gerade diese immer wieder die Augen „überdrehen“ wenn es heißt Updates und Aktualisierungen sind notwendig und müssen gemacht werden.

Natürlich ist einem jeden Systembetreuer klar: Der Anwender kennt sich nicht aus und will es auch nicht machen – macht zusätzlich Arbeit, also warum soll ich es tun. Aber Updates und Aktualisierungen sind wichtig, notwendig und JA, müssen gemacht werden.

Zu aller erst: wenn diese Updates und Aktualisierungen nicht gemacht werden, ist der PC, Laptop, Tablett aber auch das Smartphone – also alles mit dem Sie arbeiten, E-Mail abrufen, im Internet surfen oder Bankgeschäfte erledigen, egal ob im Job / Business oder Privat, gefährdet. Die Aktivitäten rund um Viren / Trojaner / Schadsoftware sind allgegenwärtig und gefährden jeden.

Datenverlust, klau von privaten Informationen und Diebstahl von Eigentum und Geld, bis hin zum Defekt der Geräte, können die Folge sein. Aus diesem Grund raten nicht nur Hersteller, IT-Fachleute oder IT-Magazine immer wieder updaten und aktualisieren Sie Betriebssysteme, Software, Apps usw. immer regelmäßig.

Nein, 1 bis 3 Mal im Jahr ist nicht regelmäßig!

Zwar ist es mit dem Aktualisieren und Updaten alleine nicht getan, aber es ist ein wichtiger und richtiger Schritt, um Sicherheit zu bekommen und zu Erhalten.

### Was sollte unbedingt aktualisiert bzw. upgedatet werden?

Eigentlich lautet die Devise, alles muss aktualisiert werden! Aber gerade die Programme, die Sie immer nutzen sind essentiell:

Betriebssystem und Office: Windows (Windows 10 wird normalerweise automatisch aktualisiert, nutzen Sie jedoch mobiles Internet und/oder ist die Internet Verbindung als getaktet eingestellt, müssen Sie händisch – also der Nutzer/Anwender selber die Updates ausführen), genauso wie Android, MacOS

Antiviren-Programme/Software/Apps: egal ob kostenpflichtig oder kostenlos

Adobe FlashPlayer und Reader (Hinweis bei der Nutzung von Internet Explorer oder Edge unter Windows wird Adobe FlashPlayer mit den Windows Updates aktualisiert, nutzen Sie jedoch z.B. Mozilla Firefox, Google Chrome oder andere müssen diese händisch – also durch den Anwender/Nutzer aktualisiert werden)

Apps auf dem Smartphone und Tablett: egal welches Betriebssystem Sie nutzen (Android, MacOS, Windows), vor allem sozial Media Apps (wie Facebook, WhatsApp, etc.) immer auf dem neuesten Stand halten, genauso wie oft genutzte Apps (z.B. Games, Fotobearbeitung, Messenger, etc.)

Java: vor allem wenn Sie Java-Games spielen (z.B. Facebook-Games)