Schieb Report

Ausgabe 2022.42

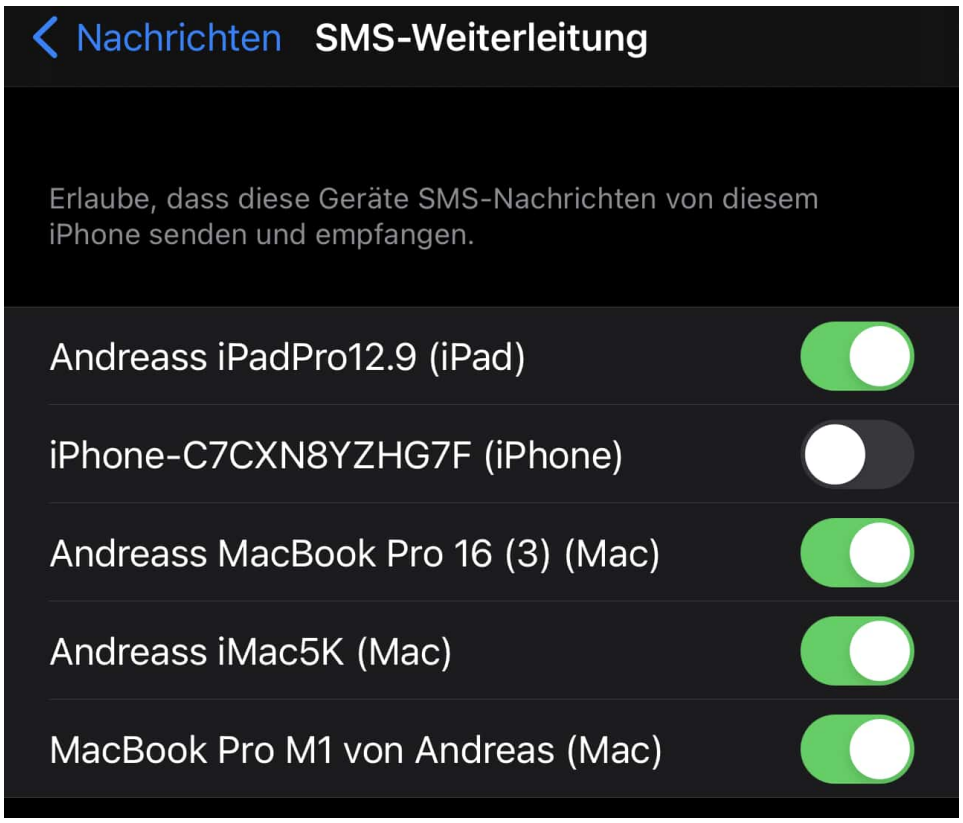
SMS auf einem neuen iPad/Mac empfangen

SMS kommen auf Eurem iPhone an. Wenn Ihr die auch auf anderen macOS/iOS-Geräten bekommen wollt, müsst Ihr iMessage, den Kurznachrichten-Service von Apple, auf jedem der Geräte aktivieren. Für jedes neue Gerät!

Wenn Ihr ein iPhone als Telefon einsetzt und dazu mit einem Mac oder iPad arbeitet, dann kennt Ihr die Situation: iMessages kommen parallel auf allen Geräten an. Wenn Ihr aber die TAN für Ihr Online-Banking oder eine andere SMS bekommt, dann kommt die nur am Smartphone an. Das unterbricht den Arbeitsablauf. Unnötigerweise, denn iOS bietet eine SMS-Weiterleitung an!

- Tippt auf dem iPhone in den Einstellungen auf **Nachrichten** > **SMS-Weiterleitung**.
- Ihr bekommt nun eine Übersicht aller Geräte, die mit der Apple-ID angemeldet sind, angezeigt.
- In dieser Liste aktiviert die Geräte, die eine eingehende SMS auf dem

iPhone als iMessage weitergeleitet bekommen sollen.



- Die weitergeleiteten SMS werden dann ganz normal in der Nachrichten-App der anderen Geräte angezeigt, als wären sie dort als SMS eingegangen.
- Wenn Ihr auf eine so zugestellte SMS antwortet, dann wird diese wieder zum iPhone übertragen und von dort aus als normale SMS verschickt.
- Für den Empfänger einer so versendeten SMS ist es nicht ersichtlich, dass sie von einem anderen Gerät kommt.

Das ganze lässt sich sogar noch einen Schritt weiter treiben: Über iMessage bekommt Ihr über diesen Hack die SMS sogar auf Android-Smartphones und -Tablets. Egal, ob diese eine eigene SIM-Karte haben und welche Rufnummer diese verwendet!

iPad Pro 2022 mit M2-Chip und Pencil-Schwebefunktion

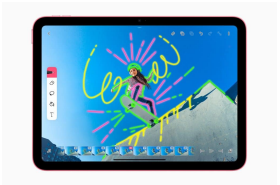
Diesmal hat Apple neue Produkte ganz ohne Produkt-Show vorgestellt. Das neue iPad Pro bietet mehr Leistung und Support für den ProRes-Codec (Video) sowie das moderne WLAN 6E. Damit will Apple Profis ansprechen. Die Euro-Preise des iPad Pro ziehen deutlich an.

Das iPad Pro wird in der Pro-Version immer mehr zu einem Notebook-Ersatz.

Apple hat heute das neue iPad Pro mit dem M2 Chip vorgestellt, das die ultimative Kombination aus Mobilität, Vielseitigkeit und überragender Leistung bietet. Das neue iPad Pro bietet neben einer innovativen Schwebefunktion für den Apple Pencil und superschnellen drahtlosen Verbindungen, das weltweit fortschrittlichste mobile Display, Pro Kameras, Face ID und Thunderbolt und ein Audiosystem mit vier Lautsprechern.

Neue Funktionen in iPadOS 16, darunter Stage Manager, vollständige Unterstützung externer Displays, Desktop Apps und der Referenzmodus machen

das iPad zu einem noch leistungsstärkeren Begleiter für professionelle Workflows. Mit seiner fortschrittlichen Hardware und iPadOS 16 verfügt das iPad Pro über ein unglaubliches Ökosystem an herausragenden Pro Apps wie kein anderes Gerät dieser Art. Das neue iPad Pro kann ab heute bestellt werden und ist ab Mittwoch, 26. Oktober in den Stores erhältlich.



Noch mehr und schnellere Grafik[/caption]

Deutlich mehr Performance des M2 Chip

Der M2, der den Start der nächsten Generation der M Chipfamilie von Apple markiert, baut die bahnbrechende Performance und Funktionalität des iPad Pro mit branchenführender Energieeffizienz, einer Architektur mit gemeinsamem Arbeitsspeicher und speziell entwickelten Technologien weiter aus.

Der M2 bietet eine 8-Core CPU — bis zu 15 Prozent schneller als beim M1 — mit Verbesserungen sowohl bei den Performance- als auch bei den Effizienz-Kernen. Eine 10-Core GPU mit einer bis zu 35 Prozent schnelleren Grafikleistung für Nutzer mit allerhöchsten Ansprüchen. In Kombination mit der CPU und GPU kann die 16-Core Neural Engine 15,8 Billionen Rechenoperationen pro Sekunde ausführen — 40 Prozent mehr als der M1.

So kann das iPad Pro komplexe Operationen rund um maschinelles Lernen noch leichter bewältigen. Außerdem liefert der M2 Chip 100 GB/s gemeinsame Arbeitsspeicherbandbreite — 50 Prozent mehr als der M1 — und unterstützt bis zu 16 GB schnellen gemeinsamen Arbeitsspeicher, was Multitasking und das Arbeiten mit großen Objekten noch flüssiger macht.

Die Performance des M2 beschleunigt selbst die anspruchsvollsten Workflows enorm, angefangen bei der Bearbeitung umfangreicher Fotobibliotheken von Fotografen über die Manipulation komplexer 3D-Objekte von Designer, bis hin zur Durchführung fortschrittlicher Bildgebung und Analysen von medizinischen Fachkräften und das Genießen grafikintensiver Spiele von Gamer.
[caption id="attachment_782396" align="alignnone" width="1030"]

Unglaubliche Power liefert der M2 zudem durch seine neue Media Engine und

den Bildsignalprozessor. In Verbindung mit den fortschrittlichen Kameras lassen sich damit erstmals auch Videos in ProRes aufnehmen. Zudem kann ProRes Videofootage bis zu 3-mal schneller transkodiert werden. Das bedeutet, dass Content Creator von einem einzigen Gerät aus Videos in Kinoqualität aufnehmen, bearbeiten und veröffentlichen können.

Daddeln am iPad: Gar kein Problem dank schnellem Prozessor[/caption]

Apple Pencil mit innovativer Schwebefunktion

Das neue iPad Pro und iPadOS 16 eröffnen Nutzer mit der Schwebefunktion des Apple Pencil (2. Generation) eine völlig neue Dimension, mit dem Display zu interagieren. Der Apple Pencil wird bereits bis zu 12 Millimeter über dem Display erkannt, sodass Nutzer eine Vorschau ihrer Markierung sehen können, bevor sie sie vornehmen.

Dies ermöglicht es Anwender mit noch größerer Präzision zu skizzieren und zu illustrieren und lässt alles, was man mit dem Apple Pencil macht, sogar noch einfacher werden. So erweitern sich beispielsweise bei Kritzeln die Textfelder automatisch, wenn der Stift in die Nähe des Bildschirms kommt, und Handschrift wird noch schneller in Text umgewandelt. Auch Apps von Drittanbietern können diese neue Funktion nutzen, um völlig neue Erlebnisse rund ums Markieren und Zeichnen zu schaffen.

WLAN, das es noch fast gar nicht gibt

Das neue iPad Pro bietet mit Unterstützung für WLAN 6E superschnelle Verbindungen über drahtlose Netzwerke, die Nutzer benötigen, um anspruchsvolle Workflows jederzeit und überall mühelos zu bewältigen. Downloads erfolgen mit bis zu 2,4 Gbit/s und damit doppelt so schnell wie bei der vorherigen Generation. Wi-Fi + Cellular Modelle mit 5G (sub?6 GHz und mmWave) unterstützen ab sofort mehr 5G Netzwerke weltweit, sodass Nutzer auch jederzeit unterwegs auf ihre Daten zugreifen, mit Kollegen kommunizieren und ihre Daten im Handumdrehen sichern können.

[caption id="attachment_782395" align="alignnone" width="1030"]

Pro Features mit iPadOS 16

Ergänzend zu den umfangreichen Updates für Nachrichten, den neuen Tools in Mail und Safari, der neuen Wetter App, sowie den erweiterten Möglichkeiten zur Interaktion mit Fotos und Videos mit Live Text und Visuelles Nachschlagen bietet iPadOS 16 eine Reihe weiterer leistungsstarker Produktivitätsfunktionen für ein noch ansprechenderes Erlebnis mit dem iPad Pro:

- **Stage Manager** sorgt für ein komplett neues Multitasking-Erlebnis, bei dem Apps und Fenster automatisch organisiert werden und Nutzer schnell und einfach zwischen Aufgaben wechseln können. Noch in diesem Jahr wird Stage Manager auch um die vollständige Unterstützung für externe Displays mit Auflösungen von bis zu 6K erweitert werden. So können sich Nutzer den idealen Arbeitsplatz einrichten und mit bis zu vier Apps auf dem iPad und bis zu vier Apps auf dem externen Display arbeiten.
- **Desktop Apps** unterstützen neue Funktionen, die für das Display des iPad Pro optimiert sind und den Funktionsumfang um neue Elemente und Interaktionen ergänzen. Dazu zählen konsistentes rückgängig machen

oder wiederholen, neu gestaltetes Finden und Ersetzen, ein neues Dokumentmenü, anpassbare Symbolleisten, die Möglichkeit zum Ändern von Dateierweiterungen, das Anzeigen der Ordnergröße in Dateien und mehr.
- Der **Referenzmodus** ermöglicht es, mit dem 12,9" iPad Pro mit Liquid Retina XDR Display den Abgleich der Farbanforderungen in Workflows wie Überprüfung und Freigabe, Farbkorrektur und Compositing vorzunehmen, bei denen präzise Farben und konsistente Bildqualität entscheidend sind. Das bedeutet, dass professionelle Anwender wie Fotografen und Videofilmern damit HDR-Aufnahmen bei maximaler, lebensechter Detailtreue direkt bearbeiten und Kameraleute am Set eine Vorschau der Aufnahmen in einem Farbprofil ansehen können, das der endgültigen Aufnahme entspricht.

Wie nachhaltig ist das iPad

Die neuen iPad Modelle sind für eine möglichst geringe Umweltbelastung entwickelt worden. Es wird erstmals beim iPad zu 100 Prozent recyceltes Gold für die Beschichtung mehrerer Leiterplatten verwendet, genauso wie recyceltes Aluminium, Zinn und Seltenerdelemente.

Alle iPad-Modelle erfüllen die hohen Standards von Apple für Energieeffizienz und sind frei von Quecksilber, bromhaltigen Flammschutzmitteln, PVC und Beryllium. Durch die neu designte Verpackung ist keine Umverpackung aus Kunststoff mehr nötig. 99 Prozent der Verpackung besteht aus Fasermaterial. Dadurch kommt Apple seinem Ziel näher, bis 2025 vollständig auf Kunststoff in seinen Verpackungen zu verzichten.

Apple ist bereits heute bei allen weltweiten Unternehmensaktivitäten klimaneutral und plant bis 2030 über alle Tätigkeitsbereiche des Unternehmens, die Zuliefererkette und den Produktlebenszyklus hinweg klimaneutral zu werden. Das bedeutet, dass jedes verkaufte Apple Gerät von der Komponentenherstellung, Montage, dem Transport, der Nutzung durch die Kunden, dem Aufladen bis hin zum Recycling und zur Materialrückgewinnung keinerlei Auswirkungen auf das Klima haben wird.

Preise und Verfügbarkeit

- Das neue iPad Pro kann ab heute, 18. Oktober

auf apple.com/de/store und in der Apple Store App in 28 Ländern und Regionen bestellt werden, darunter die *USA*, und ist ab Mittwoch, 26. Oktober in den Stores erhältlich.
- Das neue 11" und 12,9" iPad Pro wird in den Farben Silber und Space Grau und in Konfigurationen mit 128 GB, 256 GB, 512 GB, 1 TB und 2 TB erhältlich sein.
- Das 11" iPad Pro beginnt bei **1.049 Euro** inkl. MwSt. für das Wi-Fi Modell und **1.249 Euro** inkl. MwSt. für das Wi-Fi + Cellular Modell; und das 12,9" iPad Pro beginnt bei **1.449 Euro** inkl. MwSt. für das Wi-Fi Modell und **1.649 Euro** inkl. MwSt. für das Wi-Fi + Cellular Modell.
- Der Apple Pencil (2. Generation) ist separat für **149 Euro** inkl. MwSt. erhältlich und kompatibel mit dem neuen iPad Pro.
- Das Magic Keyboard ist in Schwarz und Weiß für **369 Euro** inkl. MwSt. für das neue 11" iPad Pro und **429 Euro** inkl. MwSt. für das neue 12,9" iPad Pro erhältlich, mit Layouts für über 30 Sprachen.
- Das Smart Keyboard Folio für das neue iPad Pro ist für **219 Euro** inkl. MwSt. für das neue 11" iPad Pro und **249 Euro** inkl. MwSt. für das neue 12,9" iPad Pro erhältlich.
- Das Smart Folio ist in Schwarz, Weiß und Marineblau für **99 Euro** inkl. MwSt. für das neue 11" iPad Pro und **125 Euro** inkl. MwSt. für das neue 12,9" iPad Pro erhältlich.
- Bildungspreise gelten für aktuell eingeschriebene und zugelassene Studierende und ihre Eltern sowie Lehrkräfte, Mitarbeiter und Homeschooling Lehrkräfte aller Klassenstufen. Das neue 11" iPad Pro beginnt bei **979 Euro** inkl. MwSt. und das 12,9" iPad Pro beginnt bei **1.319 Euro** inkl. MwSt. Der Apple Pencil der zweiten Generation ist für **139 Euro** inkl. MwSt. erhältlich. Das Smart Keyboard Folio für das neue iPad Pro zum Bildungspreis ist für **189 Euro** inkl. MwSt. für das 11" iPad Pro und **219 Euro** inkl. MwSt. für das 12,9" iPad Pro erhältlich. Das Magic Keyboard wird zum Bildungspreis für **339 Euro** inkl. MwSt. für das 11" iPad Pro und **399 Euro** inkl. MwSt. für das 12,9" iPad Pro erhältlich sein. Weitere Informationen unter apple.com/de/education.
- iPadOS 16, das leistungsstarke, speziell für das iPad entwickelte Betriebssystem, ist ab Montag, 24. Oktober verfügbar und kommt kostenlos mit dem neuen iPad Pro. iPadOS 16 wird als kostenloses Software-Update für iPad (5. Generation und neuer), iPad mini (5. Generation und neuer), iPad Air (3. Generation und neuer) und alle iPad Pro Modelle verfügbar sein.
- Kunden können ein aktuelles iPad in Zahlung geben und erhalten eine

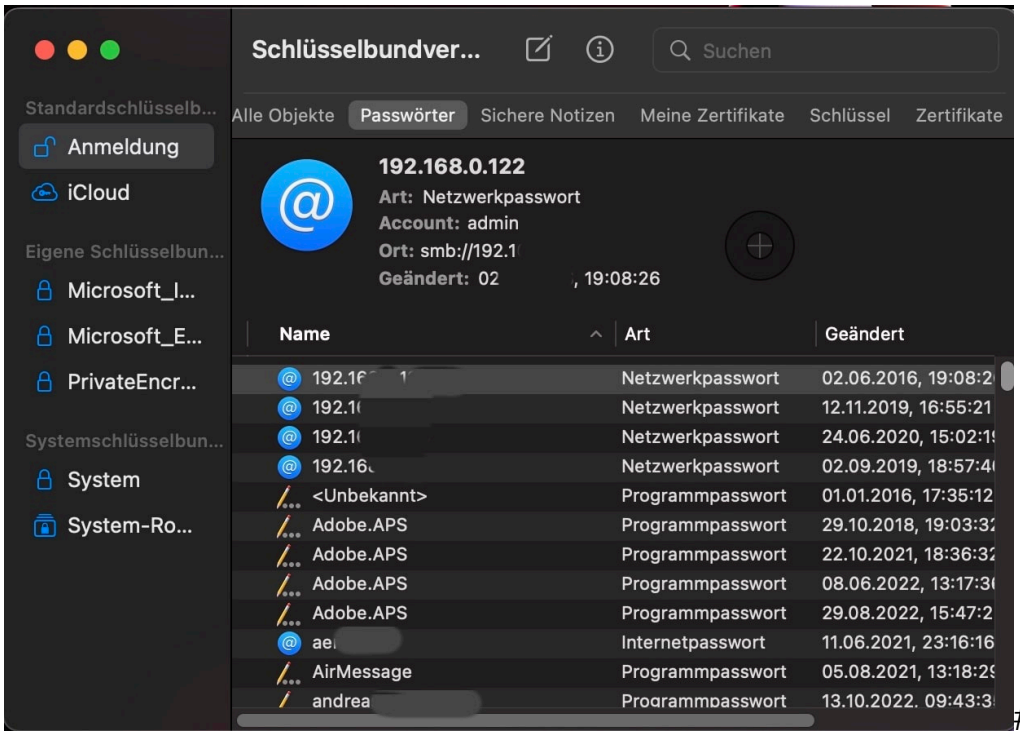
Gutschrift für ein neues. Sobald das Gerät eingegangen und geprüft worden ist, schreibt Apple den Wert auf das verwendete Zahlungsmittel gut.

- Das iPad kann kostenlos mit Emojis, Namen, Initialen und Zahlen exklusiv auf apple.com/de/store oder in der Apple Store App graviert werden.
- Apple bietet seinen Kunden im Store und online eine Reihe von Services. Mit persönlicher Unterstützung und Beratung durch Apple Specialists, praktischen Versand- und Abholoptionen sind die Apple Stores und apple.com/de/store die beste Art, Apple Produkte zu kaufen.

Herausfinden gespeicherter Passwörter bei macOS/iOS

MacOS, iOS- und iPad-OS-Geräte speichern die Passwörter ab und füllen sie bei der nächsten Verwendung komfortabel vor. Einen Nachteil hat das allerdings: Ihr merkt Euch immer weniger Passwörter. Wir zeigen Euch, wie Ihr die Passwörter auslesen könnt!

Der Kern der beschriebenen Funktionalität ist der Schlüsselbund. Der nimmt im Apple-Universum alle Passwörter auf, speichert sie verschlüsselt und macht sie bei Bedarf Anwendungen wie Browsern wieder verfügbar. Der Schlüsselbund wird zusätzlich noch mit iCloud synchronisiert, wenn Ihr das aktiviert habt. Jedes Gerät, das mit derselben Apple ID angemeldet ist, kann dann alle Passwörter nutzen, als wären sie auf dem Gerät eingegeben worden.



#

Um ein Passwort wieder auszulesen, geht wie folgt vor:

- Auf dem Mac such in Spotlight nach Schlüsselbund und startet die **schlüsselbundverwaltung.app**.
- Auf einem iPad oder iPhone klickt in den Einstellungen auf **Passwörter**.
- Klickt/tippt in das Suchfeld, dann gebt den Namen der Webseite oder des Dienstes an, für den Ihr das Passwort auslesen wollt.
- Auf dem Mac müsst Ihr zum Anzeigen des Passwortes noch das Kennwort des aktuellen Geräts eingeben.
- Ihr seht das Kennwort jetzt in Klageschrift, auf dem iPad könnt Ihr es durch Halten des Fingers auf dem Passwort-Eintrag in die Zwischenablage kopieren und dann direkt in eine Anmeldemaske eintragen.

Netzdenker | Cyberangriffe auf deutsche Medien – und was macht eigentlich das BSI?

Seit zwei Jahren mehren sich Angriffe auf IT-Infrastruktur von Medienbetrieben. Dahinter stecken weniger politische Motive als klares Kalkül. Alle müssen sich besser schützen.

Man stelle sich das mal vor: Redakteure und Autoren einer Zeitung schreiben Texte, übergeben die per USB-Stick an Layouter, die layouten die Seiten und bringen dann wieder einen USB-Stick zur Druckerei, damit die Zeitung gedruckt werden kann...

Das klingt nach keiner guten Strategie, doch die „Heilbronner Stimme“ hat diese Woche genau so gearbeitet. Auch bei einigen Zeitungen der „Funke“-Mediengruppe, zu der die „WAZ“ oder die „Berliner Morgenpost“ gehören, war rund Ende 2020 genau so. Denn Cyberangreifer hatten die IT-Systeme des Verlags lahmgelegt.

Zu schlecht gegen Cyberangriffe geschützt

Die Zeitungen mussten einige Tage in Notausgaben erscheinen, weil Cyberangreifer erfolgreich waren. Seit 2020 häufen sich die Hackangriffe auf deutsche Medienhäuser: Ob Funke-Mediengruppe, jetzt dpa oder Madsack-Verlag: Es gibt immer mehr Angriffe. Wo kommen diese Angriffe her und wieso sind sie so oft erfolgreich?

Aber wie kann das sein, dass ein Angriff ein komplettes Verlagshaus lahmlegt?

Das hatten wir in den letzten Jahren doch überall: In Krankenhäusern konnte nicht operiert werden, etwa in der Uniklinik Düsseldorf. Ganze Verwaltungen von Kommunen wurden stillgelegt durch Ransomware-Angriffe, also Erpressungs-Software. Jetzt sind verstärkt Medien dran: Weil die meisten schlecht geschützt sind, gelingt das auch.

Lohnenswerte Ziele

Verlage und Medienhäuser scheinen lohnenswerte Ziele zu sein. In der Ukraine werden seit Anfang des Angriffskriegs durch Russland andauernd Medien angegriffen.

Da muss man natürlich unterscheiden zwischen den Medienhäusern hier bei uns und denen in der Ukraine. In der Ukraine ist die Sache klar: Da werden viele Medien immer wieder mit sogenannten DDoS-Attacken angegriffen.

Das sind konzertierte Großangriffe auf Server von Zeitungen, Zeitschriften oder Sendern – und die brechen unter der Last zusammen. Das ist Brachialtaktik – funktioniert aber leider aufgrund mangelnder Sicherheitskonzepte gut.

Auf diese Weise wollen die Aggressoren, sehr wahrscheinlich Russland, die freien Medien behindern. Wenn die seriösen Quellen nicht arbeiten können, haben es Desinformationen leichter. Das ist klare hybride Kriegsführung – da sind sich Experten einig.

Solche Angriffe lassen sich abwehren, indem vor die eigentlichen Server quasi Schutzschilder aufgestellt werden. Ihre Aufgabe ist es, unsinnige Anfragen zu erkennen und abzuwehren. Wenn das gelingt, arbeiten die Server normal weiter. Doch nur die wenigsten Medien haben so etwas.

DDoS-Attacken und Ransomware

Und wie sieht es bei Angriffen auf Medien im Westen aus: Die Fälle häufen sich in den letzten Monaten ja. Auf welche Weise werden die angegriffen – und was steckt dahinter?

Den Informationsfluss zu hemmen, ist hier keine Motivation – dafür ist das Medienangebot viel zu groß. Da gibt es auch gelegentlich DDoS-Attacken – aber hier eher als Warnschuss. Es folgt eine Aufforderung, Schutzgeld zu bezahlen.

Wenn das ausbleibt, drohe ein DDoS-Attacke größeren Ausmaßes, mit den bekannten Folgen. So etwas passiert häufig. Noch häufiger sind aber sogenannte Ransomware-Angriffe. Durch Ausnutzen von Sicherheitslücken und meist durch unachtsames Anklicken eines entsprechend präparierten E-Mail-Anhangs gelangt

Schad-Software auf die PCs, teilweise auch in die Netzwerke und Server.

Alle Daten werden verschlüsselt. Ein Arbeiten ist dann unmöglich. Die Verlage werden mit einer Lösegeldforderung konfrontiert: Wenn sie nicht zahlen, würde der Schaden noch größer. Da sieht sich der eine oder andere Entscheider vielleicht genötigt zu zahlen – was allerdings auf keinen Fall empfohlen wird.

Unzureichend vorbereitet

Stellt sich die Frage: Sind die Verlage also Opfer eines gezielten Kalküls? Oder sind sie einfach zu schlecht gerüstet und vorbereitet?

Beides. Sie eignen sich zweifellos gut als Ziel. Doch Sicherheitsexperten beklagen einhellig: Die meisten Verlage unternehmen zu wenig, um ihre IT-Infrastruktur zu schützen. Sie hoffen und beten, einfach davonzukommen.

Die Verlagswelt ist finanziell unter Druck, keine Frage. Da wird dann auch und besonders an der IT-Sicherheit gespart. Ein fataler Fehler, den allerdings die aller meisten Branchen machen. Egal ob Klein- oder Mittelstand.

Die Statistiken sprechen eine eindeutige Sprache: Cyberangriffe nehmen seit Jahren immer nur zu. Das Risiko wird immer größer. Doch die meisten investieren erst in IT-Sicherheit, wenn sie mal einen Vorgeschmack davon bekommen haben, was passieren kann.

Bei Funke wurde nach den Angriffen vor zwei Jahren mächtig umgebaut und investiert. Das müssen andere Medienhäuser auch machen. Auch die Mitarbeiter müssen geschult werden: Natürlich müssen in Medienhäuser Anhänge geöffnet werden können, das ist klar. Aber Mitarbeiter sollten betrügerische Mails identifizieren können – und wissen, was zu tun ist, wenn etwas verdächtig erscheint.

Die Aufgabe des BSI

Aber was ist eigentlich mit dem BSI, dem Bundesamt für Sicherheit in der Informationstechnik. Die Behörde hat seit Böhmermann Klatsche vor zwei Wochen in ZDF Royale ja viel Aufmerksamkeit bekommen. Sind die nicht verantwortlich?

Klares Nein. Das BSI schützt aktiv nur die IT-Systeme des Bundes. Alle anderen – ob Politik, Wirtschaft, Medien oder wer auch immer – müssen sich selbst kümmern. Das BSI unterstützt durch Warnungen, Informationen und Beratungen.

Aber schützt nicht aktiv die IT-Systeme. Das BSI kann auch keine Abwehr anbieten, das ist auch nicht die Aufgabe des BSI. Das BSI prüft und zertifiziert allerdings IT-Produkte und Dienstleister und bietet Sicherheitsberatung an.

Die muss man aber auch wahrnehmen. Auf politischer Ebene sollte allerdings für eine bessere Zusammenarbeit von Polizei und Sicherheitsdiensten gesorgt werden, um proaktiv auf dieser Ebene zu schützen. Die Cyberangreifer sitzen immer im Ausland und müssten schneller ausfindig gemacht werden. Nur so lässt sich das stoppen, denn insbesondere Ransomware-Angriffe sind viel zu lukrativ.

Account Sharing: Netflix will Kontonutzung einschränken

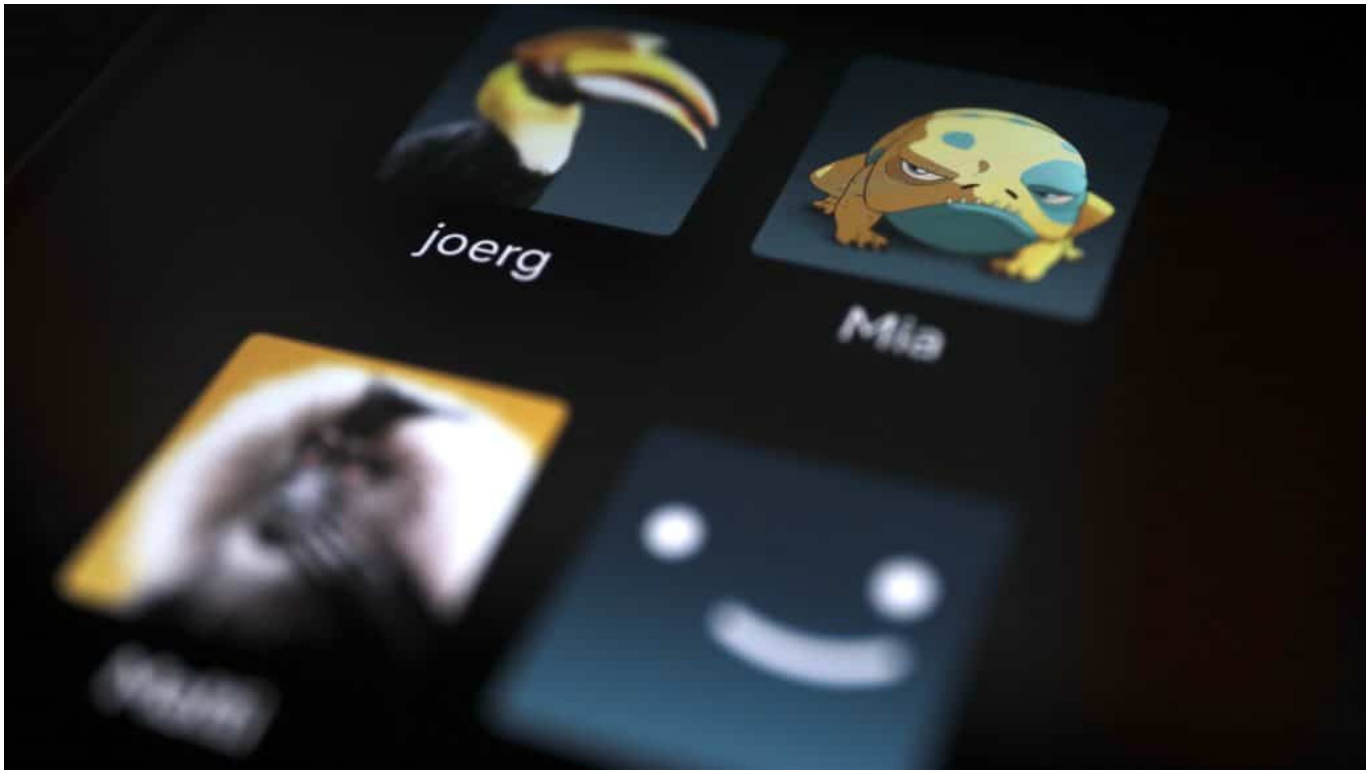
Netflix hat angekündigt: Ab Anfang 2023 wird es nicht mehr möglich sein, die Zugangsdaten zu einem Netflix-Konto mit anderen zu teilen – das kostet dann extra.

Menschen sind erfinderisch – vor allem, wenn sie dadurch Geld sparen können. Viele Kunden des Streamingdienstes Netflix teilen ihre Kontodaten mit Familie, Freunden oder Nachbarn. Nach dem Motto: Reicht doch, wenn einer bezahlt. Da könnt Ihr gerne kostenlos mitschauen.

Mehrfachnutzung von Accounts

Doch diese Praxis soll ab Anfang 2023 nicht mehr möglich sein. Schon seit Jahren versucht Netflix, eine solche Mehrfachnutzung von Abos zu erkennen und zu unterbinden. Ganz einfach ist das nicht, denn Netflix erlaubt durchaus, in einem Konto mehrere Nutzer anzulegen – etwa für Familienmitglieder. Damit die ihre eigenen Lieblingsserien im Blick behalten zum Beispiel.

In den Abomodellen „Standard“ können zwei Personen gleichzeitig mit einem Netflix-Abo streamen, im Modell „Premium“ sogar vier. Das ist also ausdrücklich vorgesehen. Doch die Nutzungsregeln sehen vor: Ein Account darf nur mit Personen geteilt werden, die im selben Haushalt leben – also am selben Ort wohnen. Die Regelung gibt es schon lange, wird aber häufig missachtet.



Rund 100 Millionen Haushalte weltweit schauen illegal

Dadurch entsteht dem Anbieter ein hoher Schaden: Laut Netflix schauen weltweit rund 100 Millionen Haushalte Filme und Serien auf Netflix an, ohne dafür zu bezahlen – weil sie Account-Daten von anderen Kunden nutzen.

Es ist für einen Betreiber wie Netflix nicht einfach, eindeutig zu identifizieren, ob wirklich nur Familienmitglieder einen Unter-Account nutzen. Der Nachwuchs könnte zum Beispiel völlig legal auf dem Tablet netflixen – und das nicht nur zu Hause, sondern auch unterwegs oder bei Freunden. Wann es die eigenen Kinder sind, die ein Konto legal nutzen und wann möglicherweise Nachbarn, mit denen man Tür an Tür wohnt oder Fremde, das lässt sich nur schwer mit Algorithmen erkennen.

Mehrfachnutzung von Accounts

Aber offensichtlich hat Netflix da Fortschritte gemacht. Das Unternehmen hat für 2023 dem kostenlosen Streamen den Kampf angesagt. Ihnen soll der Zugang verwehrt werden. In Zukunft soll jedes Unterkonto 2,99 EUR im Monat extra kosten. Der Streaminganbieter hatte zuletzt in Lateinamerika dieses Modell ausprobiert – und gute Erfahrungen gemacht. Das Preismodell soll Anfang 2023 ausgerollt werden.

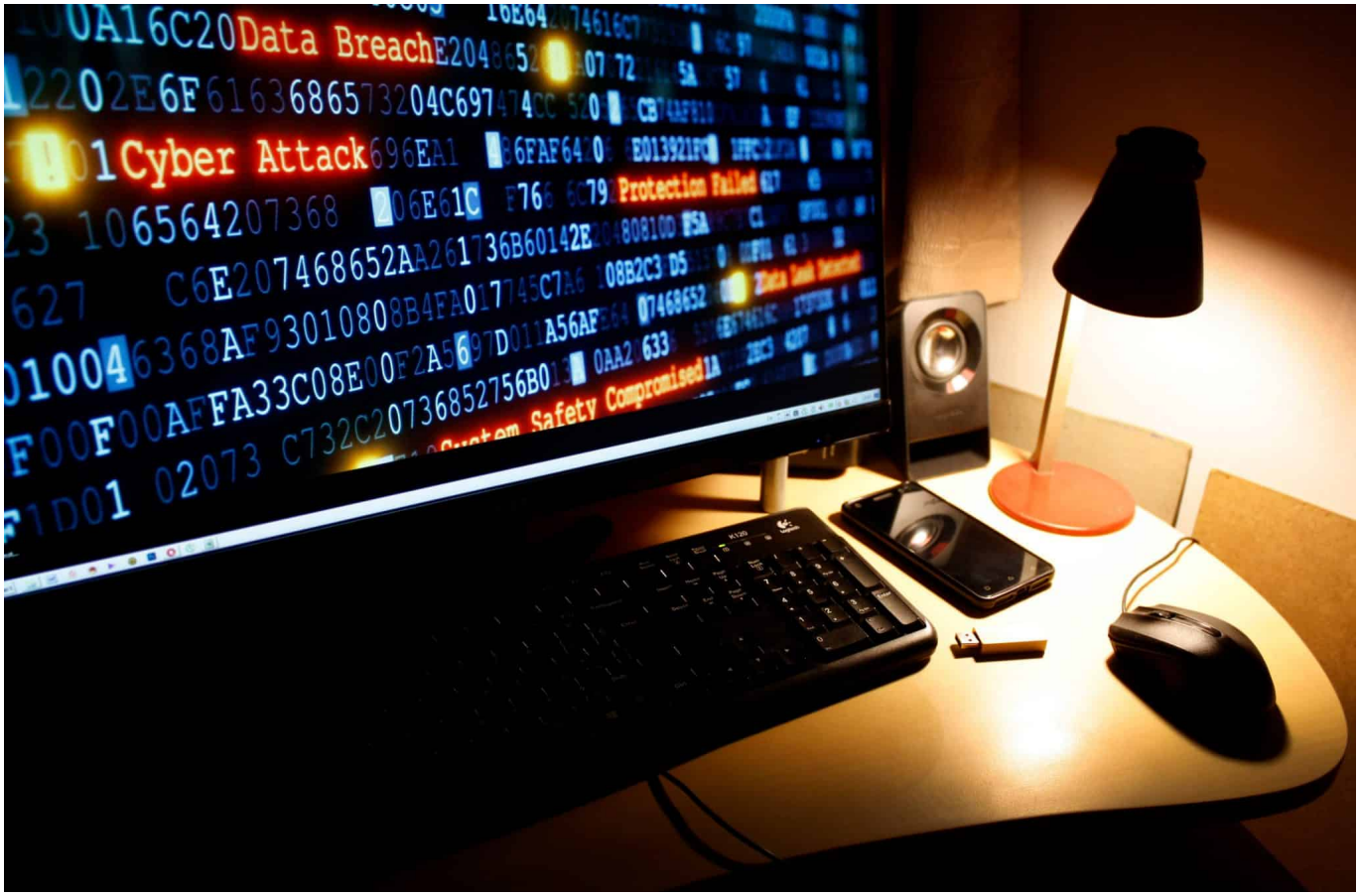
Für 2,99 EUR im Monat Zugang zu Netflix zu bekommen ist immer noch günstiger als ein eigener Account.

Netflix erwartet, dass die neue Preisstrategie insbesondere in den Ländern erfolgreich sein wird, in denen Netflix ein vergünstigtes Abomodell mit Werbeeinblendungen anbietet. In Deutschland soll das ab 3. November der Fall sein: Für 4,99 EUR im Monat gibt’s dann Zugriff auf alle Netflix-Inhalte, allerdings mit regelmäßigen Werbeunterbrechungen.

Die Abozahlen von Netflix waren zuletzt zurückgegangen. Das Unternehmen sucht nach Möglichkeiten, den Umsatz zu stabilisieren.

https://www.youtube.com/watch?v=fw9_HsPEPJM

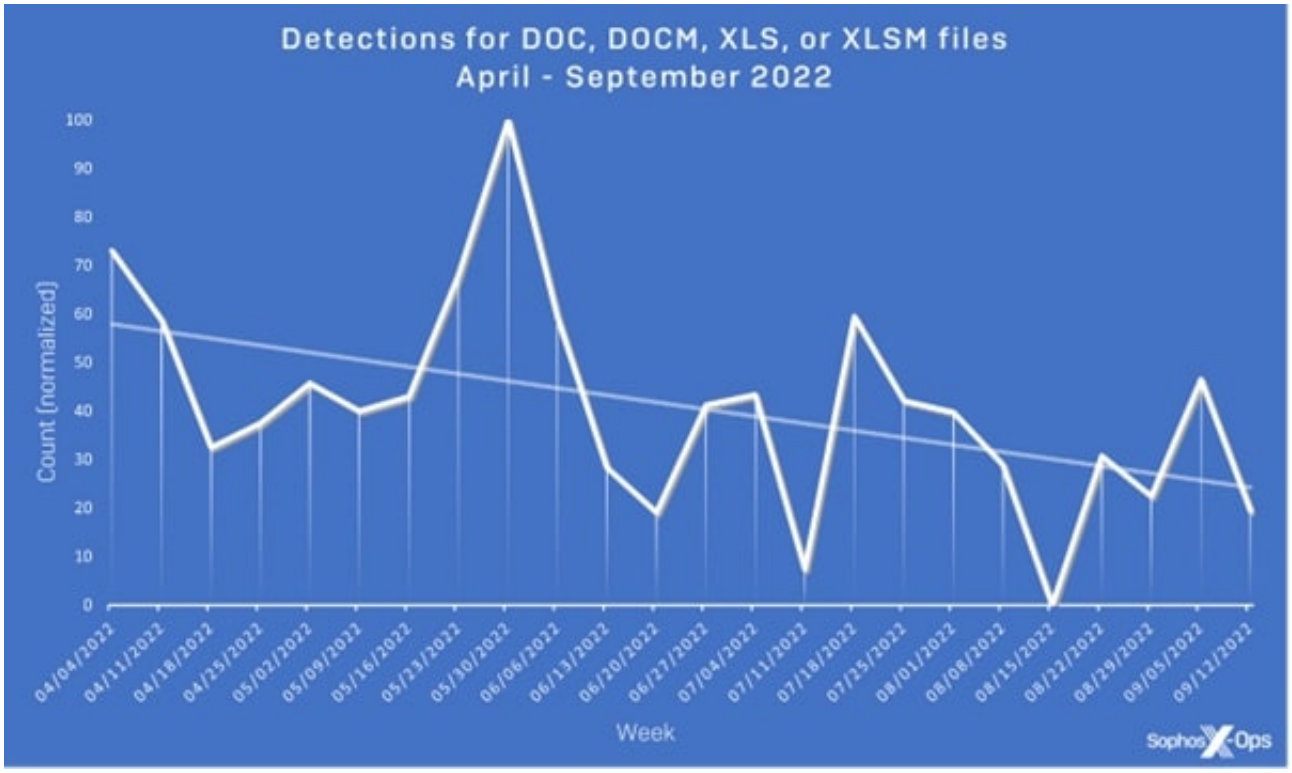
Makros sind out – Cyberkriminelle verlegen sich für die Malware-Verbreitung auf Disk-Images und Archivformate



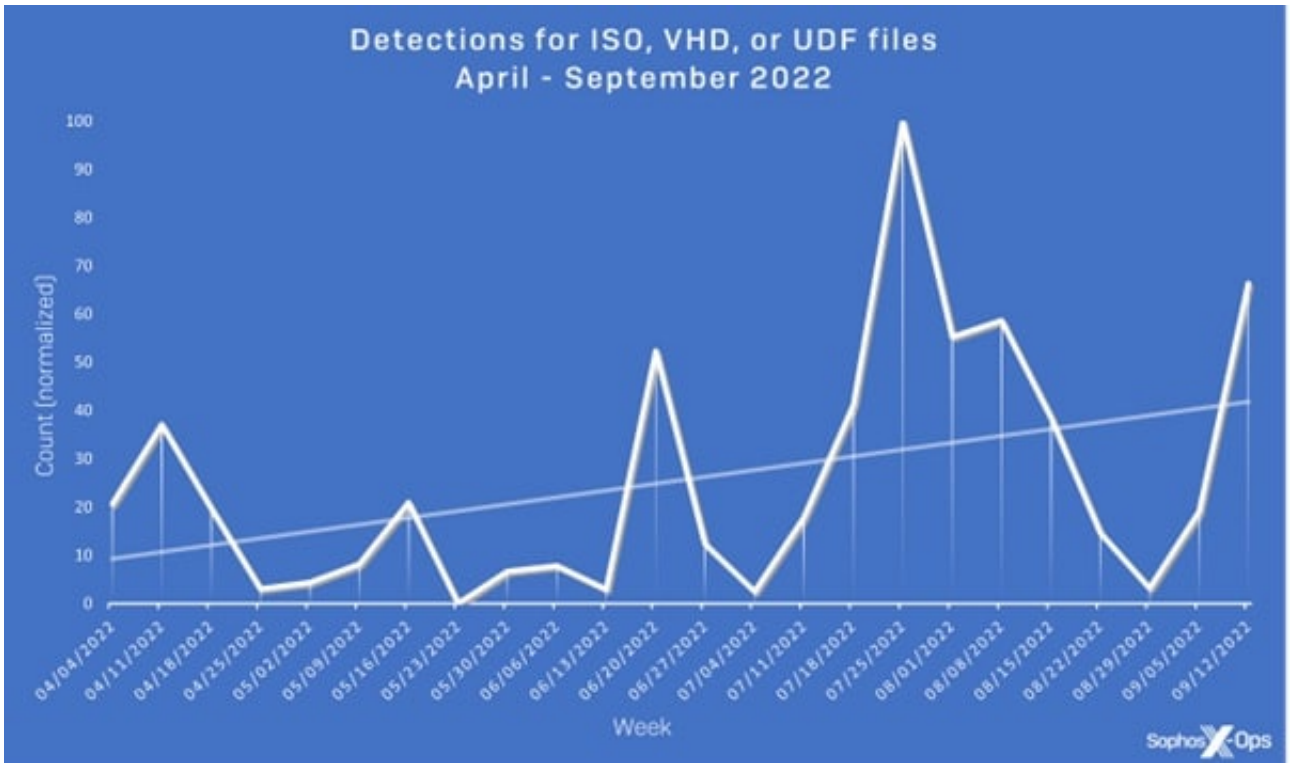
Seit Microsoft Anfang des Jahres angekündigt hat, Makros aus dem Internet zu blockieren, zeigt sich in der Cyberkriminalität ein neuer Trend. Angreifer verwenden jetzt verstärkt Archiv-Formate oder Disk-Images für die Infiltration von Systemen mit Malware. Einfallstor Nummer eins ist dabei nach wie vor die E-Mail.

Februar dieses Jahres kündigte Microsoft an, dass es Makros aus dem Internet standardmäßig blockieren würde. Solche Makros werden seit Jahren von Angreifern missbraucht, um Malware zu übermitteln. Während die Sicherheits-Community spekulierte, dass Angreifer aufgrund der Entscheidung von Microsoft auf alternative Formate ausweichen würden, hat Sophos diese Tatsache anhand seiner Telemetriedaten bereits bestätigt.

Von April bis September dieses Jahres hat Sophos einen starken Rückgang der Anzahl schädlicher DOC-, DOCM-, XLS- und XLSM-Dateien festgestellt – vier beliebte Office-Formate für die Verbreitung schädlicher Makros.



Gleichzeitig war bis Mitte Juni ein stetiger Anstieg der Verwendung obskurer Archivformate (ACE, ARJ, XZ, GZ oder LZH) und ab September ein starker Anstieg der gängigeren Archivformate (ZIP, 7Z, CAB, TAR und RAR) zu verzeichnen. Auch die Verwendung von Disk-Image-Formaten (ISO, VHD und UDF) für die Verbreitung von Malware hat stetig zugenommen.



Disk-Image-Formate sind für Bedrohungsakteure besonders attraktiv, weil sie Microsofts neue "Mark of the Web"-Funktion (MOTW) umgehen. Microsoft verwendet MOTW, um festzustellen, ob ein Makro aus dem Internet stammt oder nicht; ist dies der Fall, wird es automatisch blockiert.

Sicherheits-Software muss das im Blick haben

Sicherheitsprodukte sollten außerdem in der Lage sein, mehrere Archiv- und Disk-Image-Formate zu entpacken, darunter auch unbeliebte Formate, um diese Anhänge ordnungsgemäß auf Malware zu untersuchen. Um die Risiken weiter zu minimieren, können E-Mail-Filter so konfiguriert werden, dass bestimmte Dateiformate standardmäßig blockiert werden. Denn E-Mails zählen nach wie vor zu den Hauptangriffsvektoren.

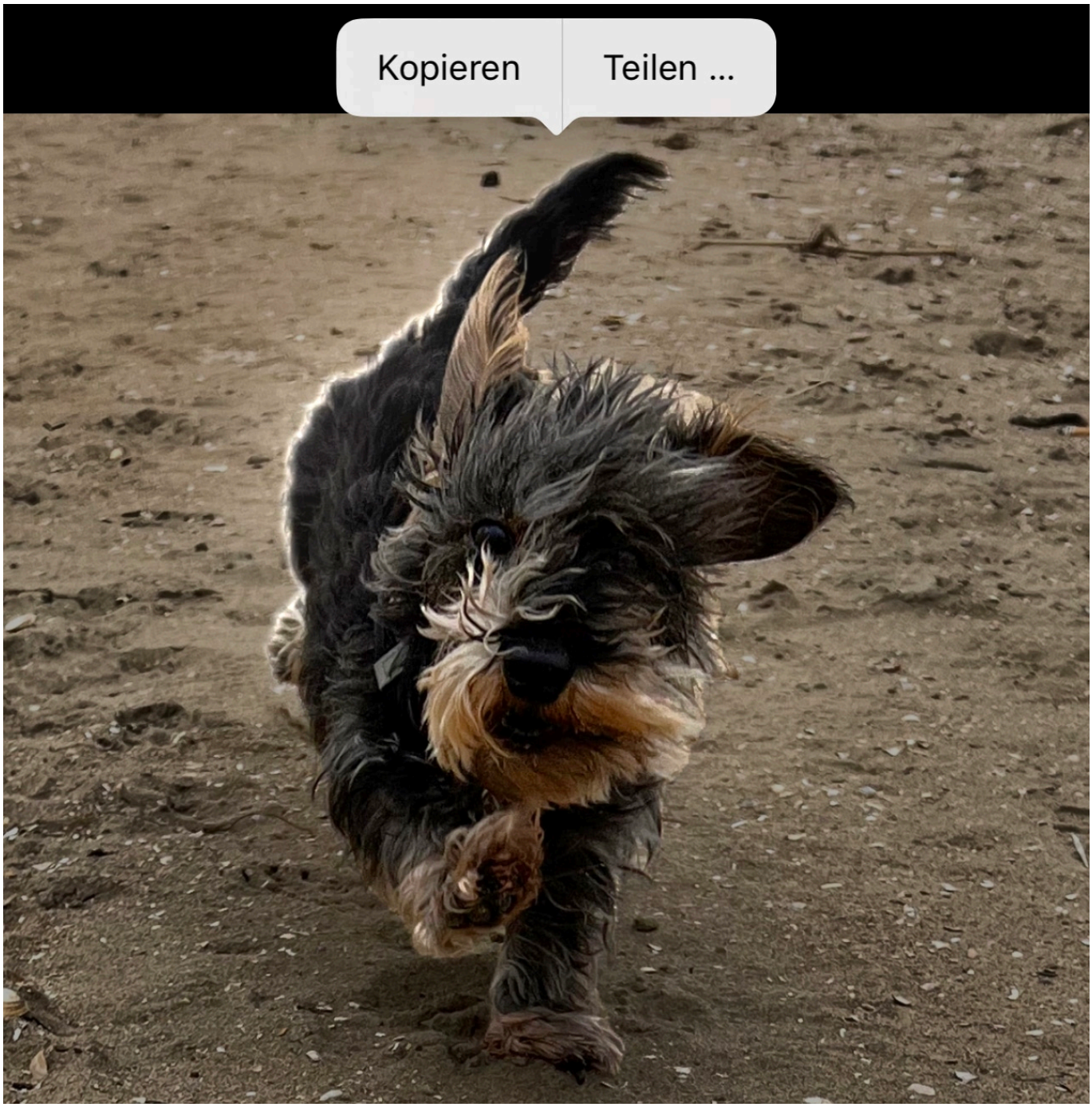
Chester Wisniewski, Principal Research Scientist bei Sophos, sagt: "Wir geben schon seit Jahren dieselben Ratschläge für die E-Mail-Sicherheit. Dinge wie 'Klicken Sie nicht auf diesen Link' oder 'Öffnen Sie keine gefährlichen Attachments'.

Die Realität ist, dass sich die Cybersicherheitslandschaft ständig verändert. Es ist unwahrscheinlich, dass Cyberkriminelle Makros vollständig aufgeben werden, denn sie passen sich mit hoher Wahrscheinlichkeit an diese neuesten

Sicherheitsmaßnahmen von Microsoft an.

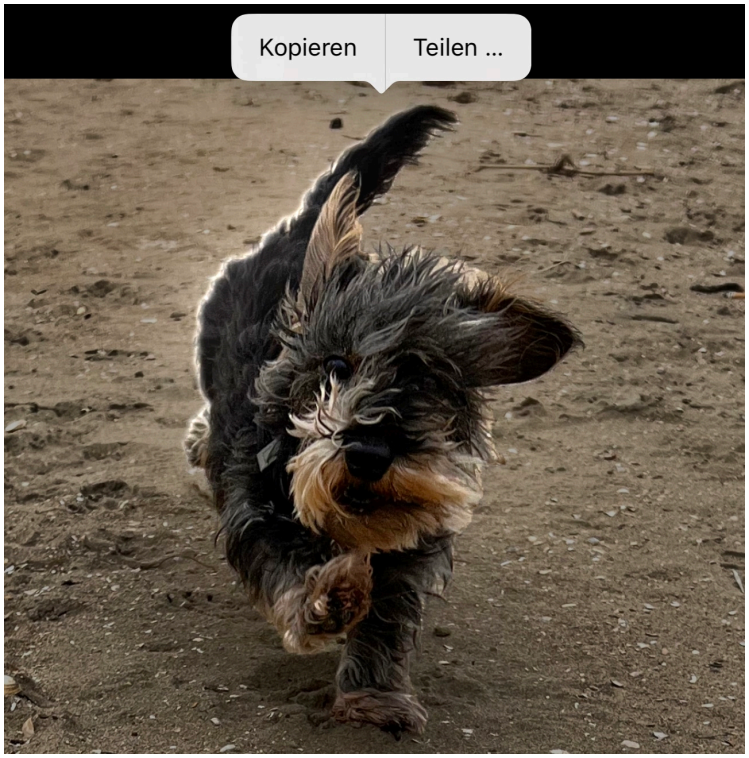
Die Unternehmen sollten das Gleiche tun. Eine gute E-Mail-Sicherheit muss zentral verwaltet werden, wobei sich die Sicherheitsteams auf die technischen Aspekte konzentrieren, z. B. darauf, welche Dateierweiterungen gefährlich sind. Zudem gilt es die Benutzer zu schulen, wie sie vermeiden können, auf das trickreiche Social Engineering der Cyberkriminellen hereinzufallen.“

Versteckter Hack: Bilder in iOS 16 freistellen



Fotos mit dem Smartphone sind schnell und unkompliziert gemacht. Leider oft mit dem Nebeneffekt, dass um das Motiv störende Objekte sind. iOS 16 bietet einen tollen Hack, der ohne großen Aufwand nur das Motiv ausschneidet!

Das so genannte Freistellen von Objekten, also das trennen des Motivs von seinem Hintergrund, ist manuell nicht ganz so einfach. Zu oft verschwimmen das Motiv und der Hintergrund miteinander, und mit manuellen Bildbearbeitungswerkzeugen seid Ihr nie so exakt, dass man die Ränder nicht seht.

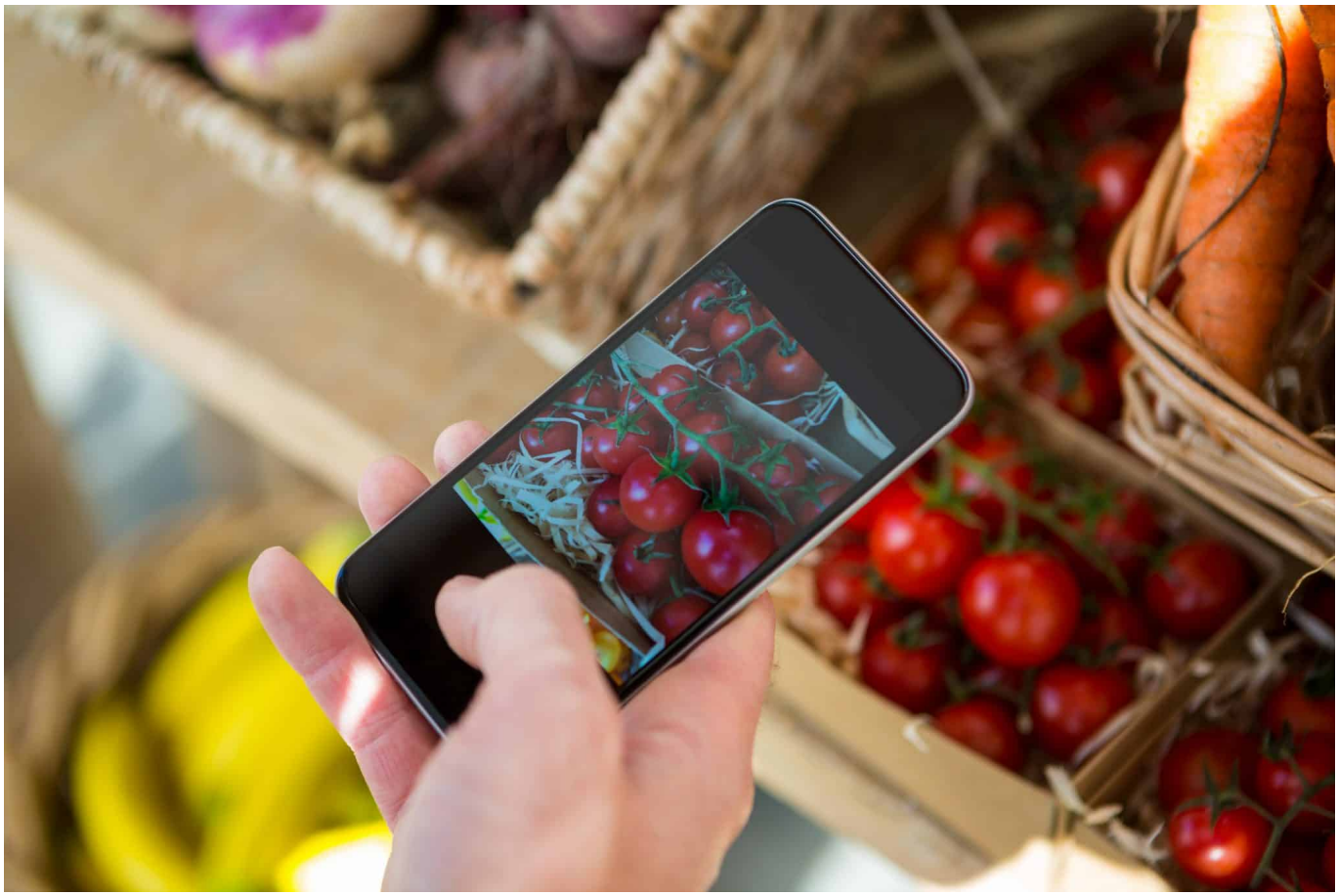


In iOS 16 hat Apple eine Funktion zum Freistellen von Bild-Teilen direkt in die Foto-App integriert.

- Öffnet das Bild, in dem Ihr ein Objekt freistellen wollt, mit der Fotos-App.
- Haltet den Finger einen Moment auf das Objekt auf dem Bildschirm.
- Wenn iOS das Objekt identifizieren konnte, dann zeigt es eine laufende Lichtleiste um das Objekt an.
- Wenn Ihr den Finger jetzt bewegt, dann bewegt sich das Objekt mit dem Finger, damit könnt Ihr leicht sehen, ob die Grenzen korrekt erkannt worden sind.
- Hebt den Finger vom Display des iPhones , dann erscheint am oberen Bildschirmrand eine neue Symbolleiste.
- Tippt auf **Kopieren**, um das freigestellte Objekt in die Zwischenablage zu kopieren und damit in eine E-Mail oder eine andere App einfügen zu können.
- Tippt auf Teilen, um es direkt über iOS an Empfänger per E-Mail,

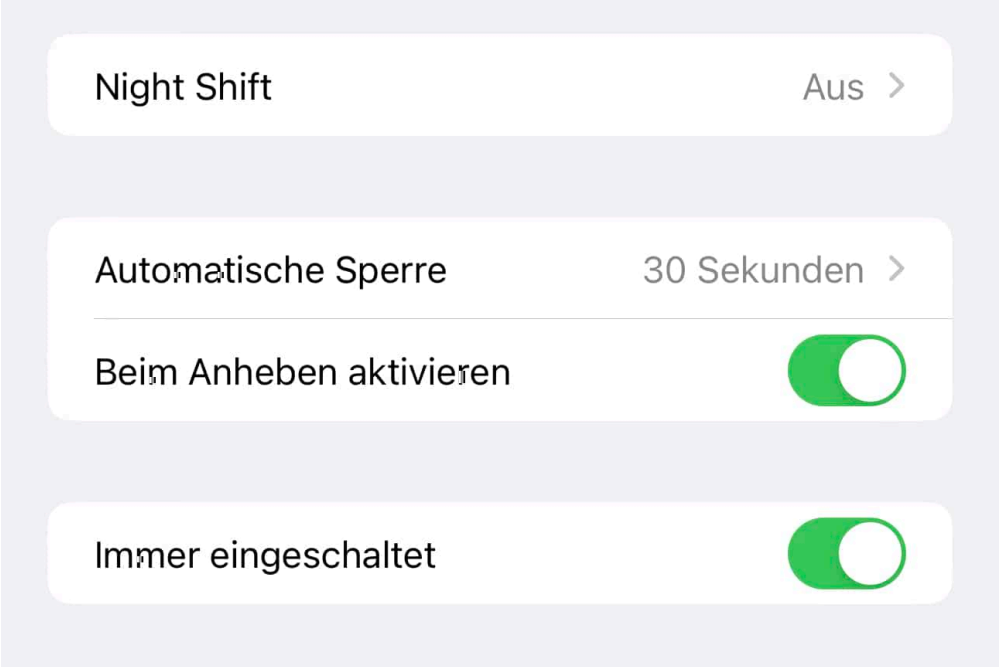
Facebook, Twitter und andere Apps und Dienste weiterzuleiten.

Aktivieren/Deaktivieren des Always On Displays in #iOS16



iOS 16 hat mit dem neuen Sperrbildschirm eine große visuelle Änderung vorgenommen. Wie bei Android lässt sich jetzt ein Sperrbildschirm mit Uhrzeit und Widgets konfigurieren und bei neueren Geräten aus als Always On Display (AOD) verwenden. Das könnt Ihr auch deaktivieren.

Der Sperrbildschirm unterscheidet sich zwischen älteren und neueren Modellen. Das iPhone 14 Pro und Pro Max kann diesen auch bei ausgeschaltetem Display/im Standbymodus darstellen, ältere Geräte nicht. Das liegt daran, dass erst mit der neuen Displaygeneration ein herunterbremsen des Displays auf ein Hertz, also eine Aktualisierung pro Sekunde, möglich ist. Damit und mit extrem verringerter Helligkeit und gedeckten Farben ist erst der stromsparende Betrieb möglich. Wenn Ihr das Always On Display nicht haben wollt, könnt Ihr es recht verdeckt ausschalten:



- Wechselt in die Einstellungen von iOS.
- Rollt nach unten, bis Ihr **Anzeige & Helligkeit** antippen könnt.
- Als vorletzte Option findet Ihr **Immer eingeschaltet**. Deaktiviert den Schalter, um das Always On Display auszuschalten.

Vergleicht ruhig die Laufzeiten des iPhones zwischen ein- und ausgeschaltetem AOD. Diese unterscheiden sich kaum voneinander. Der Stromverbrauch ist also kein Grund, es zu deaktivieren!

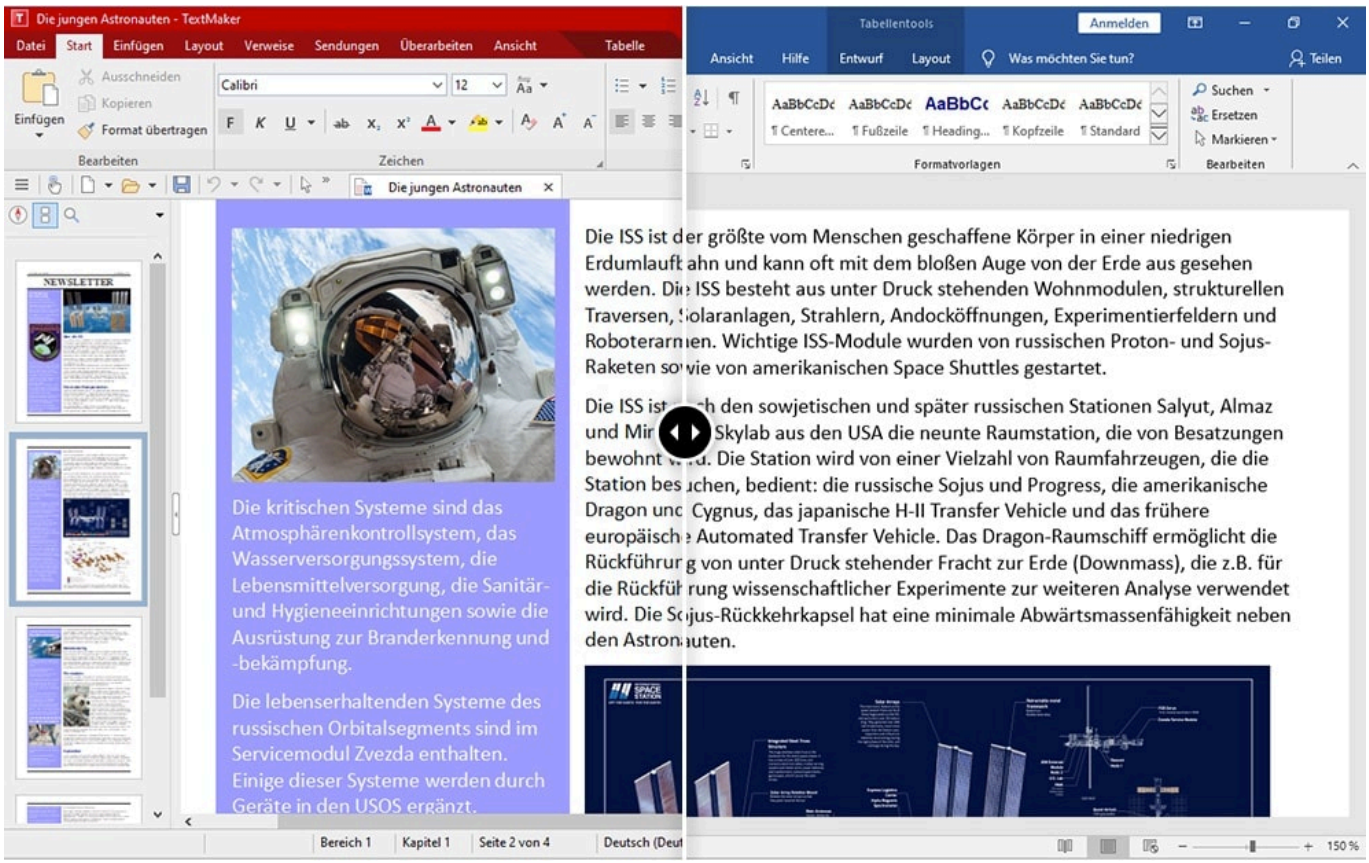
Softmaker FreeOffice: Jetzt updaten!

Es muss nicht immer Microsoft Office sein.Es gibt viele kostenlose Office-Pakete, die für die meisten Anwender vom Funktionsumfang vollkommen ausreichend sind. Beispielsweise Softmakers FreeOffice. Das könnt Ihr jetzt zeitlich begrenzt günstig auf die funktionsreichere SoftMaker Office 2021 aktualisieren.

Statt Word, Excel und PowerPoint habt Ihr bei Softmaker

- Textmaker als Textverarbeitung
- Planmaker als Tabellenkalkulation und
- Presentations als Präsentationsprogramm.

Wenn Ihr die kostenlose Version installiert habt, dann sind dir für viele Anwendungen funktional, allerdings nur als 32bit-Versionen (und damit für viele moderne Geräte nicht optimal), viele spezielle, aber gebräuchliche Funktionen sind nicht freigeschaltet. Die Dateiformate von Softmaker Office sind kompatibel mit den Microsoft Office-Produkten.



Ein wenig versteckt bietet Softmaker gerade das Update auf deren Office 2021 in der "lebenslangen" Version für ein Fünftel des Preises, nämlich EUR 14,95 an. Zusätzlich gibt es noch drei Schriftenpakete für Windows, Mac und Linux dabei. Macht das Sinn?

Hier findet Ihr die Unterschiede zwischen der freien und der kostenpflichtigen Version. Dazu gehören aus Microsoft Office bekannte Funktionen wie:

- Rechtschreibüberprüfung in mehr als 20 Sprachen, Integration des Dudens für Bedeutungs- und Grammatikprüfung.
- Mehrere Dokumente werden in Reitern angeordnet.
- Ausrichtungsfunktionen für Objekte zueinander.
- Wort- und Zeichenzähler für die Einschätzung der Textlänge.
- Recherchefunktion in diversen Online-Quellen.
- TWAIN-Schnittstelle zum direkten Ansprechen von Scannern und Kameras.
- Eine Vielzahl an Vorlagen für die drei Apps.
- Erstellen von portablen Präsentationen.

Updates: So nachhaltig sind sie für Dich – oder die Konzerne

Updates: Manchmal nerven sie, wenn sie mal wieder zu Unzeiten installiert werden müssen. Manchmal freuen wir uns darauf, weil sie neue Funktionen bringen.

Wir kennen das alle: Plötzlich poppt ein Hinweis auf dem Bildschirm oder Display auf – oft zum unpassendsten Moment! –, wir mögen doch bitte ein Update installieren. Für Windows, für MacOS, iOS, Android oder Office.

Gestern erst gab es wieder dringende Updates für Windows 11. Updates gibt es überall. Die meisten installieren diese Updates auch zeitnah, denn es bringt mehr Sicherheit. Sagen auch die Experten: Updates laden, das stopft Sicherheitslücken. Das klingt nachhaltig – wirde können die Geräte lange

benutzen.

Doch regelmäßig kommen auch neue Funktionen dazu. Die machen die Rechner oder Mobilgeräte dann zunehmend langsamer – und es entsteht der Wunsch, ein neues Gerät zu kaufen, das schneller ist. Das klingt nicht nachhaltig. Was ist also nachhaltiger: Keine Updates, dann bleibt möglichst lange alles beim Alten, oder Updates, die einem Gerät ständig neue Jugend spendieren, sie aber irgendwann auch überfordern?

Updates auf dem PC: Oft in ungünstigen Momenten[/caption]

21 Millionen neue Geräte pro Jahr

Es sind etwa 21 Millionen neue Geräte pro Jahr. Das ist eine ganze Menge bei 80 Millionen Deutschen – Babys und Rentner eingeschlossen.

Das zeigt schon, wie oft sich deutsche Konsumenten mit neuen Geräten versorgen. Deutschen halten ihre Mobilgeräte in der Regel 24-36 Monate – und tauschen sie dann aus. Nicht, weil die Altgeräte dann nicht mehr zu gebrauchen wären – sie werden ausgetauscht gegen neuere Modelle.

Updates stopfen Sicherheitslecks

Wenn Updates angeboten werden, insbesondere für Betriebssystem oder wichtige Programme wie Office, dann bin ich einer der ersten, der sagt: Unbedingt installieren.

Updates sind ungeheuer wichtig: Sie sind eine Art Frischzellenkur für ein Betriebssystem, ein Programm, eine App. Meist sind wichtige Korrekturen enthalten, die zum Beispiel Fehler beseitigen und damit Sicherheitslücken schließen. Das ist vor allem bei Betriebssystemen wichtig, aber auch beim Browser oder bei wichtigen Programmen wie Word.

Denn ungestopfte Sicherheitslücken werden ausgenutzt: Kriminelle könnten in die Geräte vordringen und dort zum Beispiel Daten abgreifen. Deshalb sind Updates unverzichtbar. Sie sorgen sogar dafür, dass wir Geräte länger benutzen können. Denn nur, wenn wir unsere Smartphones zum Beispiel auch noch Jahre nach dem Kauf mit Updates versorgen können, lässt sich sicherstellen, dass bekannte Lecks gestopft werden.
[caption id="attachment_782389" align="alignnone" width="1030"]

Gibt es keine Updates mehr, werden die Geräte zu einem Sicherheitsrisiko – und wir sollten darüber nachdenken, sie gegen neuere Geräte auszutauschen, die keine Sicherheitslecks haben. Updates sind also eindeutig ein wichtiges Werkzeug, um Geräte nachhaltig zu machen.

Android: Oft nur zwei, drei Jahre

Aber ich kenne Smartphones, die werden nicht allzu lange unterstützt. Da ist schon nach drei Jahren Schluss. Was mache ich dann?

Wenn wir vor allem über Smartphones und Tablets sprechen: Apple versorgt seine Kunden deutlich länger mit Updates. Meist fünf Jahre und mehr. Das ist in der Android-Welt anders. Da ist jeder Hersteller der Geräte selbst für den Support und das Bereitstellen der Updates mit dem lebenswichtigen Android Betriebssystem verantwortlich.

Vor allem günstigere Geräte werden oft nur zwei, maximale drei Jahre unterstützt. Bedeute: Die Hersteller setzen ein bewusstes Ende für den Gebrauch. Die etwas teureren Modelle erhalten manchmal länger Unterstützung. So hat Samsung für seine teuren Galaxy-Modelle eine Unterstützung von wenigstens vier Android-

Generationen versprochen – das sind in der Regel vier Jahre.

Samsung ist auch noch stolz darauf. Danach gibt es oft keine neuen Updates mehr – und der Druck steigt, auf ein neueres Modell umzusteigen. Das ist alles andere als nachhaltig, weil die Geräte noch problemlos funktionieren, aber nicht mehr offiziell unterstützt werden und damit ein Sicherheitsrisiko darstellen.

Fünf Jahre Update-Pflicht soll kommen

Bislang können die Hersteller selbst entscheiden, wie lange sie Unterstützung und Updates anbieten.

Aber die EU-Kommission will das ändern. Künftig sollen Hersteller wenigstens drei Jahre Updates und fünf Jahre Sicherheits-Updates (also ohne neue Funktionen) verpflichtend anbieten. Die Lobbyisten der Hersteller unternehmen alles, um das zu verhindern – denn es hemmt den Kauf von Neugeräten.

Offensichtlich waren die Lobbyisten erfolgreich, denn in der Bundesregierung waren sogar mal sieben Jahre Update-Pflicht geplant – davon ist nichts mehr zu hören. Vor allem für einige Hersteller von Android-Geräten wird das für ein Umdenken sorgen, denn viele supporten die Geräte nur zwei Jahre.

Vorbildlich sind bislang Apple, Google – mit seinen eigenen Hardwareprodukten – und Samsung bei den teuren Geräten. Gesetzlich vorgeschriebene Mindestlaufzeiten für Updates dienen eindeutig der Nachhaltigkeit: Die Menschen behalten ihre Geräte länger – und kaufen seltener neue Geräte ein.

Updates wecken auch Begierden

Updates haben aber manchmal ja auch einen gegenteiligen Effekt: Durch neue Funktionen geraten die Geräte an ihre Leistungsgrenze – ist das nicht auch ein Motor, der zum Kauf neuerer Geräte fungiert.

Das wurde noch nicht wissenschaftlich untersucht. Aber in der Tat: Manchmal werden Geräte langsamer oder der Akku hält weniger lange durch, nachdem ein Update installiert wurde. Ein Problem, das Apple zum Beispiel schon mehrmals hatte. Ot sind es aber ungewünschte Effekte von neuen Funktionen – man könnte auch „Fehler“ dazu sagen.

Dann werden Korrekturen vorgenommen, und in der nächsten Version ist wieder alles gut. Aber es stimmt auch: Updates mit neuen Funktionen machen ein Betriebssystem nicht unbedingt schlanker. Im Gegenteil: Es verbraucht mehr Speicher. Und neue Funktionen sind vielleicht mit neuen Apps verbunden, die verbrauchen auch wieder mehr Speicherplatz – ebenso die Daten, die anfallen.

Da kann durchaus der Eindruck entstehen: Allerhöchste Zeit, Dich mit einem neuen Gerät zu versorgen. Das gilt natürlich auch für den Fall, dass es neue Funktionen gibt, über die man liest, die aber nur in neuen Modellen funktionieren.

Nicht aus Boshaftigkeit, sondern weil ein bestimmter Prozessor als Mindestausrüstung vorausgesetzt wird oder besondere Sensoren oder Technologien vorausgesetzt werden. Auch das erzeugt einen gewissen Druck: Rüste auf!

Auch das ist nicht nachhaltig. In einer idealen Welt hätten User die Wahl: Nur

Sicherheits-Updates laden – die würden nicht mehr Speicher kosten und auch das Gerät nicht träger machen. Oder ein Update mit neuen Funktionen laden und installieren. Aber kein Hersteller der Welt betreibt einen solchen Aufwand.

Wenn Fenster plötzlich verschwinden

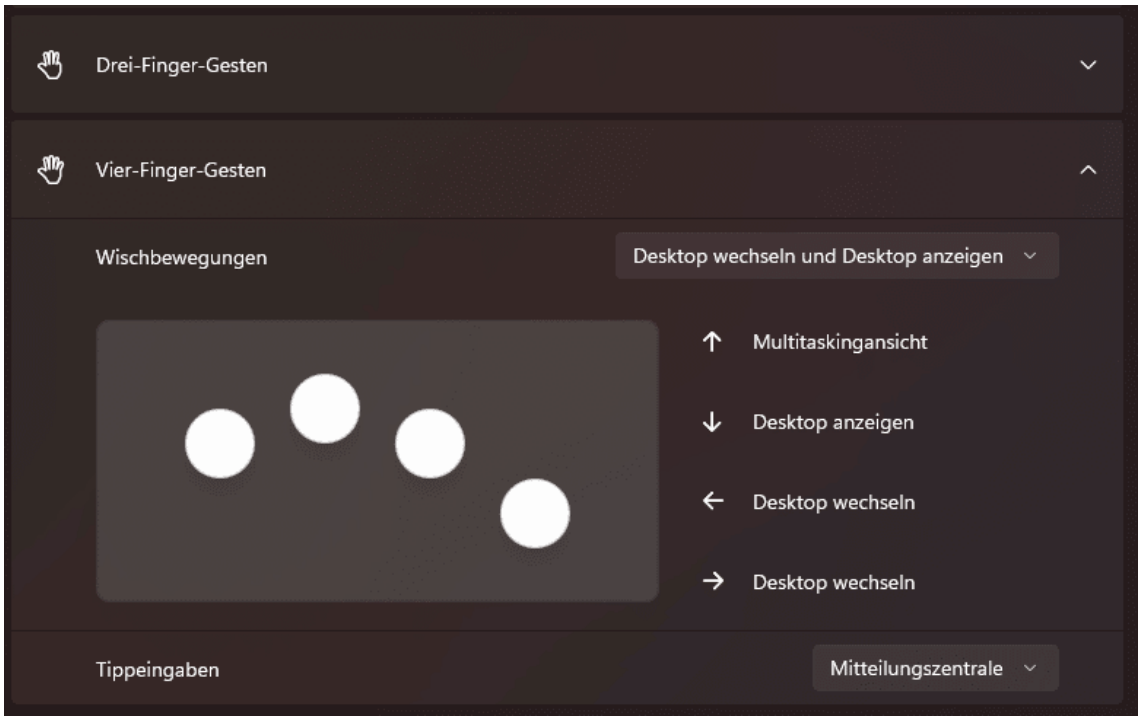
Wenn Ihr ein Touchpad auf einem Notebook oder als Alternative zur Maus verwendet, dann kennt Ihr die Situation bestimmt: Plötzlich sind alle Fenster weg und müssen manuell wieder in den Vordergrund geholt werden. Wir zeigen Euch, wie Ihr das vermeidet!

Im Gegensatz zur Maus hat das Touchpad viele Vorteile:

- Es ist vom Platzbedarf her deutlich kleiner als der Bewegungsbereich der Maus, vor allem bei einem hochauflösenden/breiten Monitor.
- Es bedarf keiner Bewegung, darum kann es gut in mobile Geräte wie Notebooks integriert werden.
- Es unterstützt Multitouch, kann also nicht nur einen Finger, sondern gleich mehrere Fingerberührungen gleichzeitig erkennen.

Gerade der letzte Punkt ist Fluch und Segen gleichzeitig: Windows unterstützt bei Touchpads Gesten mit mehreren Fingern. Wenn Ihr schnell arbeitet, dann kann es schnell vorkommen, dass ein Finger zu viel das Touchpad berührt und Windows eine Geste erkennt, die Ihr gar nicht ausführen wolltet. Beispielsweise im Standard mit vier Fingern den Desktop anzeigen (und damit alle Fenster minimieren). Diese Gesten könnt Ihr anpassen und auch deaktivieren:

- Klickt in den Einstellungen von Windows auf **Bluetooth und Geräte** > **Touchpad**.
- Klickt auf **Vier-Finger-Gesten**, dann auf das **Auswahlfeld neben Wischbewegungen**.
- Ihr könnt hier nur Profile auswählen, die automatisch alle vier Wischbewegungen festlegen, darum klickt auf den Eintrag **Nichts**.

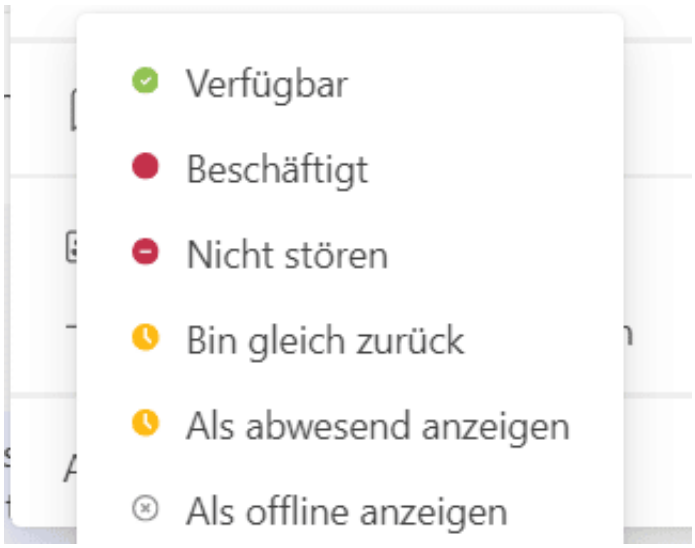


Die Zusatzgesten sind damit deaktiviert und Windows führt keinen Befehl aus, wenn Ihr das Touchpad entsprechend berührt.

Störungen in Teams vermeiden: Nicht stören

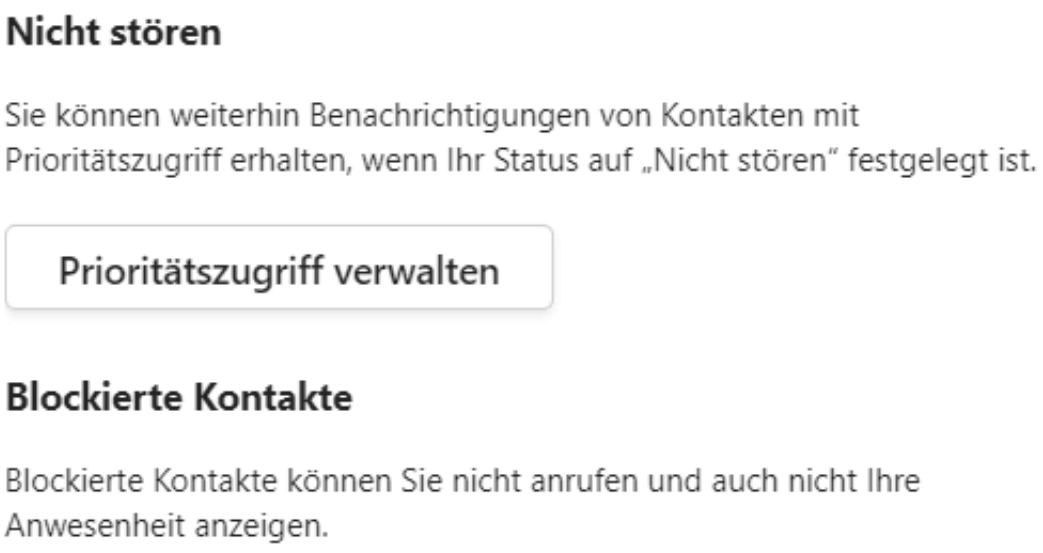
Eigentlich wollt Ihr nicht gestört werden, aber wenn der Chef anruft, dann soll der natürlich durchkommen. Was wie die Quadratur des Kreises aussieht, lässt sich in MS Teams leicht umsetzen.

Videokonferenzen haben unsere Art zu arbeiten verändert: Wir können schnell und ohne lange Reise Menschen in aller Welt erreichen. Auf der anderen Seite sind wir damit natürlich nahezu immer und überall erreichbar. Das kann schon nerven, vor allem wenn Konzentration für eine Aufgabe nötig ist. Es bietet sich an in Teams den Status **Nicht stören** zu setzen:



- Klickt auf Euer Profilbild oben rechts in Teams, dann auf aktuellen Status unten rechts neben Eurem Namen.
- Klickt auf **Nicht stören.**

Unter der Symbolleiste von Teams erscheint nun ein Infotext, dass nur dringende Nachrichten durchgelassen werden. Um festzulegen, welche Absender wichtige Nachrichten senden, klickt auf **Einstellungen ändern** in diesem Infotext.



- Teams zeigt Euch eine Liste der bereits angelegten Prioritätskontakte an.
- Um den Status eines Kontakts als Priorität zu löschen, klickt auf das Kreuz rechts vom Namen.
- Um einen neuen Kontakt mit Priorität hinzuzufügen, sucht diesen durch

Eingabe des Namens unter **Kontakte hinzufügen** aus der Kontaktliste heraus oder gebt dessen E-Mail-Adresse ein, wenn er nicht zu Eurer Organisation gehört.

Die Kontakte, die Ihr hier festgelegt habt, können Euch auch erreichen, wenn Euer status "Nicht stören" ist. Ihr könnt sie auf dem beschriebenen Weg jederzeit anpassen. Beispielsweise, wenn der Chef dann doch zu sehr nervt.

Installation des Windows 11 22H2-Updates durchführen

Neue Features sind immer willkommen. Microsoft kanalisiert diese in den halbjährlichen Windows-Updates. Gerade ist das 22H2-Update verfügbar geworden, das unter anderem den Android-App-Store bringt. Die Installation startet aber nicht automatisch. Wir zeigen Euch wie Ihr sie starten könnt!

Normalerweise sind Updates bei Windows seit einigen Monaten verpflichtend. Zu viel Schaden ist entstanden, weil Benutzer Updates nicht installiert haben. Nun haben die Funktionsupdates eine Sonderstellung: Das sind die Updates, deren Namen sich immer aus der zweistelligen Jahreszahl und dem Halbjahr zusammensetzen (22H2 ist also das zweite Halbjahresupdate des Jahres 2022). Die haben neue Funktionen und ändern die Art, wie Ihr mit Windows arbeitet. Aus diesem Grund wartet Windows auf Eure Freigabe, bevor eine solch weitreichende Anpassung von Windows vorgenommen wird.

- Wechselt in die **Einstellungen** von Windows, dann auf **Windows Update**.
- Wenn ein Funktionsupdate zur Verfügung steht, dann seht Ihr das unter den Sicherheit-Updates mit einem separaten Button **Jetzt installieren**.
- Bevor Ihr auf den klickt, speichert auf jeden Fall alle Daten in den Programmen, die Ihr gerade offen habt, ein Funktionsupdate erfordert immer einen Neustart!
- Das Herunterladen und Installieren des Halbjahresupdates könnt Ihr im Update-Bildschirm verfolgen, der Prozess dauert in der Regel bis zu einer Stunde.
- Nach Abschluss der Installation klickt auf **Jetzt neu starten**, um den Neustart durchzuführen. Während dieses Neustarts werden diverse Anpassungen in den Systemdateien gemacht. Das dauert wiederum einige Minuten.
- Wenn Ihr wieder am Anmeldebildschirm seid, dann ist die Installation abgeschlossen und Ihr könnt Windows normal benutzen.


Windows Update
Neustart erforderlich
Ihr Gerät wird außerhalb der Nutzungszeit neu gestartet.
Neustart planen
Jetzt neu starten
Windows 11, version 22H2
Neustart ausstehend
Weitere Optionen
Updates aussetzen
Für 1 Woche anhalten
Updateverlauf