Schieb Report

Ausgabe 2018.50

Trojaner Emotet verwüstet IT-Infrastruktur

Der Maschinenhersteller Krauss-Maffei meldete diese Woche einen Trojaner-Angriff. Fertigung und Herstellung wurden lahmgelegt, das Unternehmen erpresst. Kein Einzelfall. In immer mehr Institutionen und Unternehmen dringen Trojaner ein, die Schaden verursachen. Teilweise gehen die Schäden in die Millionen. Weil die Trojaner immer ausgefeilter werden. Besonders aggressiv ist derzeit ein Trojaner namens Emotet.

Trojaner kennen wir: Das sind Schadprogramme, die den Weg in unsere Rechner oder Mobilgeräte finden, sich dort verstecken und Daten ausspionieren oder Zugänge blockieren.

Doch Emotet ist mehr als nur ein Trojaner, sondern ein ausgefeiltes Betrugskonzept. Die Betrüger spionieren ihre Opfer erst aus, bevor sie sie mit Mails belästigen, um so Zugang in die Rechner und Netzwerke zu gelangen. Emotet ist deshalb so erfolgreich und gefährlich, weil die Phishing-Mails, die verschickt werden, täuschend echt aussehen.

Sie werden scheinbar von Kollegen, Freunden, Bekannten, Geschäftskollegen verschickt und haben Inhalte, die durchaus zur üblichen Kommunikation passen. Im Anhang befindet sich dann ein Word-Dokument. Wer das öffnet und das enthaltene Makro aktiviert, der lässt den Trojaner dann rein in den eigenen Rechner.

Unternehmen sind bevorzugte Ziele

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und einige Landeskriminalämter

(LKAs) melden Dutzende von Fällen, wo Emotet erfolgreich war. Vor allem in Unternehmen. Denn Unternehmen sind das beliebteste Ziel des Trojaners.

Dass die Leute das Word-Dokument öffnen, kann man verstehen, denn die Mails kommen ja scheinbar von Kollegen oder Bekannten – und enthalten einen Text, der Sinn ergibt, der sich auf eine Kommunikation davor bezieht. Da gehen bei niemandem die Alarmglocken an. Emotet ist halt sehr geschickt programmiert.

Mehrstufiger Angriff

Emotet beobachtet in einer ersten Phase das Netzwerk des Unternehmens. Wer schreibt wem, wer kommuniziert mit Leuten von außen – und worum geht es dabei? Eine Angriffsmethode, die Experten APT nennen – Advanced Persistent Thread. Wörtlich: Fortgeschrittene, dauerhafte Bedrohung.

Weil die Cyberbetrüger nicht mal eben an der Tür rütteln und schauen, ob sie versehentlich offen steht und dann reingehen. Stattdessen ist der Angriff gut geplant und in einzelne Schritte und Stadien unterteilt. Erst Ziel auswählen, dann Analyse der Infrastruktur, Nutzer ausspionieren, weiteren Angriff starten – und dann, wenn man im Netzwerk drin ist, richtig loslegen. Daten klauen. Erpressen. Das volle Programm.

Mehrstufiger Angriff

Alles Methoden, die auch bei Angriffen auf Regierungsnetzwerke wie dem Deutschen Bundestag angewendet werden. Das Gefährliche an Emotet ist, dass viele dieser aufwändigen Prozesse automatisiert wurden.

Die Algorithmen analysieren selbst, welche Schwachstellen es gibt, versuchen in die Netzwerke einzudringen, analysieren die Struktur und ermitteln die Personen, die im Netzwerk aktiv sind – und verschicken am Ende Phishing-Mails, um zum finalen Schlag zu kommen.

Das macht Emotet so gefährlich: Es werden hoch-anspruchsvolle Techniken eingesetzt, um Schaden anzurichten, und diese werden automatisiert. Ich mag mir das für die Zukunft gar nicht ausmalen, wenn die Cyberbetrüger KI einsetzen, um noch effektiver zu werden. Es drohen erhebliche Wellen von Cybercrime.

https://vimeo.com/304795972

So geht Emotet vor

Es liegt in der Natur des Trojaners, dass nahezu alles möglich ist, wenn es der Trojaner erst mal erfolgreich in ein Netzwerk geschafft hat. Der Trojaner kann zum Beispiel sensible Daten abgreifen, etwa Zugangsdaten oder vertrauliche Informationen.

Emotet könnte aber auch Produktionsprozesse stören oder lahmlegen. Das wiederum eignet sich dazu, die Opfer zu erpressen: Entweder ihr zahlt, oder wir legen alles lahm. Man kann diese Art der Bedrohung gar nicht ernst genug nehmen. Es ist Zeit, sich Gedanken darüber zu machen, wie sich derartiges besser und effektiver abwehren lässt.

Dynamite Phishing

In Fachkreisen werden die Methoden von Emotet als „Dynamite-Phishing“ bezeichnet, also sozusagen als Angeln mit Dynamit.

Wir kennen den Begriff „Phishing“: Wir bekommen eine E-Mail, die aussieht, als wäre sie von einer Bank, einem Zahlungsdienst, einem Onlineshop – doch in Wahrheit ist sie gefälscht. Wir werden ermuntert, unsere echten Zugangsdaten auf einer gefälschten Seite einzugeben.

Landen die Daten erst mal in den Händen der Kriminellen, werden sie auch missbraucht. Das ist Phishing. Angeln. Bei der neue Trojaner Emotet aber äußerst aggressiv vorgeht, unzählige

Versuche gleichzeitig unternimmt, wird von „Dynamite Phishing“ gesprochen. Also eine äußerst brutale Methode, alles andere als feinsinnig.

Aber trotzdem erfolgreich. Das gibt es auch im echten Leben: Da wird explosives Dynamit ins Wasser geworfen – und am Ende schwimmen ein paar tote Fische an der Wasseroberfläche. Dieselbe Methode, mehr oder weniger, wendet auch Emotet an. Deshalb der Begriff „Dynamite Phishing“.

Problematische Bewertungen: Warum wir ihnen nicht trauen können

Geben wir es zu: In den Wochen vor Weihnachten kaufen wir mehr ein als sonst. Geschenke. Und weil die Zeit knapp wird, das ein oder andere auch natürlich in Onlineshops. Bei Amazon und Co. Aber taugt das was, was wir da sehen? Rezensionen lesen macht schlau, oder? Ja. Und Nein. Denn auch Rezensionen sind nicht immer ehrlich, sondern gerne auch schon mal gefakt.

Viele schauen sich regelmäßig Bewertungen in Onlineshops an, bevor sie etwas kaufen. Sie fühlen sich gut informiert, weil man sieht, welche Erfahrungen andere gemacht haben. Das ist für die meisten das wichtigste Argument, Rezensionen in Onlineshops zu studieren.

Ich kann das verstehen, ich mache das auch – misstraue aber den Rezensionen weitgehend.

Denn im Grunde haben sie nur eine Funktion: Verkaufsförderung. Das wissen die Onlineshops und Portale, aber auch die Hersteller und sorgen für reichlich gute Bewertungen. Viele Bewertungen – nicht alle! – sind gefakt. Also es wird dafür bezahlt, dass sie geschrieben und eingestellt werden. Es gibt also guten Grund, den Besprechungen in den Onlineshops zu misstrauen.

Gefakte Rezensionen? Ganz einfach zu bekommen

Es ist total einfach, gite Rezensionen für eigene Produkte zu bekommen: Man beauftragt eine Agentur. Und selbst das ist nicht schwierig: Einfach „Amazon Bewertungen“ bei Google eingeben, schon erscheinen Anzeigen von Agenturen, die solche Manipulationen anbieten.

Und das funktioniert so: Man bezahlt die Agenturen dafür, dass sie Bewertungen schreiben, bei Amazon, Facebook, Google, aber auch in App-Stores und Co.

Die Agenturen verfassen Texte, manuell, gut lesbar, und stellen sie dort ein, wo der Auftraggeber sie haben will. Es ist also kein Problem, gute Rezensionen zu bekommen – es ist nur eine Frage der Investition. Einzelne manipulierte Besprechungen gibt es ab 15 EUR.

Die Agenturen sind mit allen Wassern gewaschen. Sie wissen, dass „verifizierte Käufe“ besser wirken, also kaufen sie auf Wunsch sogar die Produkte, damit sie im Onlineshop gut dastehen. Die Leser der Rezensionen glauben, sie würden eine ehrliche Bewertung lesen – tun sie aber nicht.

Sales Boost: Noch mehr Tricksereien

Keineswegs die einzige Art die Manipulation. Die Algorithmen von Amazon und Co. begünstigen Produkte, die sich gut verkaufen, sie erscheinen bei Suchanfragen weiter oben. Deshalb bieten manche Agenturen auch sogenannte „Sale Boosts“ an. Sie sorgen dafür, dass das Produkt des Kunden besser gekauft wird. Etwa, indem Gutscheine erzeugt werden, die derart hoch sind, dass ein Produkt zwar viel gekauft wird, der Hersteller daran aber gar nichts verdient.

Im Gegenteil: Er zahlt für den „Sale Boost“ eine saftige Gebühr. Doch die Verkaufsstatistik zeigt nach oben, durch die Fake-Käufe, das lockt dann irgendwann echte Käufer an. Sie sehen gute Bewertungen und gute Verkaufszahlen – Amazon zB zeigt ja auch das Ranking an – und schlagen zu. Schon hat die Verkaufsfalle wieder zugeschnappt.

Was unternehmen die Onlineshops dagegen?

Die ganz kleinen Onlineshops gar nichts, den Aufwand können sie gar nicht betreiben. Die großen haben – angeblich! – Algorithmen entwickelt, um Betrüger zu erkennen. Man kann ja sehen, wenn ein Rechner, eine IP-Adresse besonders oft oder häufig Rezensionen schreibt.

Das lässt vermuten, dass jemand für Besprechungen bezahlt wird. Heute eine Waschmaschine und einen Werkzeuggürtel bewerten, morgen ein Rosenöl und eine Handyhülle? Eher unwahrscheinlich. Auch überprüfen manche Anbieter wie Amazon, ob der Rezensent das Produkt überhaupt gekauft hat. Nur wenn ja, steht „verifizierter Käufer“ daneben. Aber das ist auch keine Garantie, dass eine Bewertung wirklich ehrlich ist.

Worauf kann man sich verlassen?

Natürlich sind unabhängige Tests wie bei der Stiftung Warentest Gold wert. Und natürlich sind auch in den Onlineportalen geschriebene Rezensionen keineswegs alle gefälscht. Aber doch recht viele. Man ist gut beraten, einzelnen Rezensionen nicht zu trauen.

Weder zu guten, noch zu schlechten. Denn es gibt auch Unternehmen, die versuchen die Produkte oder Angebote der Konkurrenz runterschreiben zu lassen. Das einzige, was man machen kann, wenn man die Rezensionen von Produkten in großen Onlineshops selbst liest:

Drüber fliegen und eine Tendenz feststellen. Die durchschnittliche Bewertung ist interessant. Aber nicht bei insgesamt drei Rezensionen, sondern wenn es mehrere Dutzend oder sogar mehrere Hundert Rezensionen sind. So viele lassen sich dann doch nicht fälschen.

Sinnvoll oder nicht?

Ich halte nicht viel von Bewertungen in Onlineshops. Sie sind Manipulationswerkzeuge. Sie sollen zum Kauf anregen, nicht informieren. Würden sie den Verkauf verhindern, würden sie Amazon und Co. nicht anbieten. Sie verleiten uns zum Kauf. Wenn ich ein Produkt kaufe bei Amazon, bekomme ich oft eine Mail:

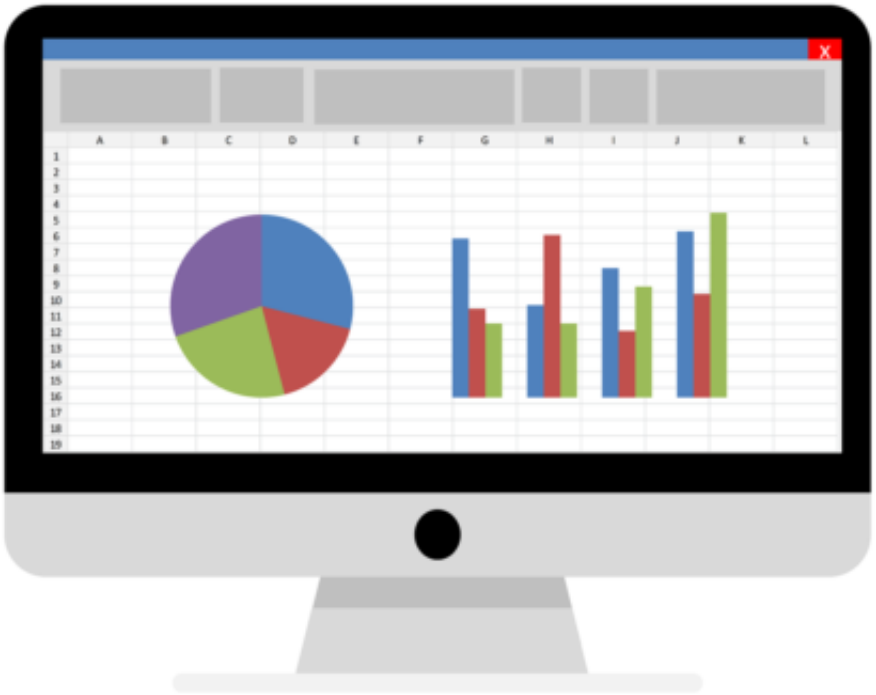
Wollen Sie das Produkt nicht besprechen? Klar, ich mache mir die Arbeit – und Amazon profitiert. Weil andere Kunden dann womöglich noch mehr kaufen. Es ist eine Pervertierung des Systems. Abgesehen davon werden die Urteile von Nichtfachleuten sowieso überschätzt: Da kommt viel Meinung und Gefühl ins Spiel. Es wird nicht objektiv und nach immer gleichen Maßstäben beurteilt. Das kann nicht wirklich fair und nützlich sein. Das ist also ein Trick. Darauf sollten wir nicht reinfallen.

4 Möglichkeiten, eine beschädigte Excel-Datei wiederherzustellen

Was kann ich tun, wenn sich eine Microsoft-Excel-Datei mit wichtigen Daten nicht mehr öffnen lässt? Ist es irgendwie möglich, in einem solchen Fall doch noch an die wichtigen Daten zu kommen, die plötzlich nicht mehr zugänglich sind? Die gute Nachricht: Ja, es gibt durchaus einige Möglichkeiten - und Rettungsanker.

Nützliche Tipps zur Verwendung von Microsoft Excel

Wenn sich eine Excel-Arbeitsdatei mit wichtigen Daten plötzlich nicht mehr öffnen lässt: Wie groß ist die Wahrscheinlichkeit einer erfolgreichen Wiederherstellung dieser Daten und was müssen Sie dafür tun?



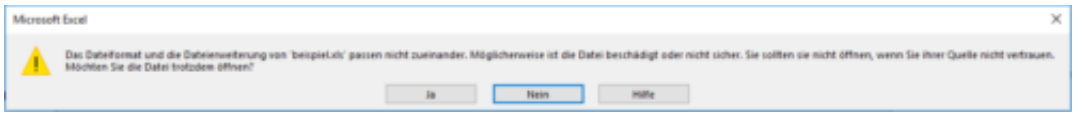
Leider passiert es vergleichsweise häufig, dass Microsoft Excel Daten verliert. Es gibt verschiedene Lösungsansätze. Erst nachdem Sie alle Optionen ausprobiert haben, können Sie feststellen, ob es möglich ist, eine beschädigte Excel-Datei wiederherzustellen.

Möglichkeiten der Wiederherstellung einer beschädigten Excel-Datei:

1. Integrierte Microsoft Excel-Funktion verwenden
2. Datei mit OpenOffice öffnen
3. Einen Online-Dienst nutzen

4. Mit einem Drittanbieter-Tool wiederherstellen

Da sollte doch auch eine Methode dabei sein, die in Ihrem Fall hilft.

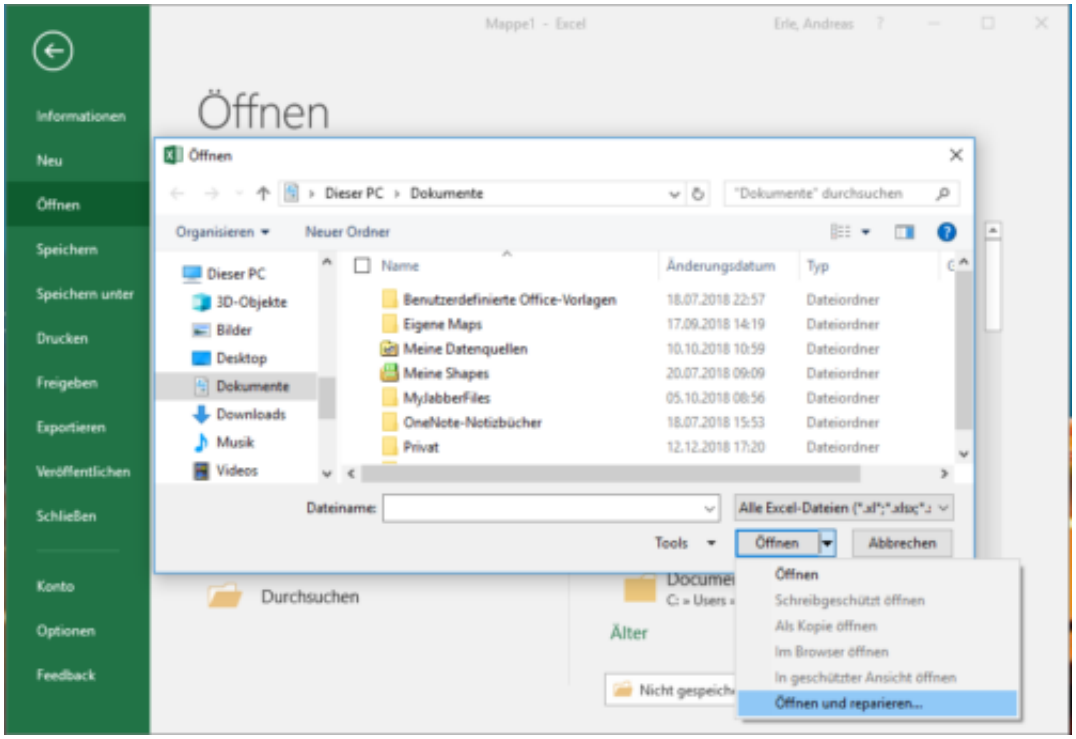


1. Integrierte Microsoft Excel-Funktion

In den neuesten Versionen von Microsoft Excel wurde die Möglichkeit hinzugefügt, eine Datei wiederherzustellen. In älteren Versionen war diese Funktion entweder gar nicht vorhanden oder hat nur eher bescheiden funktioniert. Mittlerweile hilft diese Funktion bei beschädigten Dateien immerhin in 10-20% der Fälle.

1. Wählen Sie den Menüpunkt **Datei**
2. Wählen Sie **Öffnen**
3. Wählen Sie die beschädigte Datei auf der Festplatte aus
4. Klicken Sie auf den Pfeil neben der Schaltfläche **Öffnen** in der rechten unteren Ecke
5. Wählen Sie den Punkt **Öffnen und Wiederherstellen** im Dropdown-Menü

Das alles ist ganz einfach und erfordert keine speziellen Kenntnisse. Für viele Benutzer ist diese Funktion völlig ausreichend, um eine beschädigte Excel-Datei erfolgreich wiederherzustellen. Wenn diese Methode die Datei nicht wiederherstellen konnte, kann OpenOffice.org helfen.



2. Datei mit OpenOffice öffnen

Microsoft Office-Dateien ab Office 2007 haben ein gemeinsames Format mit OpenOffice. Sie können also das Softwarepaket von OpenOffice.org herunterladen, installieren und versuchen, die Datei mit diesem Softwarepaket wiederherzustellen.

Achtung: Die Datei, die mit OpenOffice wiederhergestellt wird, muss die Erweiterung XLSX haben – das ist die Version für Excel 2007-Dateien und höher.

3. Einen Online-Dienst nutzen

Wenn die Optionen 1 und 2 nicht geholfen haben, die Datei wiederherzustellen, sind spezielle Dienste oder Programme nötig, die extra für die Wiederherstellung von Daten aus beschädigten Excel-Dateien entwickelt wurden.

Es gibt mehrere verfügbare Online-Dienste zum Wiederherstellen beschädigter Excel-Dateien. Der bequemste und günstigste (nur 5$ pro Datei) ist hier verfügbar:

https://onlinefilerepair.com/de/excel-repair-online.html

Laden Sie die Datei einfach beim Dienst hoch und warten Sie auf das Ergebnis. Laut Statistik der Entwickler dieses Dienstes können in 40% der Fälle die Daten aus der beschädigten Excel-Datei in der einen oder anderen Form wiederhergestellt werden.

Der Dienst ist praktisch, da er auf allen Betriebssystemen (Windows, MacOS, iOS, Android usw.) und auf allen Geräten (Computer, Tablet, Telefon usw.) funktioniert.

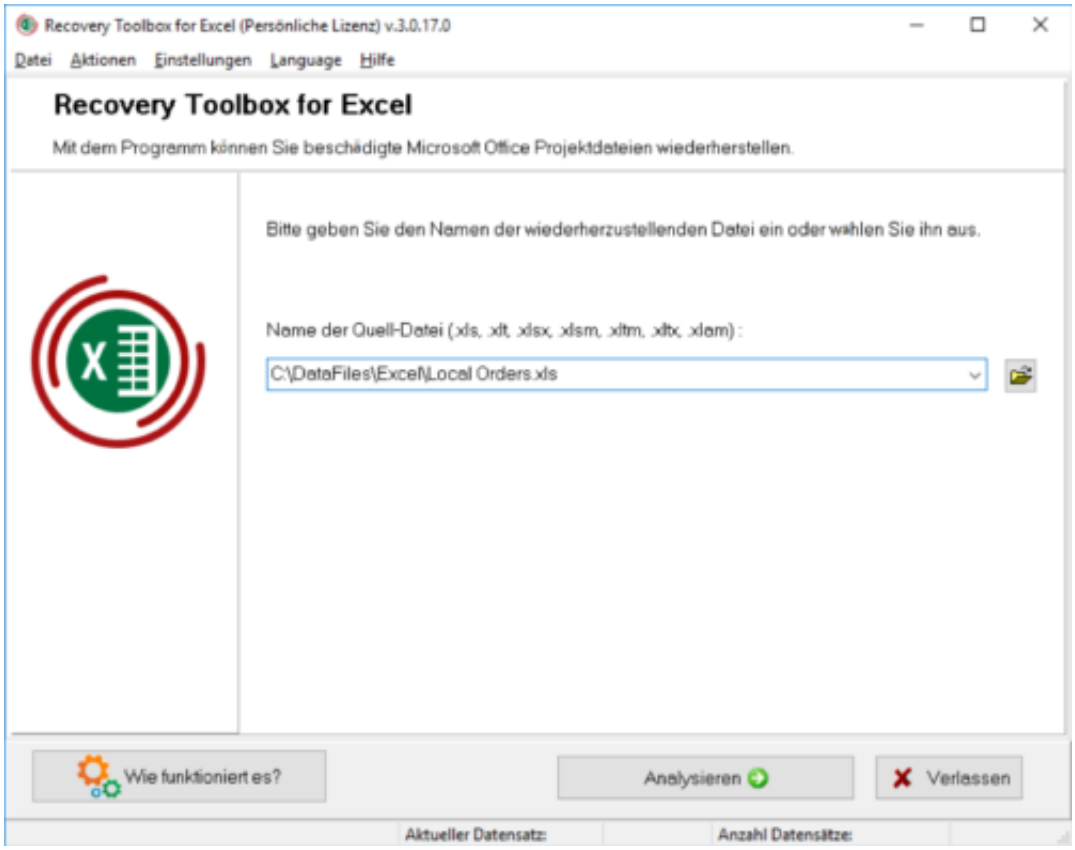
4. Mit einem Drittanbieter-Tool wiederherstellen

Wenn Sie viele beschädigte Excel-Dateien haben oder diese Dateien aufgrund ihrer Vertraulichkeit nicht an Dritte übertragen können, verwenden Sie spezielle Tools von Drittanbietern (nicht von Microsoft).

Ein Beispiel für ein solches Tool ist **Recovery Toolbox for Excel**:
https://excel.recoverytoolbox.com/de/

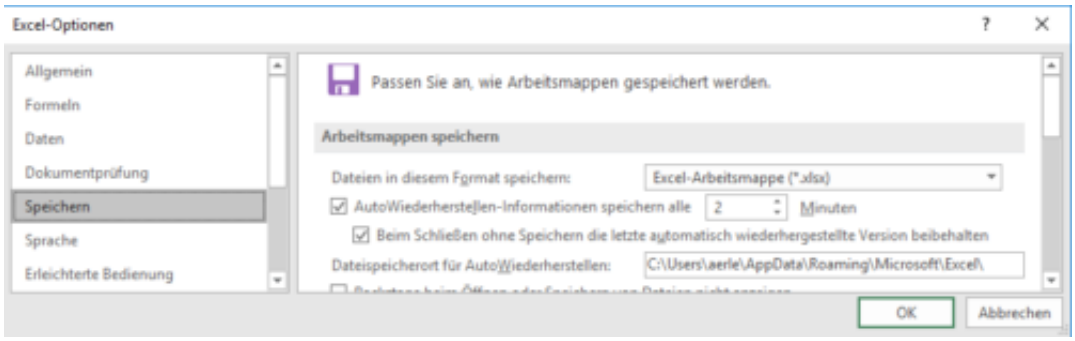
Das Tool wird seit Anfang der 2000er Jahre entwickelt und vertrieben, verfügt über eine mehrsprachige Benutzeroberfläche (einschließlich Deutsch) und stellt alle Arten von Excel-Dateien aller Versionen wieder her, beginnend mit dem heute wenig verbreiteten Excel 97.

Achtung: Das Tool funktioniert nur auf Computern mit Windows.



Nützliche Tipps zur Verwendung von Microsoft Excel

Aktivieren Sie die automatische Speicherfunktion, wenn Sie mit Microsoft Excel arbeiten. Damit vermeiden Sie Fälle, bei denen eine Fehlfunktion des Computers zum Verlust von mehreren Arbeitsstunden führt:



Office für Mac: Abo-Details herausfinden

Wie bei der Windows-Version gibt es auch die Mac-Version der Büro-Programme im Abomodell. Das Ganze nennt sich Office 365 – und wird, wie bei Windows, sowohl für private Nutzer als auch für geschäftliche Anwender unterstützt. Mit welchem Benutzerkonto die aktuelle Office-Installation aktiviert wurde, lässt sich auch am Mac mit wenigen Klicks ermitteln.

Details zum Abo erscheinen in der macOS-Version von Word, Excel und Co. allerdings nicht auf einer separaten Seite, sondern direkt bei den Infos zur genutzten Software-Version. Die lassen Sie sich mit folgenden Schritten anzeigen:

1. Zunächst starten Sie eines der Office-Programme für den Mac, etwa Word oder auch Excel. Am einfachsten geht das über das Launchpad, das sich per Klick auf das Raketen-Symbol im Dock am unteren Rand des Bildschirms aufrufen lässt.
2. Sobald das Fenster der Office-Anwendung zu sehen ist, klicken Sie oben im Menü auf den Namen des Programms, im Beispiel
3. Dann auf den obersten Eintrag klicken, **Info Microsoft Word**.
4. Neben der genauen Angabe der installierten Office-Version finden Sie hier auch die eMail-Adresse der Person, mit deren Microsoft- oder Office-365-Konto die Software auf diesem Mac aktiviert wurde.

Diese Information kann wichtig sein, wenn Sie herausfinden möchten, auf welchen Geräten Ihre Office-Abo-Lizenz bereits aktiviert ist – denn insgesamt können nur jeweils 5 Geräte mit einer einzelnen Lizenz freigeschaltet werden.

Bezahlen mit Apple Pay

In den USA gibt es Apple Pay bereits seit Oktober 2014. Auch in Frankreich und Großbritannien ist Apple Pay bereits seit einer Weile verfügbar. Nur in Deutschland nicht - die Banken und Sparkassen wollten lieber eine eigene Lösung auf den Weg bringen. Doch jetzt ist Apple Pay auch bei uns gestartet. Das Bezahlen per Smartwatch kann also losgehen.

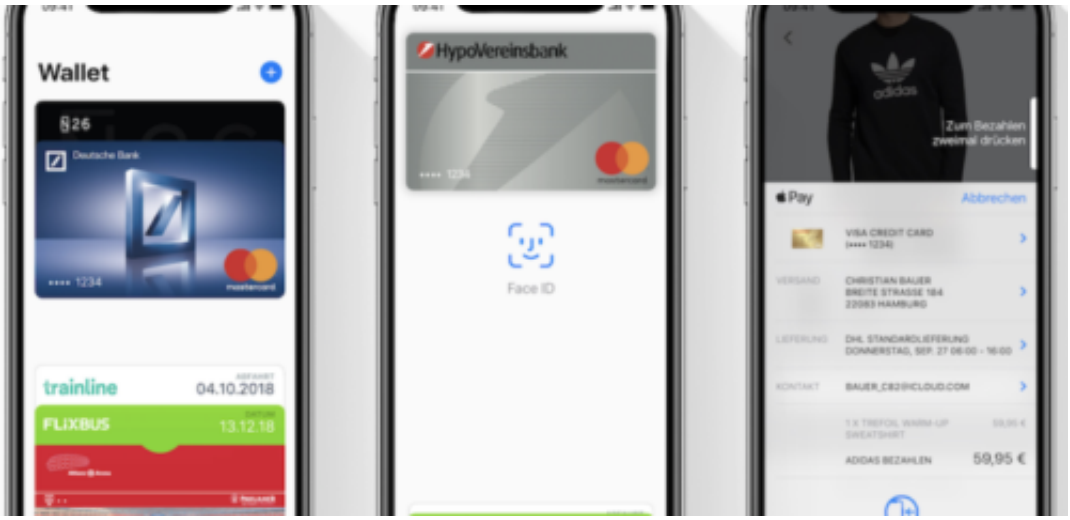
Ein Freund von mir, Dirk, hat im gemeinsamen Spanien-Urlaub beim Bezahlen an der Kasse immer wieder einen Knicks gemacht - was lustig aussieht, bei einem Kerl seiner Statur. Doch mit der aller größten Freude hat er Restaurantrechnungen und einzelne Getränkeflaschen am Strand durch Hinhalten seiner Apple Watch bezahlt.

Dirk war mächtig stolz: Er hat sich extra eine Debit-Karte bei einer schottischen Bank besorgt, um seine Apple-Uhr mit der Pay-Funktion auszurüsten. Bezahlen ohne Bargeld oder Kreditkarte, sondern mit der Watch. In Deutschland ging das im Sommer noch nicht.

Viele Bank- und Kreditkarten funktionieren

Seit heute (11.12.2018) kann man nun auch in Deutschland mit Apple Pay bezahlen. Zwei Jahre nach dem offiziellen Start in den USA. Apple ist dazu Kooperationen mit einigen Geldinstituten und allen großen Kreditkartenfirmen eingegangen.

Bezahlen kann man mit Apple Pay praktisch überall, wo man kontaktlos bezahlen kann. Wo man also keine Karte ins Lesegerät stecken muss, sondern das Hinhalten der Kreditkarte reicht.



Doch es machen längst nicht alle Geldinstitute mit. Die Sparkassen zum Beispiel sind nicht mit an Bord. Sie haben seit Sommer eine eigene App zum mobilen Bezahlen am Start, die allerdings nicht sehr erfolgreich ist. Was unter anderem daran liegt, dass nicht alle Sparkassen mitmachen - und es auch nur mit Android-Handys funktioniert.

Denn Apple erlaubt anderen Anbietern nicht, den NFC-Funk-Chip im iPhone für Bezahl-Apps zu nutzen. So behindern mal die einen, mal die anderen die Entwicklung.

https://vimeo.com/305738363

Bequem ja - aber auch unbedenklich?

Apple ist wahrlich nicht der erste Anbieter von Mobile Payment in Deutschland. Bereits vor einigen Monaten ist Google Pay in Deutschland gestartet. Kurz danach die Sparkassen. Doch Apple hat am meisten Banken an Bord. Das macht Apple Pay meiner Ansicht nach interessanter für alle, die bargeldlos mit Smartphone oder Smartwatch zahlen wollen.

Weil beim Zahlvorgang sogenannte "Token" verwendet werden (bei Google Pay ebenso), bleiben die eigenen Daten geheim. Der Händler erfährt nicht, wer bezahlt hat. Man bezahlt also fast so anonym wie mit Bargeld. (Es sei denn, man hält auch noch eine Kundenkarte hin.) Auch ein Entwenden von digitalem Geld ist nahezu unmöglich.

Trotzdem bleibt ein unangenehmer Nachgeschmack: Weil sich (wieder mal) ein US-Unternehmen in einen Bereich drängt, in dem es eigentlich nichts verloren hat. Nun wandern Daten in die USA, die dort nicht hingehören. Unsere Daten. Zahldaten. Dirk hat das nicht gestört. Mich aber schon.

https://soundcloud.com/jschieb/mobile-payment-chancen-und-risiken

Kinder haben auch Rechte: Kinderfotos im Netz

Heute wird viel fotografiert. Auch Babys und Kinder. Später landen die Aufnahmen dann häufig in Social Networks wie Facebook, Instagram oder anderen Diensten. Viel zu viele Fotos zeigen Kinder in Situationen, die peinlich oder unangenehm sind. Erwachsene sollten Kinder fragen - und ihre Rechte achten.

Die sogenannten Sozialen Netzwerke haben einen Dammbruch zu verantworten. Seitdem wir digital fotografieren können, fotografieren wir mehr. Es kostet ja nichts. Und seitdem wir mit dem Smartphone fotografieren können, fotografieren wir praktisch ununterbrochen.

Der Fotoapparat ist schließlich immer mit dabei. Wer sich wegducken wollte, wann immer er einen fotografierwütigen Menschen in seiner Umgebung sieht, müsste wie Quasimodo durchs Leben laufen. Denn irgend einer hält praktisch immer gerade sein Smartphone zum Fotografieren oder Videofilmen hoch.

Lieber einmal öfter verpixeln: Eltern sollten Regeln beachten

Kinder können sich nicht wehren

Nun gibt es Menschen, die können sich nicht richtig wehren. Je kleiner sie sind, desto weniger: Kinder sind der Fotografiesucht ihrer Eltern, Großeltern oder anderen Erwachsenen nahezu schutzlos ausgeliefert. Das Netz ist voll von Fotos, die Kinder in peinlichen oder prikanten Situationen zeigen. Aufnahmen, die so niemals hätten veröffentlicht werden dürfen. Sie werden trotzdem online gestellt.

Denn Instagram, Facebook und Co. wollen es so. Wer Aufmerksamkeit erreichen will - und sind Instagram, Facebook und Co. nicht genau dafür da? -, der postet auch schon mal unangemessene Fotos. Der Ehepartner würde einen vielleicht zurechtweisen, der Nachbar

anschnauzen, der Freund fragen, ob man noch alle Tassen im Schrank hat. Aber vielleicht auch nicht, denn allzu viele "Erwachsene" sind längst angesteckt vom Wir-zeigen-alle-Fotos-Irrsinn. Allerdings haben Kinder keine Stimme.

https://vimeo.com/305045036

Auch Kinder haben Rechte: Krasse Beispiele von Kinderfotos

Erwachsene handeln oft verantwortungslos

Das Deutsche Kinderhilfswerk fordert: Veröffentlicht keine Fotos von Kindern in peinlichen, unangenehmen oder unangemessenen Situationen! Schade, dass man das überhaupt sagen muss. Aber wer sich die Aufnahmen in den sogenannten Sozialen Netzwerken anschaut, weiß, dass dieser Aufruf leider mehr als nötig ist.

Und ungehört zu verhallen scheint. Bei so mancher Aufnahme auf Instagram, Facebook oder auch Twitter muss man sich fragen: Ja denken die Menschen denn gar nie nach? Müssen sie Begriffe wie "Verantwortung" oder "Anstand" im Wörterbuch nachschlagen?

Das allein belegt schon eindrucksvoll, dass Soziale Netzwerke eben nicht sozial sind. Doch von Instagram, Facebook und Co. hört man nichts in Sachen Kinderschutz. Warum auch? Jedes Foto, das Aufmerksamkeit erzeugt, ist gut für die Firmenkasse.

Noch mehr Datenlecks bei Facebook

Schon wieder scheint Facebook Daten veruntreut zu haben. Im großen Stil sogar. Das belegen interne Papier, die vor kurzem beschlagnahmt und vom britischen Parlament veröffentlicht wurden. Mark Zuckerberg persönlich hat zumindest mit dem Gedanken gespielt, für Nutzerdaten richtig ordentlich abzukassieren.

Klingt skandalös, Doch die Zahl der Mitglieder wird nicht kleiner, sondern größer. 2,5 Milliarden User weltweit – Tendenz: steigend. Wieso geht keine Welle der Empörung durch die Facebook-Landschaft? Darüber spreche ich jetzt mit unserem Digitalexperten und Netzwelt-Kolumnisten Jörg Schieb.

Das britische Parlament hat interne Dokumente veröffentlicht – und die lassen jedem Datenschützer die Haare zu Berge stehen.

[caption id="attachment_758940" align="alignnone" width="500"]


geralt / Pixabay[/caption]

Demnach hat Mark Zuckerberg persönlich im Oktober 2012 in einer Mail an mehrere hochrangige Mitarbeiter des Konzerns eine Idee von ihm diskutiert: Er wollte anderen Netzwerken wie Pinterest oder Spotify – die wurden sogar ausdrücklich genannt – Zugriff auf Nutzerdaten von Facebook gewähren. Mehr, als sie sonst bekommen hätten – und dafür 10 Cent pro User und Jahr berechnen.

Diese Gebühr sollten die Unternehmen aber nicht direkt zahlen, sondern im entsprechenden

Wert Werbung auf Facebook schalten. Ein kluger Schachzug, denn so kann Zuckerberg weiter durchs Land ziehen und behaupten, Facebook verkaufe keine Daten von Usern, sondern ausschließlich Werbung.

Wir wissen nicht, ob Facebook die Idee in die Tat umgesetzt hat, aber es zeigt doch, wie Mark Zuckerberg tickt: Er hält diese Idee zumindest für umsetzungswürdig. Er schlägt sie sogar vor, als „Tauschgeschäft“. Er will Nutzerdaten konkret zu Geld machen. Abstoßend!

Auch Airbnb, Netflix und Tinder betroffen

Nicht der einzige Verstoß gegen Datenschutz und Vertrauen, den man in den internen Papieren entdecken kann. Offensichtlich sind auch größere Datenmengen an Netflix, Airbnb und Tinder geflossen. Was steckt da hinter?

Viele User melden sich bei Drittanbietern wie Airbnb, Tinder oder Netflix mit ihren Facebook-Daten an. Sie müssen so kein weiteres Konto eröffnen. Es scheint so zu sein, dass die genannten Onlineplattformen Zugang zu vielen Daten der User hatten – und zu denen der Freunde noch dazu, so ähnlich wie beim Cambridge Analytica Skandal.

Wer sich mit seinem Facebook-Konto woanders anmeldet, hat womöglich – ohne es zu merken – den Zugang zu vielen Daten freigegeben. Bei Tinder war der Zugang sogar anfangs ausschließlich über Facebook möglich. Hier ist das Problem also besonders groß. Nach Facebook müssen sich nun also auch Tinder, Airbnd und Netflix Fragen gefallen lassen: Welche Daten sind geflossen, was ist mit den Daten passiert? Facebook zieht andere Konzerne mit in den Sumpf hinein.

Da Facebook immer nur zugibt, was nicht mehr zu leugnen ist, muss man wohl davon ausgehen, dass auch diese Probleme tatsächlich bestanden haben. Gut möglich, dass das Cambridge-Analytica-Datenleck am Ende das kleinere Problem war. Obwohl hier 50 Millionen User betroffen waren.

[caption id="attachment_760727" align="alignnone" width="500"]


TeroVesalainen / Pixabay[/caption]

Interne Dokumente veröffentlicht

Aber wie kommt es, dass interne Dokumente öffentlich werden? Natürlich hat Facebook sie nicht selbst veröffentlich.

Wie wir alle wissen, zieht Zuckerberg durch die Lande mit seiner Mea-Culpa-Tour. Überall entschuldigen, das muss reichen. Das Unternehmen leistet keinen ernsthaften Beitrag zur Aufklärung.

Die internen Papier kommen aus einem Rechtsstreit zwischen einem App-Entwickler und Facebook in den USA. Ein Komitee im britischen Parlament war schlau genug, eine ausgefallen Regel das britischen Rechtssystems zu nutzen, um sich die Dokumente anzueignen – durch eine Beschlagnahmung.

So sind die Informationen in die Hände der Briten geraten. Mark Zuckerberg ist dort mehrfach vorgeladen worden, aber nie im Britischen Parlament erschienen. Er hat stets einen Vertreter geschickt. Das rächt sich jetzt: Das Parlament ist zu Recht aufgebracht und ist nun im Besitz äußerst brisanter Informationen.

Die in Teilen nun veröffentlichte Kommunikation lässt tief blicken: Zuckerberg setzt sich nicht für Datenschutz ein, sondern – im Gegenteil – für den ausdrücklichen Verkauf vertraulicher Informationen.

[caption id="attachment_760729" align="alignnone" width="500"]

PublicDomainPictures / Pixabay[/caption]

Warum bleiben die User treu?

Es ist ein bisschen wie „Und täglich grüßt das Murmeltier“. Denn es vergeht doch praktisch keine Woche, ohne dass irgendwelche kleineren oder größeren Datenschutzprobleme bei Facebook bekannt werden. Müssten da die User nicht in Scharen verschwinden?

Viele User haben sich in der Tat daran gewöhnt. Es lässt sich mehr oder weniger kalt, wenn wieder mal ein Datenschutzproblem bekannt wird. Sicherlich auch deswegen, weil einige der Probleme derart technisch anspruchsvoll sind, dass das wahre Ausmaß nicht verstanden wird.

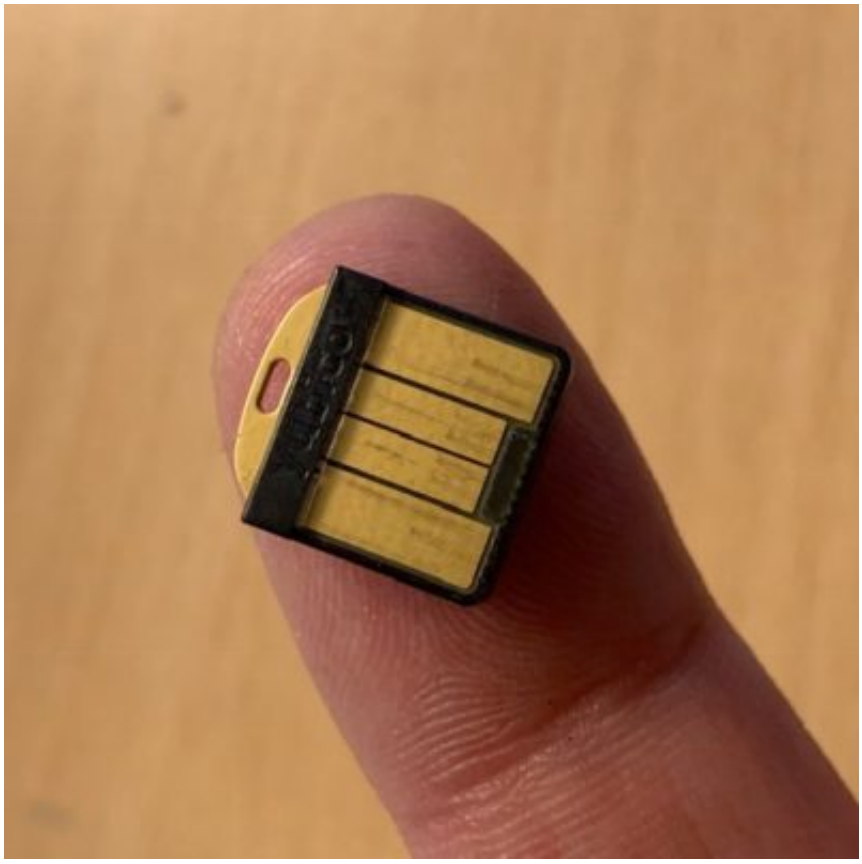
Aber auch, weil sich Facebook zwar unrechtmäßig bereichert und Daten veruntreut, aber kein Loch ins eigene Portemonnaie gerissen wird. Dann sähe der Protest ganz anders aus: Die Leute würden sich viel lautstarker beschweren.

Dass der Betrug derart leise vonstatten geht, spielt Mark Zuckerberg und seinem Unternehmen in die Hände. Er sitzt die Sache aus. Darüber hinaus ist es ein Problem, dass es keine ernsthafte Alternative zu Facebook und WhatsApp gibt. Wer will das alles schon verlassen und seine Kommunikation wieder umstellen?

Windows 10-Anmeldung mit Hardware-Token

Der einfachste Anmeldeschutz für Windows 10 sind Passwort und PIN. Auch Kamera und Fingerabdruckleser, die in manchen Notebooks und Tablets verbaut sind, erlauben eine sichere und gleichzeitig komfortable Anmeldung am PC. Eher unbekannt, nichtsdestotrotz aber charmant ist die Verwendung eines Hardware-Tokens. Eine Art Schlüssel, um den Rechner aufzuschließen. Solche Tokens sind schon für deutlich unter EUR 100,- zu bekommen.

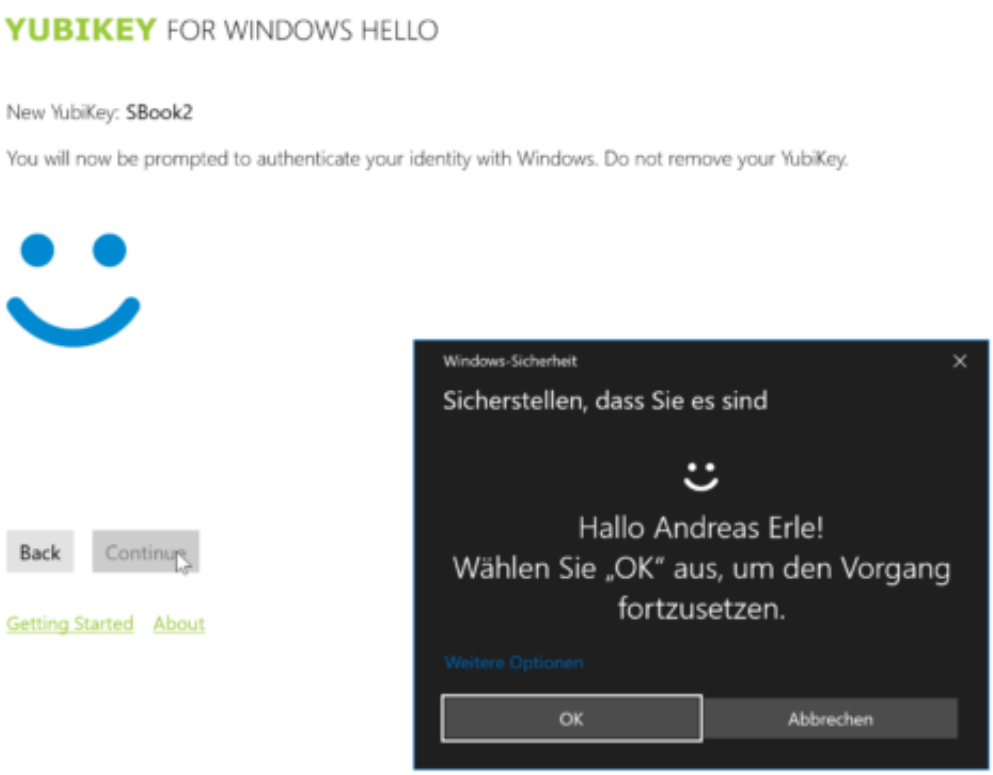
Wo früher noch eine Smartcard oder ein großer USB-Stick nötig waren, hat die Miniaturisierung ebenfalls Einzug gehalten: Security Keys haben heute oft nur die Größe eines Fingernagels und können an einem normalen USB- oder sogar USB-C-Anschluss verwendet werden. Wichtig dabei: Windows 10 muss diese auch unterstützen!



Konfiguration im PC durch Windows Hello-App

Nicht viele Sicherheit-Tokens unterstützen auch die Anmeldung bei Windows 10 direkt. Yubicos Yubikeys erreichen dies durch eine separate Windows Store-App, die dem Anmeldebildschirm von Windows 10 eine weitere Authentifizierungsmethode hinzufügt.

Einmal konfiguriert wird der Anmeldebildschirm automatisch geschlossen, wenn das Token bei den Anmeldung eingelegt ist. Keine Passworteingabe mehr, denn die Berechtigung für die Anmeldung an Ihren PC ist mit der initialen Einrichtung auf dem Token abgelegt worden.



Bei einigen der Modelle ist ein Sensor verbaut, mit dem aus dem Token ein vorkonfigurierbares Kennwort abgerufen werden kann. Dieses wird dann wie eine Tastatureingabe an Windows übergeben. Die einfachste Version, komplexe Kennwörter nicht manuell eingeben zu müssen!

Werbung in Apps ausknipsen

Viele Mobile-Apps refinanzieren sich über Werbung. Das kann ungeheuer nervtötend sein Ständig erscheinen Reklamebotschaften, mal am oberen, mal am unteren Bildschirmrand. Manchmal sogar bildfüllend - das ist dann besonders nervig. Mit einem Trick lassen sich die lästigen Werbeeinblendungen häufig vermeiden.

Viele Apps brauchen keine Onlineanbindung. Das gilt zum Beispiel für viele Games, aber auch Foto-Apps. Wenn keine Onlineanbindung erforderlich iat, kann folgender Trick weiterhelfen: Einfach in den Flugmodus gehen (oder das WLAN abschalten). Denn wenn keine Internetverbindung besteht, können keine Werbebanner nachgeladen werden.

Am besten mal ausprobieren: Nerven die Werbebanner in einer App, einfach mal die Verbindung zum Netz kappen. In vielen Fällen reicht das, um die Reklame mundtot zu machen.

Mit Werbeblockern lässt sich das Ergebnis nicht erzielen. Die funktionieren meist nur im Browser.

https://vimeo.com/286137614

Luna Display: Das iPad als Zweitmonitor am Mac

Das iPad ist als eigenständiges Gerät ohne Frage eine Bereicherung. Durch sein hochauflösendes Display weckt es aber auch den Wunsch, als externer Zusatzmonitor genutzt zu werden. Zumindest für Macs und Macbooks ist dieser Wunsch durch ein kleines Dongle für umgerechnet gerade einmal EUR 80,- leicht erfüllbar.

Das Luna Display ist ein kleines Dongle, das in den USB-C (Thunderbolt 3-) Anschluss der neueren Macbooks und iMacs gesteckt wird. Eine Version für den Mini DisplayPort-Anschluss gibt es ebenfalls. Es gaukelt dem Mac vor, ein „normaler“ externer Monitor zu sein, der kabellos über WLAN genutzt werden kann.

App- und Softwareinstallation auf Mac und iPad

Zum Betrieb muss sowohl auf dem Mac als auch auf dem iPad eine App installiert werden. Diese sorgen dafür, dass die Verbindung zwischen dem Mac und dem iPad aufgebaut wird. Die weitere Konfiguration wird dann wie gewohnt in MacOS vorgenommen, das iPad erscheint als normaler Monitor und kann über die Systemeinstellungen von der Position zu den anderen Monitoren im System angeordnet werden. Auch die Auflösung und die Betriebsart (Verwendung als zusätzlicher Monitor oder Spiegeln der Inhalte des Hauptmonitors) kann festgelegt werden.

Aktuell ist das Luna Display-Adapter nur auf Macs verwendbar. Der Hersteller hat allerdings auf Nachfrage angegeben, dass auch eine Windows-Version in der Entwicklung ist. Damit wäre es dann möglich, auch für Surface Book, Surface GO und andere Geräte mit USB-C die selbe Funktionalität zu erreichen. Einen Erscheinungstermin gibt es dafür leider noch nicht.

Mac-Cursor für Windows 10

Bei Windows haben Sie als Nutzer nur eine kleine Auswahl vorgegebener Mauszeiger. Schließlich hat jeder einen anderen Geschmack, was das Zeiger-Design angeht. Wenn Ihnen der schwarze Maus-Cursor von macOS eher zusagt als die Standard-Windows-Variante, können Sie auch einen Mac-Mauszeiger nutzen.

Der Clou an der Sache: Mauszeiger sind nicht bloß einzelne Bilder. Stattdessen können Sie sich Mauszeiger wie ein komplettes Design – mit verschiedenen Bildern und Animationen für unterschiedliche Zustände, wie Pfeil, Warten, Textbalken usw.

Wer den Mac-Cursor auf seinem Windows 10-PC nutzen möchte, lädt die ZIP-Datei zunächst von DeviantArt herunter. Dann entpacken Sie diese und klicken anschließend mit der rechten Maustaste auf die enthaltene Datei **install.inf**. Hier rufen Sie die Option zum **Installieren** auf. Wichtig: Hier erfolgt keine optische Bestätigung der Installation.

Jetzt drücken Sie [Win]+[R], geben **main.cpl** ein und klicken auf **OK**. Nun wechseln Sie zum Tab **Mauszeiger** und öffnen das Dropdown-Feld. Dort markieren Sie den Eintrag **El Capitan** und bestätigen die Änderung schließlich, indem Sie auf **OK** klicken.