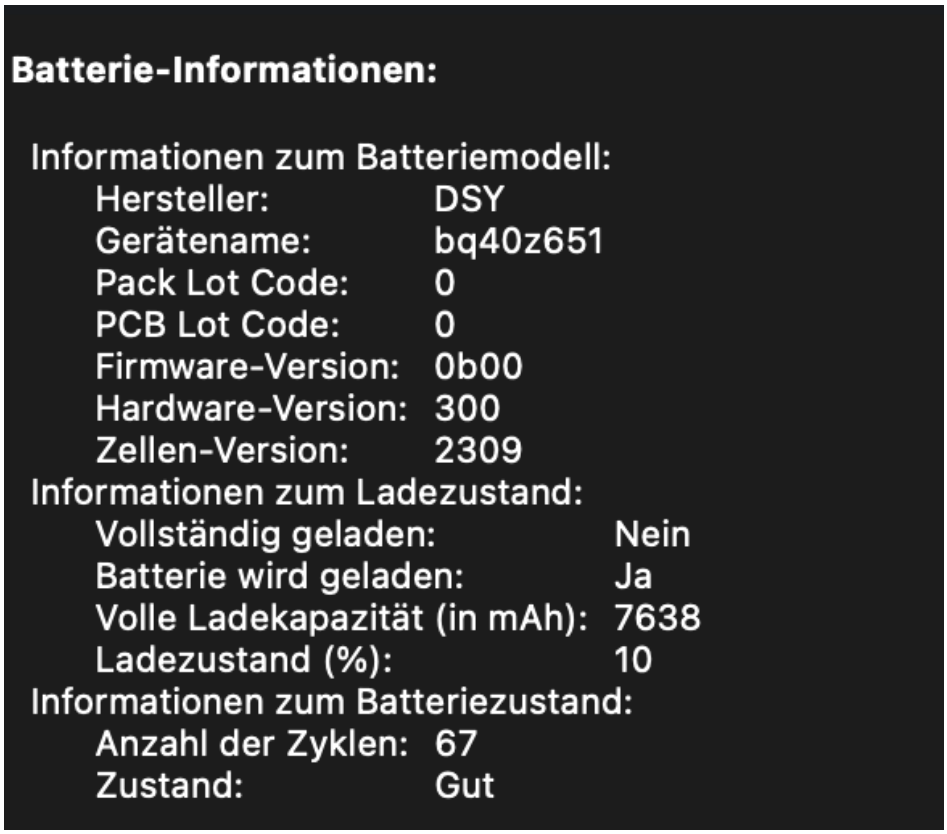
Schieb Report

Ausgabe 2022.20

Ladezyklen und Batteriezustand beim Macbook finden

Der Akku ist eine der wichtigsten Komponenten bei einem Notebook. Wichtig also, diesen vor Kauf zu kontrollieren. Beim MacBook ist das mit wenig Aufwand möglich.

Auch wen die Zeiten lange vorbei sind, als der Benutzer seinen Akku nach einem mehrseitigen Handbuch ganz präzise laden und entladen musste, ganz ohne Effekt ist der proaktive Umgang mit dem Akku nicht. Moderne Akkus und deren Ladeelektronik im Gerät lernen vom Benutzer und seiner Nutzung des Notebooks und passen das Laden des Akkus darauf an.



Trotzdem solltet Ihr den Akku immer mal wieder so weit wie möglich entladen, das tut nicht nur den Zellen gut, sondern kalibriert auch die Anzeige der Restlaufzeit des Akkus.

Unabhängig davon gilt: Je häufiger ein Akku geladen wird, desto näher rückt der Zeitpunkt, an dem er Kapazität verliert. Ein "wenig genutztes" Gerät kann trotzdem viele Akkuladungen hinter sich haben, weil es nach den kurzen Einsätzen immer direkt geladen wurde. Unter macOS könnt Ihr das kontrollieren:

Klickt auf den Apfel oben links, dann auf **Über diesen Mac** > **Systembericht**. In der Übersicht findet Ihr die Kategorie **Batterie-Informationen**. Klickt die an, dann seht Ihr unter **Informationen zum Batteriezustand** zwei Informationen:

- Die **Anzahl der Zyklen** zeigt an, wie oft ein Akku geladen wurde. Je höher dieser Wert, desto schlechter.
- Der **Zustand** bewertet den Allgemeinzustand des Akkus. Alles schlechter als "Gut" sollte Euch vom Kauf abhalten.

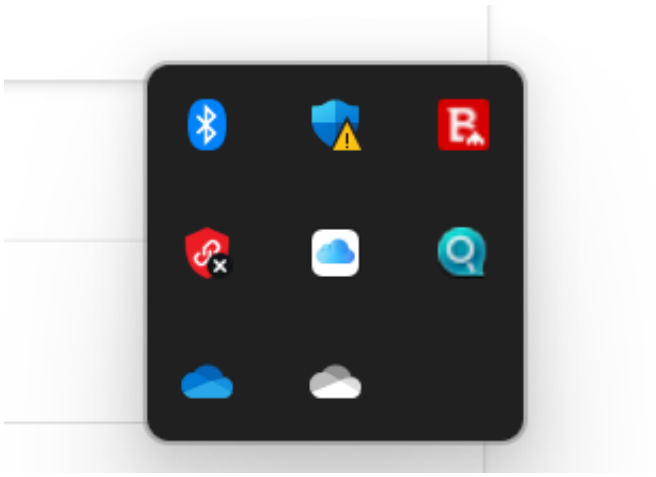
Bitdefender VPN ausschalten

Werbung nervt. Auch dann, wenn sie Teil eines Produktes ist, das man tatsächlich verwendet. Bitdefender als Virenlösung ist da ein gutes Beispiel. Schluss mit dem Werbewahn!

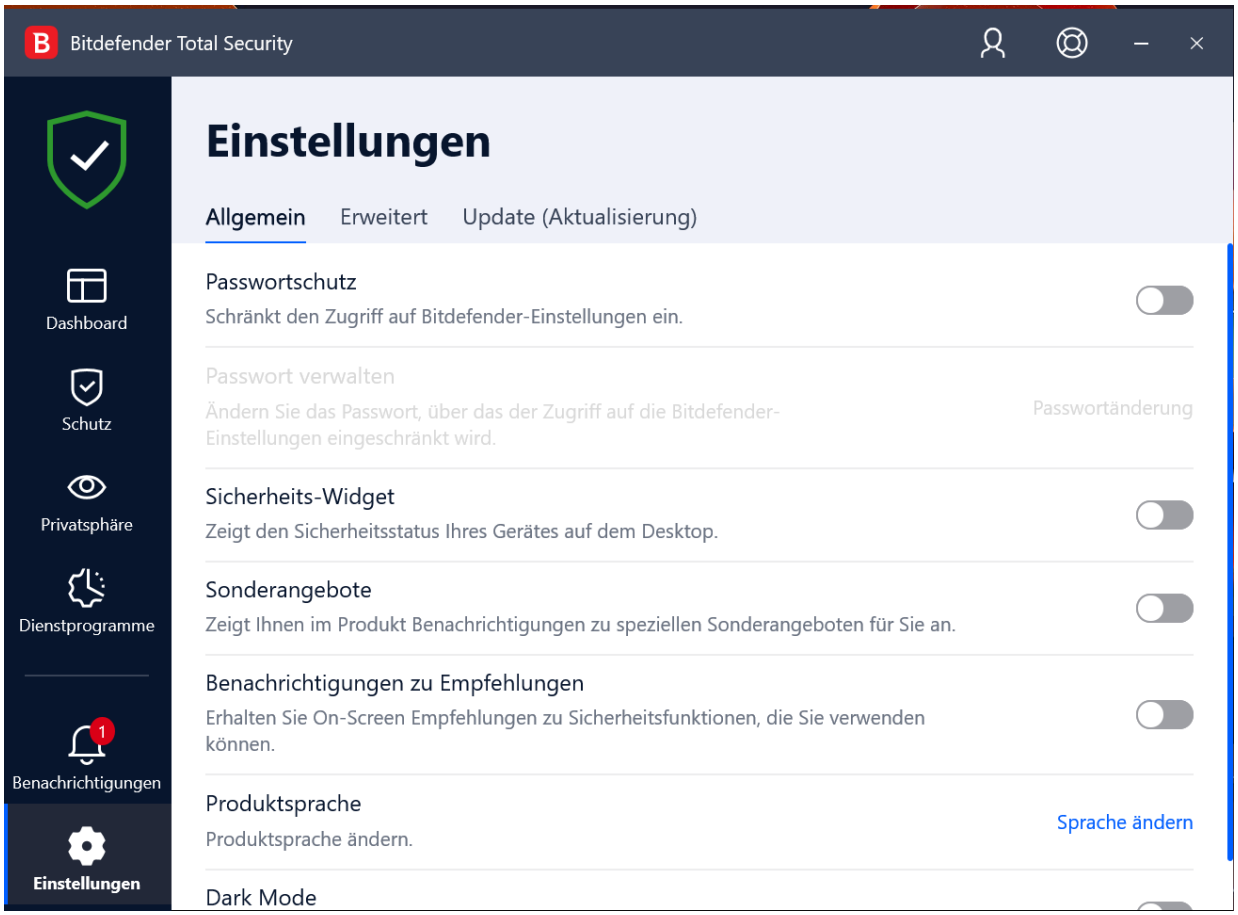
Die Bitdefender Internet Security in ihren diversen Ausprägungen ist immer wieder in den Hitlisten der besten Antiviren-Lösungen vorne dabei. Als wenn der nicht geringe Preis nicht genug wäre, versucht der Hersteller, Euch weitere Produkte anzupreisen. Spätestens dann, wenn dauernd irgendwelche Banner über den Bildschirm flattern, stört das gewaltig.

Bitdefender VPN deaktivieren

VPN-Verbindungen haben viele Vorteile für den Anwender. Die lassen sich aber auch deutlich günstiger und verträglicher als über Bitdefender.



Um das Tool erst einmal zu deaktivieren - es wird beim Start von Windows einfach mal mit gestartet - klickt in den Benachrichtigungsbereich von Windows unten rechts in der Taskleiste. Ein Rechtsklick auf das Symbol von Bitdefender VPN (das Schild mit der Kette darin) und Beenden **schließt** es für die aktuelle Sitzung.



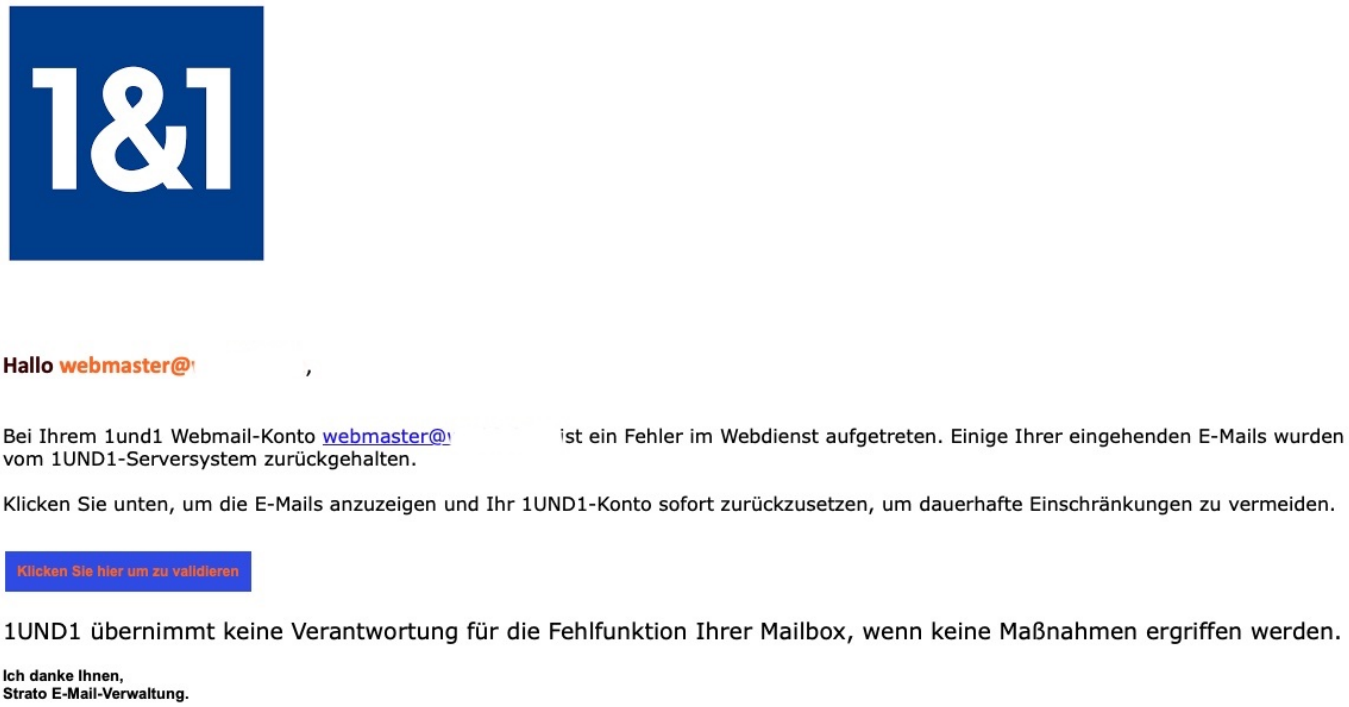
Werbungen allgemein ausschalten

Allgemein findet Ihr den Werbewust von Bitdefender im Hauptfenster der App. Klickt unten rechts auf das Zahnrad neben **Einstellungen**. In der Registerkarte **Allgemein** schaltet die Optionen **Sonderangebote** und **Benachrichtigung zu Empfehlungen** aus. Bitdefender zeigt jetzt nur noch Benachrichtigungen an, die zu Sicherheitsvorfällen gehören, beispielsweise gefundene Viren oder Webseiten, die als Phishing-Sites bekannt sind.

Vorsicht bei angeblichen Mailproblemen bei 1&1

Phishing-E-Mails sind ein zunehmendes Übel. Je besser sie gemacht sind, desto eher reagieren Anwender darauf und geben unfreiwillig ihre Zugangsdaten preis. Gerade macht ein angebliches technisches Problem bei 1&1 die Runde. Vorsicht!

Wie versetzt man einen Anwender schnell in Panik? Man sagt ihm, dass ein wichtiger Dienst nicht funktioniert und er umgehend Maßnahmen ergreifen muss, um das Problem zu beheben. Da bietet sich das eigene E-Mail-Konto natürlich an! Die Phishing-Email von "1und1 Webmail" macht genau das: Angeblich sind aufgrund eines technischen Problems die Mails eines existierenden Postfaches nicht zustellbar. Um das zu lösen, müsst Ihr Euch sofort anmelden und das "Konto zurücksetzen" (was immer das heissen mag).



Hallo webmaster@ ,

Bei Ihrem 1und1 Webmail-Konto webmaster@ ist ein Fehler im Webdienst aufgetreten. Einige Ihrer eingehenden E-Mails wurden vom 1UND1-Serversystem zurückgehalten.

Klicken Sie unten, um die E-Mails anzuzeigen und Ihr 1UND1-Konto sofort zurückzusetzen, um dauerhafte Einschränkungen zu vermeiden.

Klicken Sie hier um zu validieren

1UND1 übernimmt keine Verantwortung für die Fehlfunktion Ihrer Mailbox, wenn keine Maßnahmen ergriffen werden.

Ich danke Ihnen,
Strato E-Mail-Verwaltung.

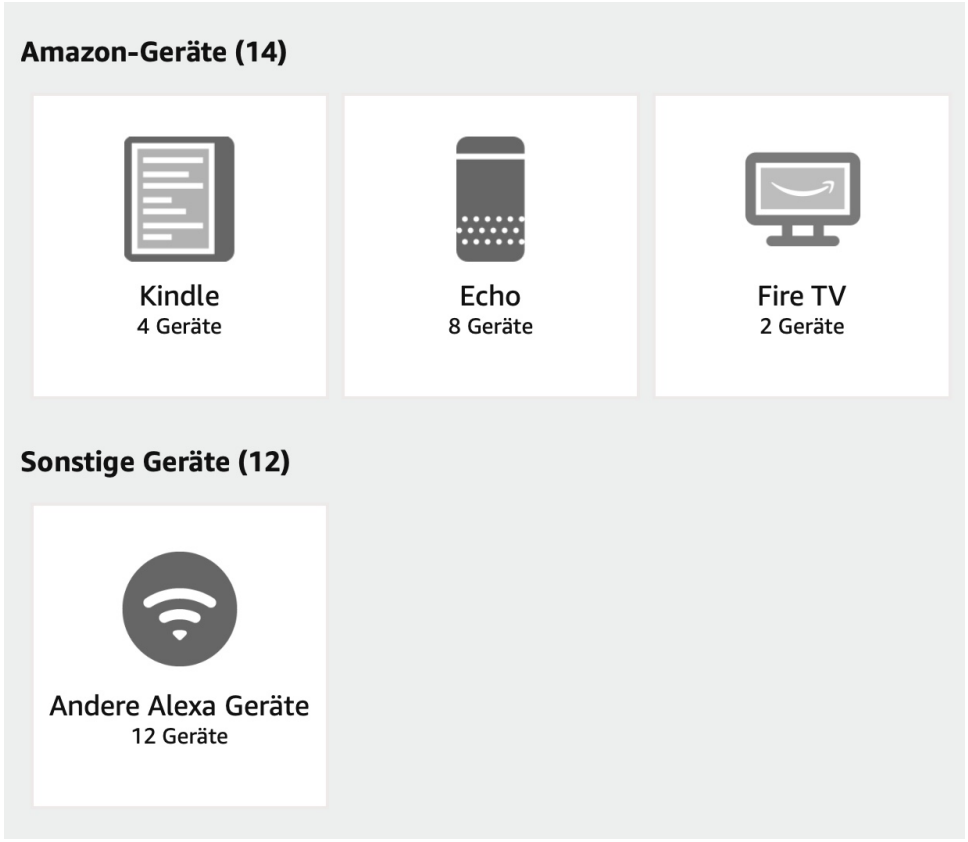
Nun führt der Link in der E-Mail aber nicht zur echten 1&1-Anmeldeseite, sondern zu einer Fake-Seite, die Eure Anmeldedaten abgreift. Erst damit habt Ihr dann das Problem: Mit diesen Daten können sich die Angreifer dann tatsächlich an Euer Konto anmelden und es übernehmen. Darum Vorsicht: Klickt niemals auf die Links in einer solchen E-Mail, sondern ruft manuell im Browser die Webseite des Anbieters auf. Dort meldet Euch an.

Sollte wirklich ein Problem mit dem Konto oder Dienst bestehen, dann wird Euch das im Portal gemeldet. Ist das nicht der Fall, dann handelt es sich um eine Phishing-E-Mail, die Ihr einfach ignoriert und löscht.

Verwenden von ePub-Dateien mit Kindles

Einen Kindle als eBook-Reader zu nutzen ist bequem, wenn man sowieso ein Amazon-Konto hat. Das Standard-Format ePub unterstützt der nämlich nicht direkt. Über diesen Hack könnt Ihr aber trotzdem ePubs am Kindle lesen!

Seit vielen Jahren ist ePub das verbreiteste Format für eBooks. In der Folge unterstützen fast alle eBook-Reader dieses Format. "Fast alle", denn Amazon verweigerte sich bisher erfolgreich und machte den Einsatz von Drittanbieter-Tools wie Calibre nötig. Nicht wirklich komfortabel.



Ein wenig versteckt hat Amazon das Verfahren jetzt vereinfacht: Wer eine ePub-Datei an die E-Mail-Adresse des Kindles schickt, der bekommt das eBook auf dem Kindle angezeigt: Seit neuestem konvertiert die Kindle-Software nämlich ePubs in das geräteeigene AZW-Format. Allerdings nur dann, wenn die Datei nicht verschlüsselt bzw. mit einem Kopierschutz versehen ist.

Wie findet Ihr nun die E-Mail-Adresse des Kindle?

- Meldet Euch bei Eurem Amazon-Konto an und klickt unter **Digitale Inhalte und Geräte** auf **Inhalte und Geräte**.
- Klickt auf den Reiter **Geräte**, dann auf Kindle und sucht Euch den Kindle heraus, an den Ihr eine Datei senden wollt.
- In der Geräteübersicht findet Ihr die E-Mail-Adresse. Die ist meist kryptisch, durch einen Klick auf **Bearbeiten** könnt Ihr sie - Verfügbarkeit der gewünschten Adresse vorausgesetzt - verändern.

Schickt eine E-Mail mit einer ePub- (oder PDF-) Datei an diese E-Mail-Adresse, dann steht das Buch nach kurzer Zeit in Eurer Bibliothek zum Lesen bereit.

Hackerverbund Killnet: Hackangriffe der „kleinen Nadelstiche“

Der Verfassungsschutz warnt vor allem Unternehmen vor mehr Cyberangriffen – und mahnt zur Vorsicht. Der prorussische Hackerverbund „Killnet“ greift Ziele im Westen an. Was dahinter steckt – und wie jeder einzelne für mehr Sicherheit sorgen kann.

Seit Beginn des russischen Angriffskrieg auf die Ukraine warnen deutsche Behörden vor vermehrten Cyberangriffen durch russische Hacker. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hatte zuletzt sogar vor der Einsatz der aus Russland stammenden Sicherheitssoftware „Kaspersky“ gewarnt.

Bundesamt für Verfassungsschutz warnt vor Angriffen

Generell wurden Angriffe auf NATO-Staaten befürchtet, auch auf Einrichtungen und Unternehmen in Deutschland. Jetzt warnt das Bundesamt für Verfassungsschutz aktuell vor vermehrten Angriffen, allerdings nicht vor militärischen Angriffen, sondern vor Spionage. Vor allem das Risiko für Wirtschaftsspionage seien nach Einschätzung der Behörde gestiegen. Insbesondere, weil die russische Wirtschaft zunehmend vom Rest der Welt abgekoppelt ist und versuchen könnte, durch Spionage Schritt zu halten.

Namentlich wurde die prorussischer Hacker-Gruppierung „Killnet“ genannt. Ein loser Hackerverbund, der sich – ähnlich wie nach dem Aufruf des westlichen Hackerverbunds „Anonymous“ – über den Messengerdienst „Telegram“ organisiert. Hier werden potenzielle Angriffsziele besprochen, neben dem „European Song Contest“ (ESC) vor einigen Tagen nun auch deutsche Webseiten aus Privatwirtschaft und Forschung.

Hackerverbund Killnet setzt auf DDoS

Dabei warnt die Behörde insbesondere vor sogenannten „DDoS“-Angriffen. Bei diesen als „Distributed Denial of Service“-Attacken choreografieren Angreifer

koordinierte Angriffe auf Webseiten oder Onlinedienste. Indem Tausende, teilweise Zehntausende von gleichzeitigen Angriffen erfolgen, brechen Server unter der ungewohnten Last zusammen und sind nicht mehr erreichbar.

Der auf IT-Sicherheit spezialisierte Experte Manuel Atug, der auch die Bundesregierung in Sachen Kritische Infrastruktur berät, vergleicht solche Angriffe mit einer „digitalen Sitzblockade“ und hält sie für vergleichsweise harmlos. Weil der Spuk irgendwann wieder vorbei geht – und nicht zerstört, sabotiert oder gestohlen wird. Dennoch sind solche DDoS-Angriffe lästig – und können die Bevölkerung verunsichern.

Jeder sollte sich aktiv schützen

Das Tückische an solchen DDoS-Angriffen: Die Angreifer verwenden in der Regel unzählige Computer und Smartphones ahnungsloser Menschen, die irgendwann mal mit Schad-Software infiltiert wurden, um solche Angriffe durchzuführen. Die Geräte gehören dann zu einem „Botnet“, das ferngesteuert wird. Meistens bemerken die Betroffenen das nicht einmal – sie sind aber Teil einer kriminellen Aktivität.

Ein Grund mehr, dafür zu sorgen, dass die eigenen Rechner und Smartphones sicher sind – und nicht gekapert werden können. Weder für DDoS-Angriffe, noch für Spionagezwecke oder ernsthafte Angriffe wie sogenannte „Ransomware“-Attacken. Hier werden durch Ausnutzen von Sicherheitslücken Schadprogramme auf Computer und später in komplette Netzwerke aufgebracht, die alle Daten verschlüsseln und ein Lösegeld (englisch: „Ransom“, daher der Name) einfordern. Ein im höchsten Maße krimineller und bedrohlicher Vorgang.

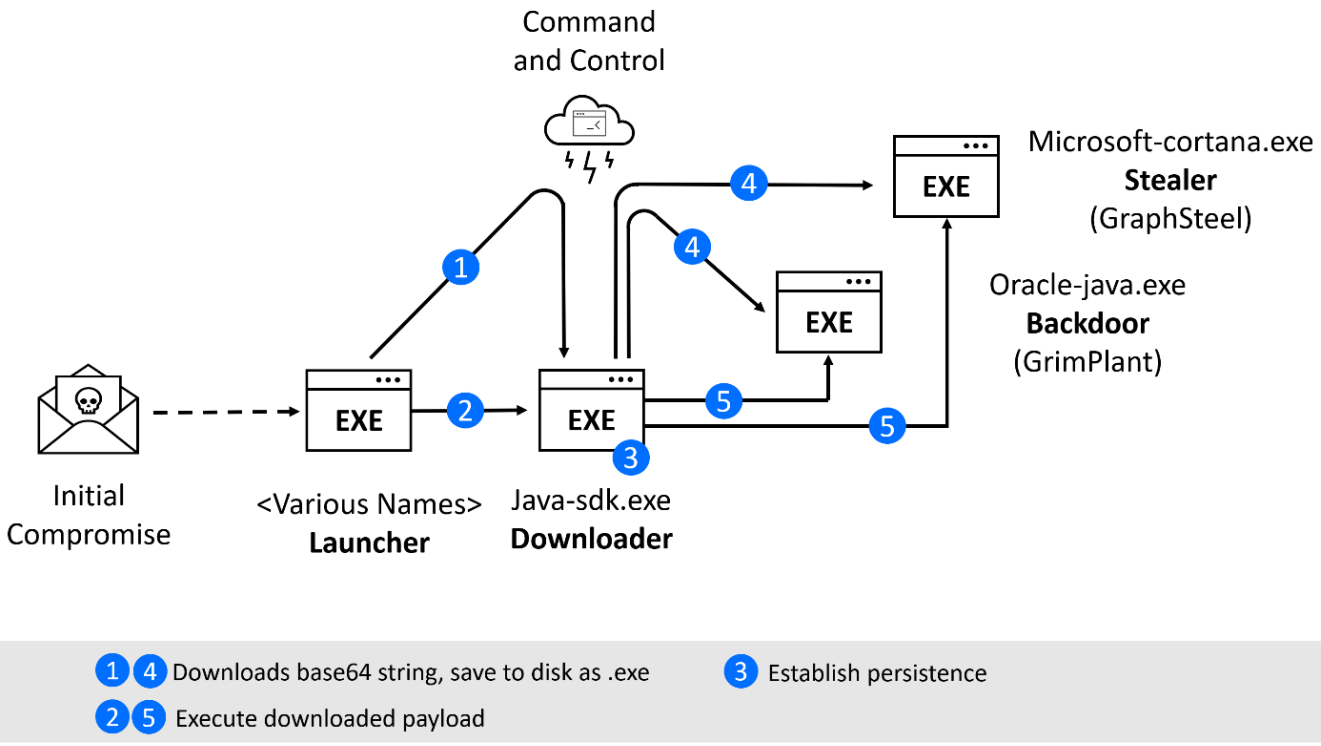
Was jeder einzelne deshalb tun kann – und sollte:

1. Immer Betriebssystem und Software aktuell halten. Alle angebotenen Updates laden und einspielen. Dadurch werden bekannte Sicherheitslecks geschlossen. Das Risiko, Opfer eines Angriffs zu werden, wird dadurch erheblich reduziert.
2. Nicht ungeprüft auf Links klicken, die per E-Mail, SMS oder Messenger-Nachricht kommen. Das Risiko, dass es sich hier um einen Phishing-Angriff handeln könnte (Abgreifen sensibler Daten), ist sehr hoch.
3. Warnhinweise des Arbeitgebers oder Providers ernst nehmen: Wenn

Hinweise auf Missbrauch gemeldet werden (etwa, weil man Teil eines Bot-Netzes sein könnte), die eigenen Geräte untersuchen (lassen).

4. Die eigenen Onlinekonten wo immer möglich durch die „**Zwei Faktor Authentifizierung**“ absichern: Dann ist neben Benutzername und Passwort noch die Eingabe einer weiteren ID erforderlich, die in der Regel im eigenen Smartphone generiert wird.

Komplexe Cyberspionage im Zuge des Ukraine-Krieges



Der Krieg in der Ukraine ist auch ein Cyberkrieg. Unternehmen in dem angegriffenen Land oder in unterstützenden Nationen mit Verbindung in die Ukraine sind von klassischen IT-Angriffsmechanismen bedroht, deren Urheber diesmal politisch motiviert sind. Zu diesen gehört neben dem Löschen von Informationen die Spionage. Die Bitdefender Labs haben die dafür verwendeten anspruchsvollen Angriffsmechanismen des sogenannten "Elephant Framework" analysiert.

Threat-Intelligence-Experten und Analysten von Managed-Detection-and-Response-Teams haben seit Ausbruch des Krieges die Cybersicherheitslage beobachtet. Unternehmen und Organisationen in der Ukraine, insbesondere im Bereich Behörden und Kritische Infrastrukturen, sind wie zu erwarten unter den bevorzugten Opfern.

Seit März 2021 betreibt etwa die pro-russische UAC-0056-Gruppe aktiv Cyberspionage. Die Gruppe – ebenfalls bekannt unter den Namen Lorec53, UNC2589, EmberBear, LorecBear, BleedingBear, SaintBear und TA471 - ist verantwortlich für Angriffe zur Datenexfiltration mit Stealer Malware wie OutSteel

oder GraphSteel.

Vor allem GraphSteel wendet ein anspruchsvolles Instrumentarium von Techniken an, um Passwörter zu erfahren oder Informationen in den weitverbreiteten Office-Formaten wie .docx oder .xlsx und anderen wichtigen Datentypen wie .ssh, .crt, .key, .ovpn, oder .json zu exfiltrieren.

GraphSteel

Die Komplexität und Professionalität solcher Angriffe belegen Angriffe mit GraphSteel, deren Urheber höchstwahrscheinlich aus dem Umfeld der UAC-0056-Gruppe stammen. Die GraphSteel-Malware ist Teil des Elephant-Frameworks, einem in der Programmiersprache Go verfassten Malware-Toolset. Die Angreifer setzten sie jüngst in einer Reihe von Phishing-Attacken auf ukrainische Regierungsbehörden (gov.ua-Ziele) ein.

Zunächst begannen sie mit einer anspruchsvollen Spearphishing-Attacke. Die Hacker legten eine hohe Expertise bei Social-Engineering-Angriffen an den Tag und nutzten gespoofte ukrainische E-Mail-Adressen. Inhalte der gefälschten Mails waren vermeintliche offizielle Bekanntmachungen oder Themen rund um Corona.

In einer Mail warnte der vermeintliche Autor vor einer Zunahme von russischen Cyberangriffen, gab Sicherheitstipps und verwies auf einen vermeintlichen Download einer Bitdefender-Software. Die Opfer kompromittierten ihre Rechner entweder durch einen Klick auf einen Link im Mailtext oder durch das Öffnen einer Excel-Tabelle mit eingebetteten Macros.

Launcher

Als Launcher verwenden die Hacker in einigen Fällen ein Python-Script, welches zu einer ausführenden Datei konvertiert worden war. In anderen Fällen verfassten sie den Code – wie im gesamten Elephant-Framework – in der Programmiersprache Go. Bei der Entscheidung spielte vielleicht eine Rolle, dass nicht jede Sicherheitssoftware eine in Go verfasste Malware erkennt.

Dies wiederum liegt wohl darin begründet, dass gut- wie böswillige Programmierer

Go nicht oft verwenden. Ein weiterer Vorteil der Sprache für die Hacker ist aber, dass der Payload sowohl für Windows wie für Linux kompiliert werden kann, ohne den Code zu ändern.

Außerdem ist er einfach anzuwenden und lässt sich um Module von Drittanbieter-Malware erweitern. Der Launcher dient dann als eine Kombination von Downloader oder Dropper und verbindet das Opfer-System mit dem Command-and-Control-Server, um die eigene Verfügbarkeit mitzuteilen und zum gegebenem Zeitpunkt einen ausführbaren Malware-Payload zu empfangen.

Downloader

Der Downloader lädt dann zwei verschiedene Malware-Dateien: GraphSteel (Microsoft-cortana.exe) und GrimPlant (Oracle-java.exe), die sich beide automatisch ausführen. GrimPlant erlaubt es, remote PowerShell-Kommandos auszuführen. GraphSteel entwendet Daten wie Zugangsdaten, Zertifikate, Passwörter oder andere sensible Informationen (siehe Abbildung 1).

GraphSteel Stealer

Hauptzweck von GraphSteel ist die Exfiltration von Dateien, welche die Malware dann verschlüsselt mit AES Cipher über Port 442 überträgt. Für die Kommunikation mit dem Command-and-Control-Server nutzt das Tool Websockets und die GraphQL-Sprache. Der Stealer entwendet Zugangsdaten für Wifi, Chrome, Firefox sowie Daten aus den Passwort-Vaults, dem Windows Credential Manager oder SSH-Sessions und Thunderbird.

Vermeintlich im Namen von Bitdefender

Laut einem Eintrag vom 11. März 2022 im CERT-UA nutzen andere Angriffe aus dem UAC-0056-Umfeld dringende Appelle, die IT-Sicherheit zu erhöhen und ein vermeintliches Bitdefender-Antivirus-Produkt von einer vermeintlichen Bitdefender.fr-Seite herunterzuladen, für ihre Angriffe aus. Hinter Bitdefender.frverbirgt sich aber die Domain forkscenter.fr mit einer gespooften Bitdefender.fr-Webseite (Abbildungen 2 und 3).

Diese Attacke installiert zunächst einen Discord-Downloader, der dann zwei ausführbare Dateien implementiert: Zum einem Alt.exe, einen bekannten Go-Launcher, der das Elephant Framework herunterlädt, zum anderen One.Exe, einen Cobalt Strike Beacon.

Am Ende wird im letzteren Fall eine cesdf.exe heruntergeladen, die leider zurzeit nicht für eine Analyse vorliegt, weil die Administratoren der angegriffenen Organisation ihren Server mittlerweile abgeschaltet haben. (Abbildung 4)

Derart komplexe Angriffe abzuwehren, erfordert eine gestaffelte Cyber-Sicherheit, die einen Angriff während mehrerer Phasen abwehren kann: Schon beim Abblocken der Phishing-Mail, beim Ausführen des Payloads oder beim Unterbinden der weiteren Kompromittierung und bei der Kommunikation mit dem C-&-C-Server.

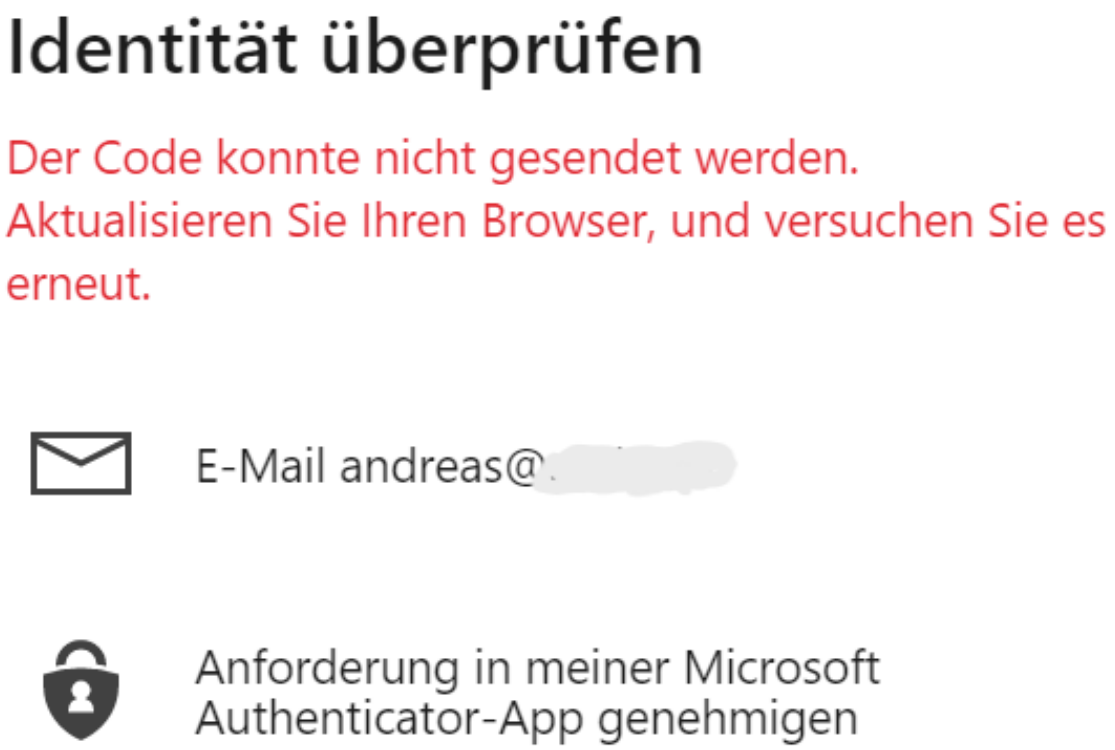
Die vollständige Analyse der oben beschriebenen Angriffe finden Sie hier: https://businessinsights.bitdefender.com/deep-dive-into-the-elephant-framework-a-new-cyber-threat-in-ukraine?utm

Fehlende Apps im Windows Store

Einige Anbieter sind hingegangen und haben ihre Apps aus dem Windows Store zurückgezogen. Im Internet findet Ihr dazu dann sogar noch Links, auch wenn die Apps nicht mehr laufen. Wie Ihr damit umgehen könnt, lest Ihr hier.

Die Windows Store-Apps waren eine gute Idee von Microsoft: Der Store sollte als zentrale Plattform für PCs, Tablets und Smartphones dienen. Von den Smartphones hat man sich mittlerweile verabschiedet, und auch die Softwareanbieter sind nicht mehr so ganz begeistert. Verschiedene Apps wie Amazons Kindle, DAZN und andere sind aus dem Store verschwunden. Meist zu Gunsten von Webseiten, die die Inhalte ebenfalls darstellen können.

Veraltete Links im Google-Suchergebnis deuten an, dass es die Apps immer noch gäbe. Klickt Ihr die dann an, dann kommt eine Fehlermeldung des Windows Store, die fälschlicherweise auf eine fehlerhafte Authentifizierung Eures Kontos schließen lässt.



In einem solchen Fall bleibt Euch nicht viel anderes übrig, als die Installation abzubrechen und Euch anders zu behelfen! Wenn es eine Webseite gibt, die die Informationen so darstellen kann, wie Ihr es braucht, dann legt aus der Webseite eine Web-App an. Diese könnt Ihr wie eine normale App benutzen, sie erscheint im Startmenü und lässt sich als Fenster bewegen.

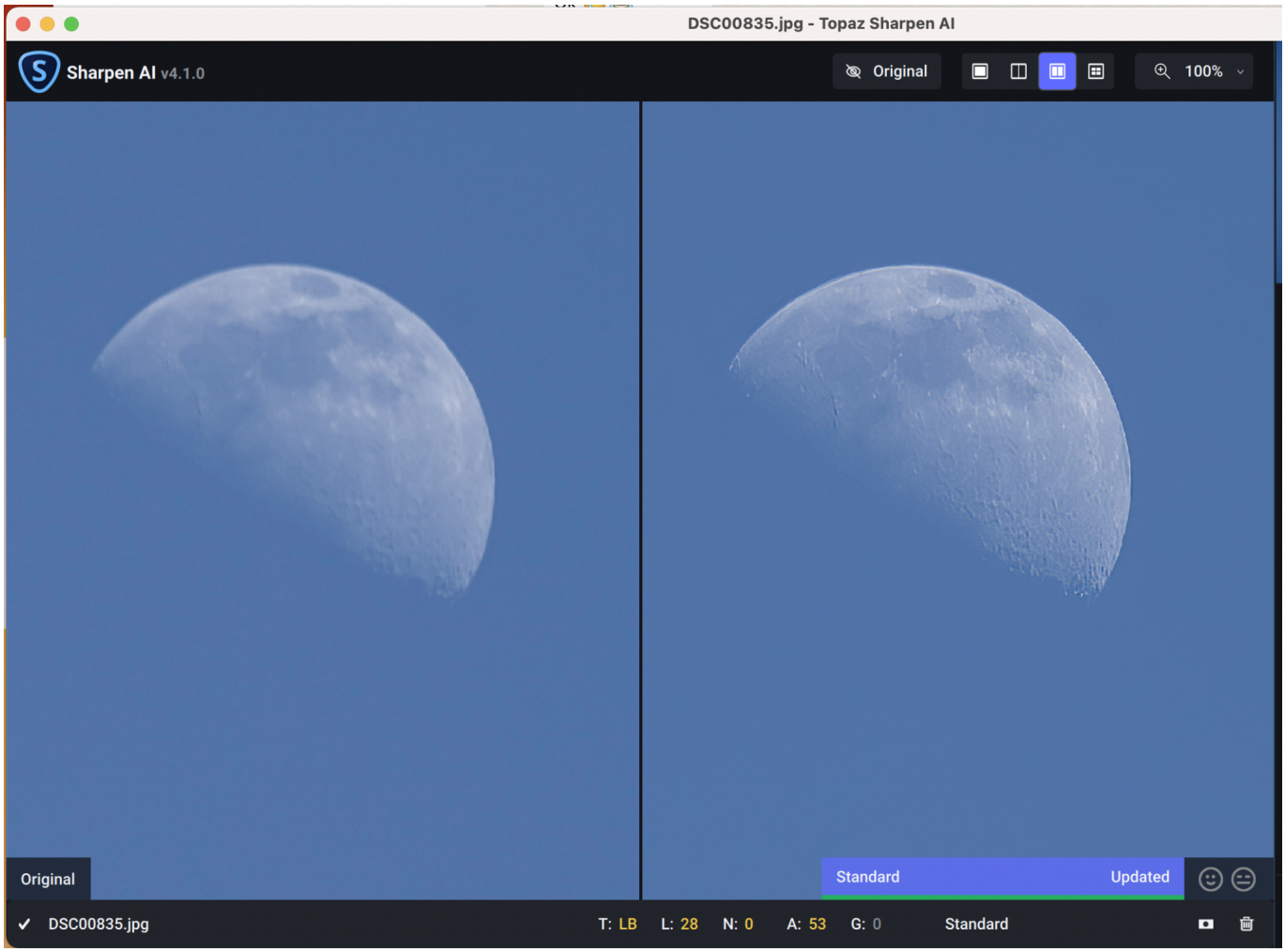
Alternativ sucht Euch eine App, die den selben Zweck erfüllt, was allerdings bei den genannten und anderen Hersteller-spezifischen Apps schwer möglich sein wird.

Bilder schärfen und verbessern mit AI: Topaz

Fotos können immer noch besser sein: Rauschen, Unschärfen zu geringe Auflösung: Das lässt sich mit den AI-Tools von Topaz Labs schnell nachbearbeiten.

Smartphone, Systemkamera oder Spiegelreflex: Die Automatikprogramme sind ausgeklügelt, aber nicht ohne Fehl und Tadel. Es ist zu dunkel, dann rauscht das Bild. Das Tele-Objektiv ist am langen Ende nicht ganz so scharf, wie es sein soll. Oder nicht so stark, dass das Motiv groß genug wird, und Ihr müsst digital heranzoomen und riskiert damit sichtbare Pixel.

Solche Mängel manuell zu beheben ist nicht leicht, denn nicht alle Änderungen werden in allen Bereichen anzuwenden sein. Idealerweise würde man einen Experten dransetzen, der mit vielen manuellen Schritten das Optimum aus dem Bild herausholt.



Diesen Ansatz verfolgen die Tools von Topaz Labs. Nur, dass der Experte nicht ein menschlicher ist, sondern eine künstliche Intelligenz (AI, Artificial Intelligence). Im Hintergrund sitzen unterschiedliche Experten, die die Algorithmen anpassen und die Software lernen lassen, was "Verbesserung" eines Bildes bedeutet. Dieser Prozess ist nie abgeschlossen.

Diese Verbesserungen kommen dann als Modelle auf die Rechner der Benutzer. Die Apps prüfen beim Start immer auf neue Modelle und laden diese dann nach. Dies gilt für die drei Bildtools:

Sharpen AI berechnet im Motiv Verbesserungen an Stellen, an denen der Fokus nicht sitzt, Bewegungsunschärfen vorhanden sind oder Verwackler entstanden sind. Im Standard wählt Sharpen AI die optimale Schärfung, der Benutzer kann aber auch manuell eingreifen und verschiedene Parameter verändern.

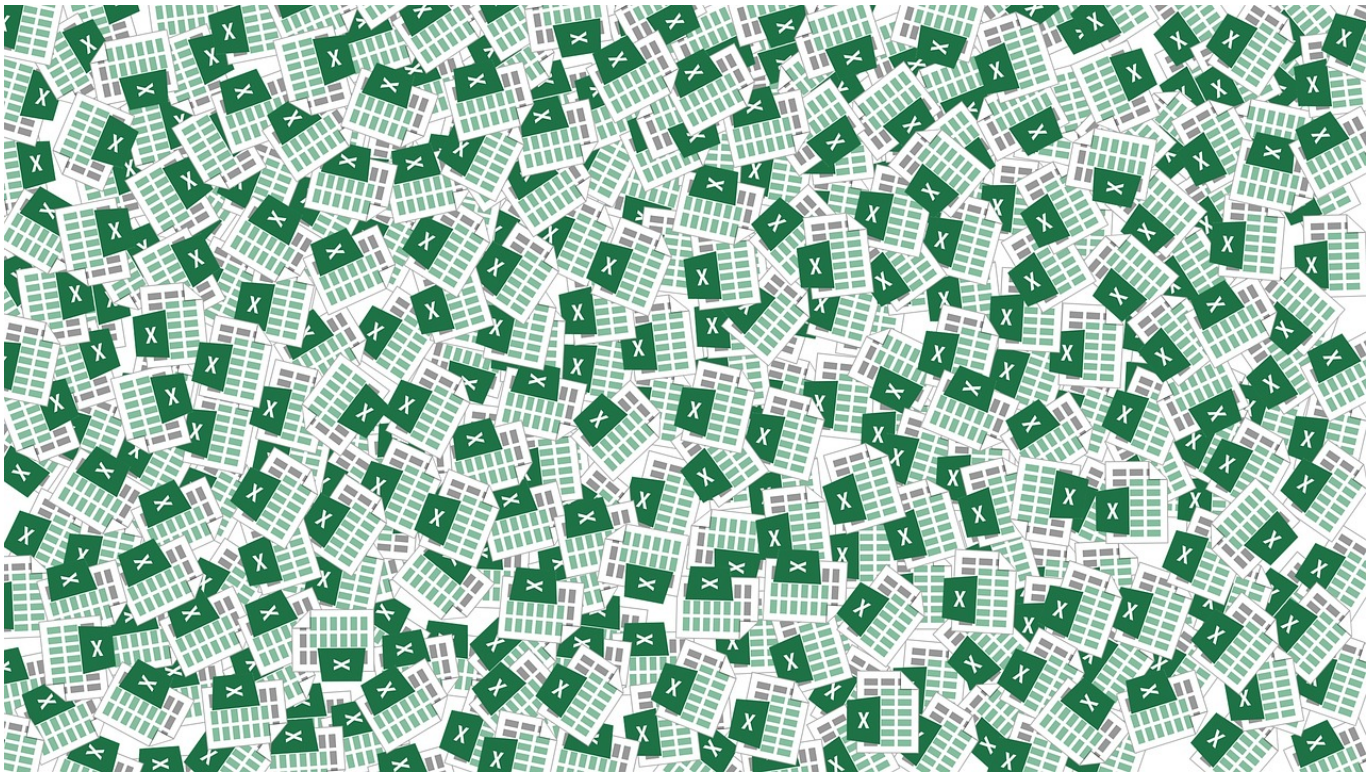
Denoise AI entfernt Rauschen aus Bildern, das sich klassischerweise durch einen Verlust von Details und nicht farbstabile Flächen äußert und entsteht oft durch

falsche ISO-Einstellungen oder schlechte Belichtungssituationen.

Gigapixel AI lässt sich am besten mit einem Begriff aus der Unterhaltungselektronik erklären: Upscaling. Aus unzähligen Einzelbildern lernen die Algorithmen, was "photorealistisch" bedeutet. Bilder werden damit so umgerechnet, als wären sie mit einer deutlich höher auflösenden Kamera aufgenommen worden. Das bringt Details zu Tage, die beim Motiv vorhanden waren, es aber nicht ins Bild geschafft haben - zumindest nicht für das menschliche Auge.

Es fällt eine einmalige Gebühr zwischen USD 79,- und USD 99,- an, alle drei Tools im Paket gibt es oft im Bundle zwischen USD 160,- und USD 199,- (regelmäßiges Nachschauen lohnt sich also!). Darin enthalten ist ein Jahr an Updateservice für die Modelle. Danach bleiben diese auf dem Stand zum Ende der Laufzeit oder müssen kostenpflichtig erneut zum Update aktiviert werden.

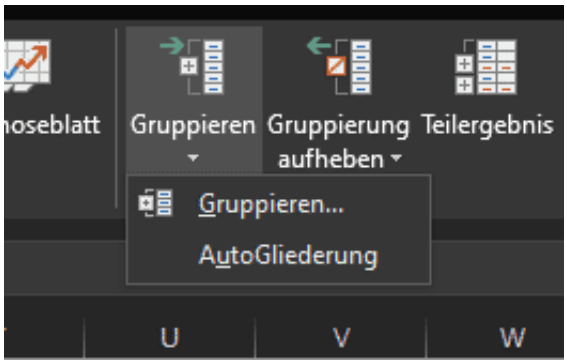
Gruppieren von Zellen in Excel



Excel ist als Tabellenkalkulation ungeschlagen: Die Möglichkeiten, Daten zu erfassen, auszuwerten und zu visualisieren, nehmen von Version zu Version zu. Die Vielzahl der Möglichkeiten bringt aber auch ein Risiko mit sich. Excel-Tabellen werden schnell zu Tapeten, die voller Zahlenreihen sind. Das ist für eine Präsentation oder die eigene Übersicht eine Herausforderung. Wir zeigen Ihnen, wie Sie hier Abhilfe schaffen!

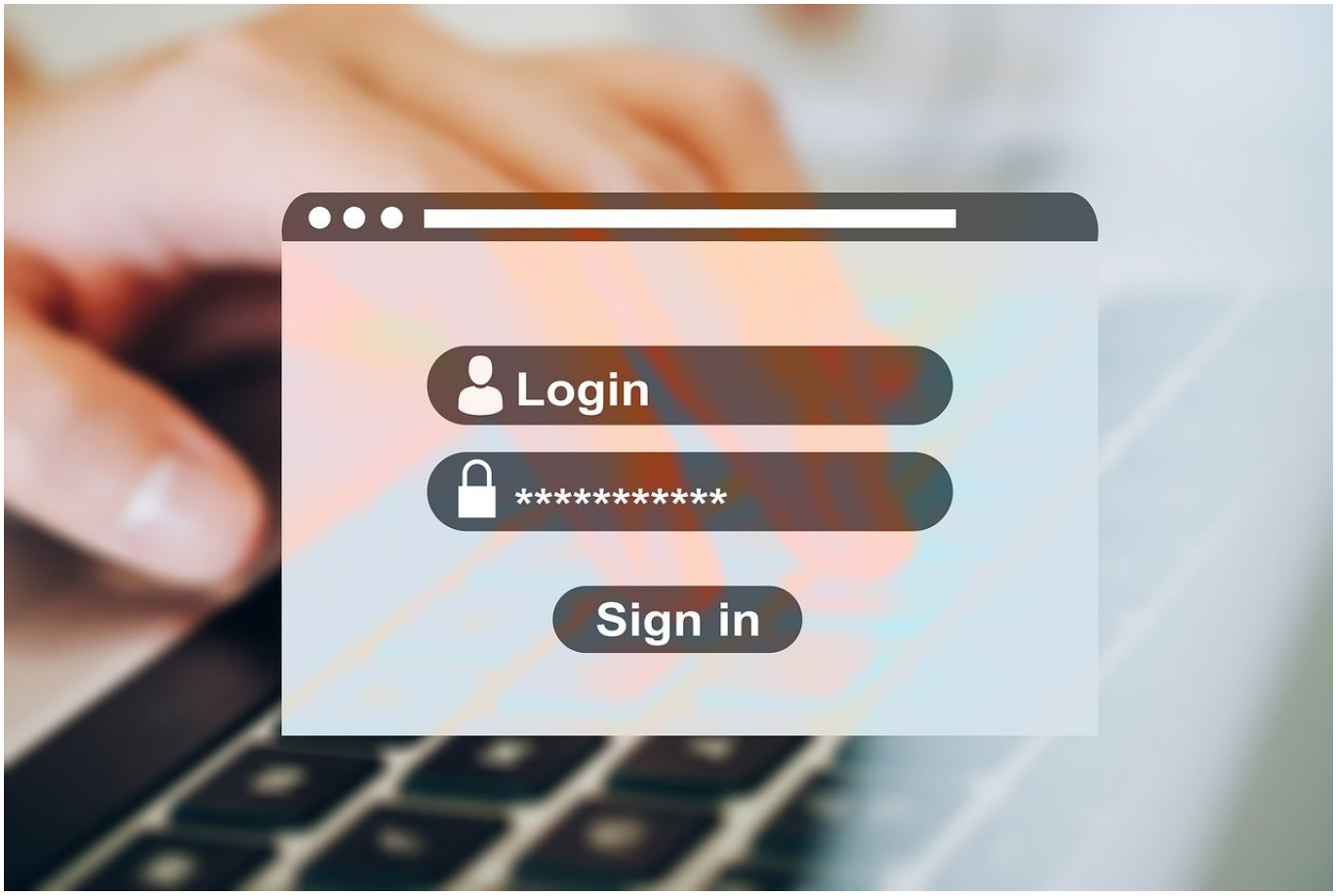
Meist lassen sich die Datenreihen in zwei Kategorien unterteilen: Die einen sind nur für die Berechnung und Auswertung wichtig, sagen dem Betrachter aber so erst mal wenig bis nichts. Die anderen tragen die Aussage der Tabelle und sollen möglichst sichtbar für den Betrachter sein. Das Löschen von Zellen ist keine Option. Entweder Sie blenden Zellen aus. Wenn die Zellen aber auf Wunsch schnell wieder verfügbar gemacht werden sollen, dann ist das Gruppieren die bessere Alternative. Das geht in wenigen Schritten:

Wenn Zeilen oder Spalten verschwinden und auch erst einmal nicht mehr zugreifbar sein sollen, dann markieren Sie diese. Klicken Sie dann auf **Gruppieren**.



Die Zeilen bzw. Spalten werden nicht mehr angezeigt, Sie finden darüber ein **Plus-Zeichen**. Wenn Sie darauf klicken, dann werden die gruppierten Zellen eingeblendet und das Symbol ändert sich auf ein **Minus-Zeichen**.

Windows 11 und die temporären Accounts

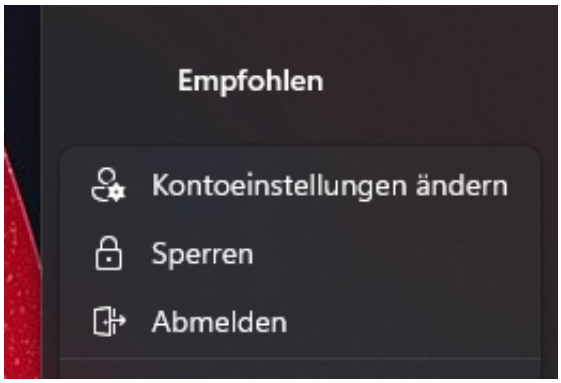


Seid Ihr plötzlich mit einem temporären Konto in Windows angemeldet? Keine Sorge, das lässt sich schnell beheben!

Viele der persönlichen Dinge in Windows 11 sind an den Benutzeraccount gekoppelt: Die Bibliotheken, Dateien, Einstellungen, Designs werden nur dann zugänglich gemacht, wenn Ihr Euch mit einem lokalen oder Microsoft-Konto anmeldet. Nun ist Windows 11 manchmal ein wenig verwirrt und meldet Euch mit einem temporären Konto an.

Besonders, wenn Ihr eine neue Version von Windows installiert oder ein größeres Update durchgeführt habt, könnt Ihr die Meldung "Sie können nicht angemeldet werden" oder "Sie sind mit einem temporären Konto angemeldet erhalten.

Der erste Schritt, der sich empfiehlt, ist der Neustart des PCs. Danach bekommt Ihr in den meisten Fällen den normalen Anmeldebildschirm angezeigt und könnt Euch mit dem Konto neu anmelden.



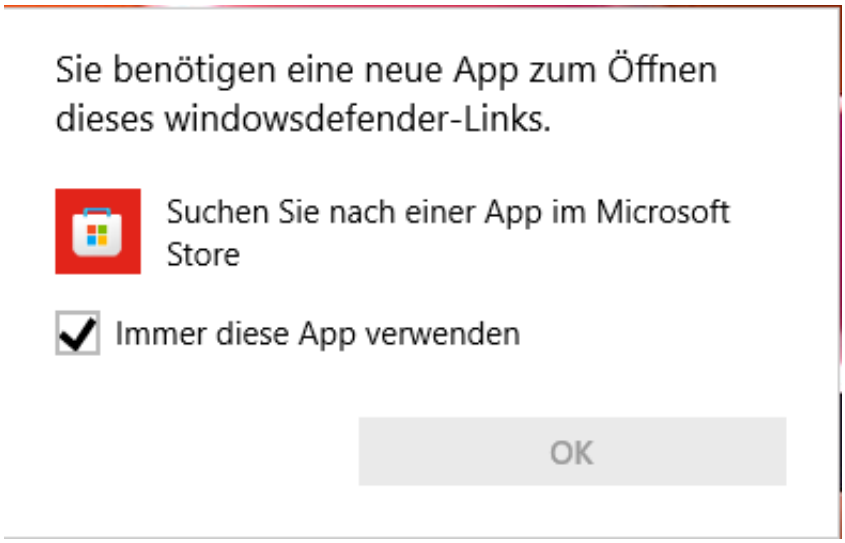
Ist das nicht der Fall, dann klickt auf **Start** > **Kontobild** > **Abmelden**. Windows 11 meldet Euch dann ab und bringt Euch auf den Anmeldebildschirm. Hier solltet Ihr dann wieder die Möglichkeit haben, Euch mit dem richtigen Konto anzumelden.

Wenn Ihr in einer solchen temporären Sitzung Daten eingegeben haben, dann sichert diese am Besten extern: Schließt einen USB-Stick oder eine USB-Festplatte an und sichert Datei durch Klick auf **Datei** > **Speichern unter**. Gebt dann als Ziel das externe Laufwerk an. Wenn Ihr dann wieder mit dem normalen Konto angemeldet seid, können Ihr die Dateien einfach wieder auf die Festplatte in Eure Bibliotheken herüberkopieren.

Fehler bei Windows 10-Sicherheitseinstellungen lösen

Beim Öffnen einer der Sicherheitseinstellungen von Windows 10 kommt die Fehlermeldung "Sie benötigen eine neue App zum Öffnen dieses windowsdefender-Links"? Wir zeigen Euch, wie Ihr den Fehler behebt!

Windows kann manchmal komisch sein. Vor allem dann, wenn eine Standardaktion statt mit der Ausführung des Befehl mit einer abstrusen Fehlermeldung beantwortet wird. So bei Windows 10 aktuell immer wieder beim Umgang mit Sicherheitseinstellungen des Windows Defender. Ob Ihr im Benachrichtigungsbereich eine Warnung habt und darauf klickt oder über **Einstellungen** > **Datenschutz und Sicherheit** > **Windows Sicherheit** eine Einstellung ändern wollt, die Fehlermeldung bleibt die gleiche.



Sie weist darauf hin, dass der Windows Defender zwar installiert ist, Windows aber keine Befehle an ihn weitergeben kann. Das ist kein Hinweis auf einen Virebefall, sondern schlicht und einfach ein Bug. Den könnt Ihr im Handumdrehen beheben:

1. Klickt auf die Lupe unten in der Taskleiste, dann gebt **powershell** ein.
2. Klickt rechts auf **Als Administrator ausführen**.
3. Gebt an der Eingabeaufforderung den Befehl *Add-AppxPackage -Register -DisableDevelopmentMode "C:\Windows\SystemApps\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy\AppXManifest.xml"*

Macht Euch nicht die Mühe, den Befehl abzutippen, sondern markiert ihn und kopiert ihn in die Zwischenablage. An der Eingabeaufforderung der Powershell könnt Ihr sie dann wieder einfügen und durch Drücken der Eingabetaste ausführen.

Nach dem Abschluss der Installation ist keine weitere Aktion nötig: Die Links zu den Windows Defender-Funktionen funktionieren sofort wieder.