Schieb Report

Ausgabe 2019.02

Datenleak: Wie die Medien damit umgegangen sind

Das neue Jahr war kaum angebrochen, da hatten wir auch schon den ersten handfesten Datenskandal in Deutschland. Der ist diesmal aber nicht auf das Konto von Facebook und Co. gegangen. Es hat jemanden gegeben, der Informationen über Prominente und Politiker erforscht und dann auf Twitter veröffentlicht hat.

Die Medien haben sich überschlagen, der Druck auf die Ermittlungsbehörden war enorm. Wenige Tage später war der mutmaßliche Täter auch schon dingfest gemacht.

Seit dem 4. Januar wird über den Datenleak rauf und runter berichtet. In allen Medien. Mittlerweile ist der mutmaßliche Täter gefasst. War dieses Ausmaß an Berichterstattung gerechtfertigt?

Rückwirkend muss man sagen: Definitiv Nein!

Der Fall war eigentlich mehr oder weniger eine Bagatelle. Nicht, dass es keine Straftat gewesen wäre. Aber sicher keine, die die Republik und die Politik tagelang hätte in Atem halten müssen.

Man darf nicht vergessen: Wir reden von der Veröffentlichung von vertraulichen Daten, die sich der mutmaßliche Täter auf illegale Weise besorgt hat, die aber in aller Ruhe vom 1. Dezember an auf Twitter veröffentlicht wurden. In aller Seelenruhe. Jeden Tag eine andere Indiskretion. Zuerst von Internet-Sternchen. Dann von Fernsehmoderatoren und Journalisten. Am Ende von Politikern. Und erst da haben die Alarmglocken geschrillt.

Qualität der Berichterstattung

Aber wie war denn die Berichterstattung inhaltlich? Fachlich korrekt, angemessen – oder eher hysterisch?

Ich habe von allem etwas gesehen. Aber man muss schon sagen: Es gab viel Hysterie – und vor allem von Dummheit und Unkenntnis geprägte Desinformation. So wurden schon früh in der BILD-Zeitung die Russen verantwortlich gemacht. Ohne dass es auch nur ein Indiz, geschweige einen Beleg dafür gegeben hätte.

Mangels konkreter Fakten wurde vor allem gemutmaßt. Denn im Grunde konnte man nicht viele Fakten berichten: Da gibt es einen Twitter-Account, über den persönliche und private Daten öffentlich gemacht werden – gegen den Willen der Betroffenen.

Offensichtlich wurden die Informationen aus unseriösen Quellen geholt. Mehr wusste man nicht. Daraus wurden dann Hackaktionen aus Russland oder gezielte Attacken aus der sogenannten „rechten“ Ecke, weil keine AfD-Politiker Opfer wurden. Es wäre garantiert „kein jugendlicher Hacker mit Pizzakartion in der Ecke“, hieß es bei BILD. Genau so ist es am Ende aber gekommen.

Sofern die Behörden den Richtigen geschnappt haben, wissen wir doch mittlerweile: Es waren nicht die Russen. Auch kein Geheimbund. Sondern ein ganz normaler Mensch. Ein Schüler.

Wie einfach ist Doxing?

Ich würde nicht unbedingt sagen, dass es kinderleicht ist – aber es ist eben nicht so schwierig, wie man denkt. Der mutmaßliche Täter ist kein Hacker-Genie, aber er war entschlossen und fleißig.

Er hat auf bekannte Informationsquellen zurückgegriffen, sich dort Daten besorgt – etwa Mail-Adresse und Passwörter aus alten Hackangriffen – und diese dann offensichtlich durchprobiert in den völlig unzureichend gesicherten Cloud-Diensten der Betroffenen.

Im Grunde alles bekannt: Seine Mail-Accounts und seine Cloud-Dienste muss man auch gut sichern, sonst kann so etwas halt passieren. Der aktuelle Fall ist daher geeignet für eine öffentliche Debatte: Wo müssen wir selbst darauf achten, unsere Daten besser zu schützen. Aber was kann der Gesetzgeber tun, um die Anbieter zu einem besseren Schutz zu zwingen. Und da ist eine Menge möglich.

Verwendung der Begriffe

Schauen wir noch mal auf die Berichterstatter: Hier wurden ständig Begriffe wie Hacker oder Doxing verwendet. Sie wurden leider nicht immer korrekt benutzt.

Ich habe mich erschreckt: In Berichten, aber auch auf dem Sender wurde von Doxing geredet, als wäre das ein Synonym für Hacken. Dabei ist die Bedeutung völlig unterschiedlich. Bei einem Hackangriff versucht man gezielt, in ein gesichertes System einzudringen, etwa durch Ausnutzen von bekannten Sicherheitslücken oder durch rüde Methoden.

Es gibt viele Methoden. Beim Doxing spielt das keine Rolle, denn hier werden öffentlich im Netz zugängliche Informationen über eine Person zusammengetragen und dann veröffentlicht, meist mit der Absicht, der Person zu schaden. Das ist etwas völlig anderes. Es kann in Tateinheit geschehen, muss aber nicht. In den Medien wurde unfassbar viel gemutmaßt – und auch viel Unsinn geredet.

Mail-Accounts absichern: Gar nicht so einfach

Der aktuelle Datenleak hat mal wieder Schwachstellen deutlich gemacht. Vor allem in Mail-Diensten und Cloud-Diensten. Die populärsten deutschen Mail-Anbieter GMX und T-Online bietet bislang keine Möglichkeit an, die Postfächer mit einer Zwei-Faktor-Authentifizierung abzusichern. Ohnehin machen davon nur viel zu wenige User Gebrauch.

Jetzt ist also klar, wer hinter dem "Datenklau" steckt: ein 20-Jähriger Schüler aus Hessen. Kein Russe. Kein Geheimdienst. Kein Profi-Hacker, der mit allen Wassern gewaschen ist.

Es reicht also der entschlossene Wille zum Doxxing - bestimmt das Wort des Jahres 2019 -, um die Nation tagelang in Atem zu halten. Die Umstände im aktuellen Fall machen deutlich, wie gering die Hürde ist, um an die Daten anderer Leute zu kommen. Es gibt viele Schwachstellen in unserer digitalen Welt. Aber insbesondere eine ließe sich nun wirklich leicht absichern: das E-Mail-Konto.

Weniger Sicherheit als möglich - aus reiner Bequemlichkeit

Wer die Zwei-Faktor-Authentifizierung (2FA) nutzt, macht sein E-Mail-Konto nahezu sturmsicher. Bei der 2Fa muss der Nutzer beim Login nicht nur ein Passwort eingeben, sondern auch noch einen zweiten Faktor - meist einen Code, der per SMS zugeschickt oder durch eine spezielle App erzeugt wird. Die Folge: Wer das Passwort klaut, kann damit nichts anfangen. Denn nur in Kombination mit dem individuell erzeugten Code gibt es Zugriff.

Klar, das ist ein bisschen umständlicher als nur mit Passwort. Hat man sich aber erst mal daran gewöhnt, geht einem das locker von der Hand. Außerdem muss man seinen Rechner oder sein Smartphone nur ab und zu durch den zweiten Faktor freigeben.

https://vimeo.com/310068776

GMX ist Schlusslicht in Sachen Sicherheit

Vermutlich denken die meisten Leser: Ja, habe ich schon mal gehört - ist mir aber zu schwierig. Ein großer Fehler!

Unverantwortlich ist zudem, dass die, die es besser wissen müssten, nur an ihren Geldbeutel denken. Ob Google, Yahoo, Microsoft, Amazon, Apple, Facebook oder Twitter: Fast überall gibt es die Zwei Faktor Authentifizierung.

Sie ist aber nicht voreingestellt, quasi mit Sicherheit als Standard, sondern muss vom User explizit aktiviert werden. Klar, dass das nur ein Bruchteil macht. Die Onlinedienste verzichten auf ein Mehr an Sicherheit, um die User nicht mit mehr Aufwand zu belästigen.

Noch schlimmer sind aber Mail-Dienste wie GMX - immerhin einer der größten Mail-Dienste in Deutschland: GMX bietet schlicht keine Zwei-Faktor-Absicherung an. Ich habe beim Unternehmen nachgefragt. Die Antwort: Im zweiten Quartal 2019 soll sie kommen, die 2FA. Bis dahin ist GMX aber sicherheitstechnische Diaspora. Wem seine Daten wichtig sind, sollte schleunigst wechseln.

Aber auch die Politik trägt Schuld. Anstatt nun ein Cyberabwehrzentrum Plus Deluxe mit Sternchen (und Wochenenddienst) einzuführen, wäre es doch eher angeraten, die Zwei-Faktor-Authentifizierung bei sicherheitsrelevanten Logins (wie beim E-Mail-Postfach) gesetzlich zum Mindeststandard zu erklären. Gefällt nicht allen? Egal! Wir müssen uns im Auto doch auch anschnallen.

Wieso gibt es eigentlich so wenig gute Lösungen zum Datenschutz?

Der aktuelle Fall des Datenleak macht deutlich: Wenn etwas passiert, sind alle aufgeregt - und berichten intensiv. Aber schon wenige Tage später kehrt wieder Ruhe ein. Ernsthafte Konsequenzen will aber keiner ziehen. Dabei müssten alle etwas unternehmen, um Daten sicherer zu machen. Allzu groß ist das Angebot allerdings nicht.

Was macht der Mensch normalerweise, wenn ihm eine Gefahr bewusst wird? Richtig; Er wappnet sich für den Ernstfall. So lassen sich Hamsterkäufe erklären. Oder das Rollen über die Autobahn mit 20 km/h, wenn es anfängt zu schneien. Aber was passiert, wenn mal wieder im großen Stil Daten geleakt werden?

Es gibt zwar eine Welle der Empörung und jede Menge Spekulationen über die Hintergründe. Doch was eher nicht kommt, ist eine Welle der Einsicht, die den sofortigen Wunsch nach mehr Datensicherheit nach sich zieht.

Auf der CES keine Lösungen

Doch nichts passiert. Auf der "Consumer Electronics Show" (CES) in Las Vegas gibt es alles Mögliche zu sehen: 8K-Monitore, autonome Autos, die ersten 5G-tauglichen Smartphones und Geräte, Digitale Assistenten, VR und AR - aber keine bahnbrechenden Neuheiten oder Konzepte in Sachen Datensicherheit. Denkbar wären doch zum Beispiel unknackbare Festplatten, für Hacker unerreichbare Cloud-Dienste, monstermäßig sichere Login-Verfahren...

Warum wohl kümmert sich niemand in der Branche um so etwas? Gute Lösungen müssten den Anbietern doch aus den Händen gerissen werden. Müssten. Passiert aber nicht. Denn die meisten wollen für mehr Sicherheit kein Geld ausgeben. Nicht mal kostenlose Dienste werden genutzt. Beispiel: Mittlerweile kann man seine Onlinekonten fast überall mit der Zwei-Faktor-Authentifizierung absichern. Kostenlos. Ein dramatisches Plus an Sicherheit. Aber nur wenige

nutzen es.

https://vimeo.com/309889811

So funktioniert die Zwei-Faktor-Authentifizierung

Es braucht verbindliche Sicherheitsregeln

Es braucht also dringend ein völlig anderes Verständnis von Sicherheit - und der Tragweite, wenn Daten in fremde/falsche Hände geraten. Klar, wenn man selbst tatsächlich mal betroffen ist, wenn Fremde auf meine Kosten etwas online bestellen oder brisante Daten im Netz landen, dann denkt man sich: Hätte ich doch etwas unternommen. Doch wenn nichts passiert, sind die möglichen Folgen zu abstrakt und mit keinem Preisschild versehen. Deshalb die geringe Investitionsbereitschaft.

Da kommt der Gesetzgeber ins Spiel. Er müsste die Bandagen anziehen: Datenklau und Datenverlust müssten mit Strafen und/oder Schadenersatzansprüchen verknüpft sein. Das würde ganz schnell die Nachfrage nach Sicherheitslösungen vorantreiben. Die Nachlässigkeit der Nutzer ist eine Sache. Der Mangel an Einsicht, dass passieren wird, was passieren kann und der daraus resultierende Wille, das Schlimmste zu verhindern, eine andere.

Wir müssen uns im Auto schließlich auch anschnallen, oder? Ein vergleichbarer Sicherheitsanspruch wäre ja auch in der Onlinewelt möglich.

https://www.youtube.com/watch?v=x665fq2eajs&t=99s

WLAN im Smarthome: Neue Herausforderungen

WLAN: Heute fast in jeder Wohnung eine selbstverständliche Einrichtung.

Bereits heute stößt das drahtlose Internet (WLAN) in einigen Haushalten an seine Grenzen. In den kommenden Jahren wird sich die Nutzung über das Abrufen von Videoinhalten und viele weitere Funktionen am Rechner hinausbewegen. Während vor gut zehn Jahren die Smartphones ans Netz angehängt wurden, werden in den nächsten Jahren viele weitere Haushaltsgeräte folgen - und damit die Belastung spürbar steigern.

Größere Datenmengen werden kommen

Das Konzept des Smarthomes sieht vor, für eine Vernetzung der Elektronik des Haushalts mit einer zentralen Steuereinheit zu sorgen. Flexibel ist dies mithilfe des ohnehin verfügbaren WLAN-Netzes möglich.

Bereits in den letzten Jahren konnte eine Entwicklung in diese Richtung beobachtet werden. So wurden viele Drucker mit WLAN-Anbindung ausgerüstet. Vorteil: Der Drucker lässt sich von jedem Gerät im WLAN ansprechen. Selbst vom Smartphone. Solche WLAN-tauglichen Drucker gibt es inzwischen von vielen Herstellern, auf der Homepage von tonerpartner.de sind einige zu finden.

In Zukunft sollen möglichst viele Geräte, von der Waschmaschine bis zum Kühlschrank, mit dem WLAN-Netz verbunden werden.

Damit alle Prozesse innerhalb des Smarthomes geordnet ablaufen können, wird es dabei von großer Bedeutung sein, die Zuverlässigkeit des Internets zu erhöhen. Die allgemeine Belastung des Netzes wird damit unweigerlich steigen. In einigen Regionen Deutschlands wird aus diesem Grund ein weiterer Ausbau der digitalen Infrastruktur erforderlich sein.

Zugriff über die Steuereinheit

Bereits heute bieten Fertighaushersteller ihren Kunden die Möglichkeit, in ihren eigenen vier Wänden eine große Steuereinheit einzubauen. Dort ist es nach und nach möglich, neue Funktionen zu integrieren und für einen geregelten Austausch der Daten zu sorgen. Von der Heiztechnik bis hin zu den Sicherheitsmechanismen des Hauses können dort Eingriffe vorgenommen werden.

Sichtbar ist letztlich ein großer Touchscreen, über den auf all diese Elemente zugegriffen werden kann. Einige Ausrüster bieten inzwischen auch die Fernwartung an, um auftretende Probleme zügig korrigieren zu können und ihre Kunden aus der Distanz zu unterstützen.

Neue Anfälligkeiten kommen

Während deutliche Vorteile in puncto Komfort und Nachhaltigkeit erreicht werden könnten, lässt das Smarthome an anderer Stelle wichtige Fragen offen. Ist etwa der WLAN-Router nicht mehr in der Lage, die anfallenden Datenmengen zu bewältigen, kommt es kommt zu Störungen. Schlimmstenfgalls lässt sich dann die Heizung nicht mehr regeln, die Beschattung kann nicht mehr angepasst werden und auch der Einbruchsschutz wird nicht mehr aufrechterhalten.

Um diesen drohenden Szenarien aus dem Weg gehen zu können, wird es für die Hersteller bedeutsam sein, eine analoge Nutzung ihrer Geräte nach klassischem Muster anzubieten. In der Not muss es möglich sein, auch ohne die direkte Verbindung zum World Wide Web auf alle Geräte zuzugreifen.

Ansonsten würden viele Haushalte bei einem Abbruch der Verbindung zum Internet ihre Aktivität einstellen und wären nicht mehr dazu in der Lage, den normalen Alltag zu bestreiten. An diesem Punkt schlägt den Verantwortlichen und ihrem Konzept sogleich Skepsis entgegen.

Aufrüstung erfolgt schrittweise

Bis wir alle Geräte unseres Haushalts auf diese Weise vernetzen werden, wird es wohl einige Zeit dauern. Anstelle eines blitzartigen Umstiegs verfolgen die Verantwortlichen ein geordnetes Umstellen in mehreren Phasen. Wird ein neues Elektrogerät angeschafft, so kann dieses mit der Steuereinheit verbunden werden. Nach und nach erweitert die Smarthome-Technologie auf diese Weise ihren Wirkungsbereich und kann neue Menschen erreichen.

CES in Las Vegas: Die Trends

Die „Consumer Electronics Show“ (CES) ist die größte Messe ihrer Art, wenn es um Unterhaltungselektronik, Computer und Internet geht. Grund genug, um über die Trends in diesem Jahr zu sprechen: Was kommt, was entwickelt sich, womit müssen wir rechnen?

Den ersten Datenskandal haben wir bereits. Datenschutz sollte doch vielleicht eins der wichtigsten Themen sein in diesem Jahr – in unser aller Interesse.

Aber auf der Messe spielt das Thema praktisch keine Rolle. Die Industrie denkt sich ständig neue Sachen aus. 8K-Fernseher zum Beispiel. Aber Datenschutz ist kein echtes Thema.

Das müssen wir als Warnsignal verstehen: Würden wir uns alle – also Politik, Industrie und wir Privatleute – für den Datenschutz interessieren und intensiv dafür einsetzen -, würden wir bevorzugt oder ausschließlich Produkte kaufen oder nutzen, die sichere Daten bieten, dann würde die Industrie umschwenken.

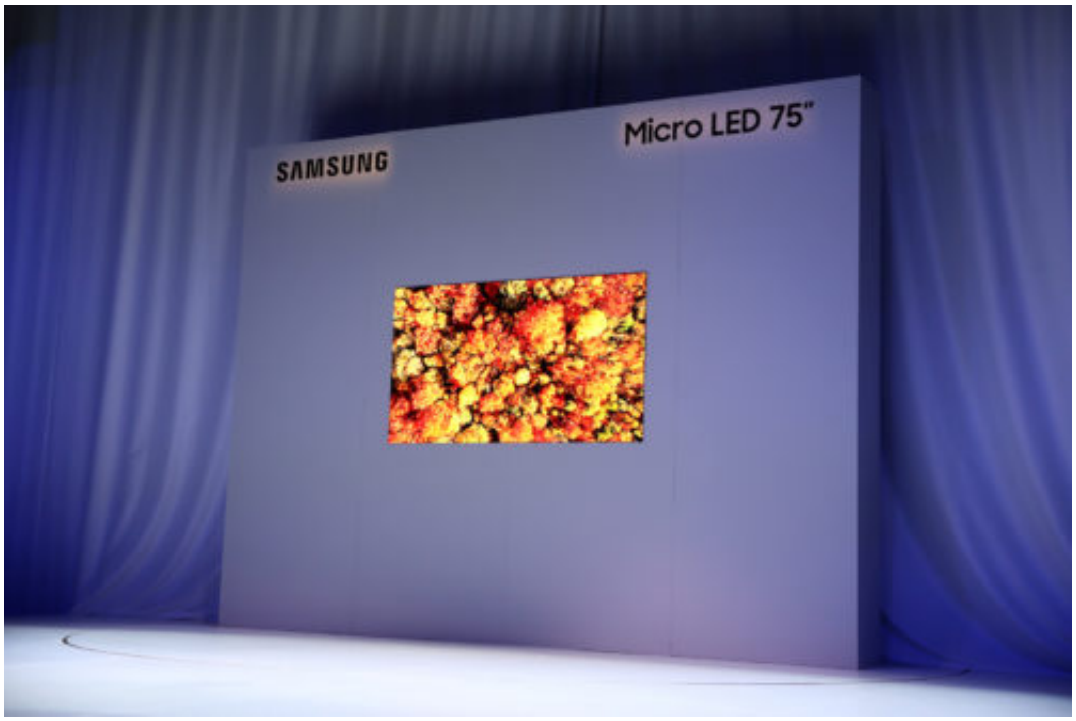
Weil wir uns aber nicht sonderlich für Datenschutz interessieren, passiert auch nichts bis wenig. Es gibt jedenfalls kaum Produkte, mit denen wir unsere Daten sicher speichern können, ob zu Hause, in der Firma oder in der Cloud. Und Cloud ist ja ein wichtiges Stichwort: Wie es aussieht, könnte der Hacker sich gerade hier bedient haben. Ich würde mir also wünschen, wenn Datenschutz 2019 zum Trendthema würde.

Neuer Trend 8K

Es sind erste Fernseher zu sehen, die das bieten. Ultrahochaufgelöst. Natürlich nützt es nichts, wenn ein Fernseher 8K beherrscht, aber sonst kein Gerät. Denn es müssen Signale auf den

Fernseher, die das auch nutzen. Wer einen 4K-Fernseher hat, schaut nicht schärfer Fernsehen, da die Sender 4K nicht unterstützen.

Aber Amazon und Netflix bieten einige Filme und Serien in 4K. Auch Games lassen sich in 4K dadddeln... Nun ist die nächste Runde eingeläutet. Erste 8K-Kameras gibt es bereits. Davon wird es in Zukunft mehr geben, dann wird es Spiele geben, die 8K können... Bis wir YouTube-Videos in 8K sehen können oder sogar Filme und Serien auf Netflix, werden aber sicher noch ein paar Jahre vergehen. Aber: Der erste Schritt ist gemacht.



Künstliche Intelligenz - KI

Die Bundesregierung hat im vergangenen Jahr drei Milliarden Euro zur Förderung von Künstlicher Intelligenz (KI) in unserem Land ausgelobt. Ein klarer Trend: Alle entwickeln gerade an der sogenannten Künstlichen Intelligenz. Ich sage „sogenannte“, weil es keine echte Intelligenz ist, sondern bestenfalls eine Simulation.

Aber hier stecken die Unternehmen gigantische Summen hinein. Vor allem Unternehmen, die wir alle kennen: Apple, Google, Facebook, Microsoft – und Samsung. Samsung soll 22 Milliarden Dollar investieren in seine KI-Systeme wie Bixby.

Aber auch Apple, Amazon, Google, Facebook und Microsoft wollen ihre Digitalen Assistenten schlauer machen. Sie sollen alle Fragen verstehen, besser und schneller. Ein Wettbewerb, der viel Umsatz verspricht, denn die Betreiber binden die Nutzer an ihre Dienste und Plattformen. Die meisten nutzen nur einen Assistenten, nicht mehrere. Wer den Job am besten macht, bekommt die meisten User – und verdient Geld mit Werbung, Provisionen und überhaupt.

Leider geht es auf der CES praktisch gar nicht um die kritischen Aspekte der KO. Die CES ist halt eine „Show“, eine Verkaufs-Show. Wir brauchen dringend eine kritische Auseinandersetzung mit KI: Was soll die Software dürfen, wo sind Grenzen? Die ethischen Fragen sollten eine größere Rolle spielen.

Augmented Reality boomt

In den letzten Jahren haben wir auf den Messen immer dasselbe Bild gesehen: Menschen mit Cyberbrillen, die sich komisch bewegen.

Doch Virtual Reality (VR) entwickelt sich langsam weiter, wird aber auch dieses Jahr nicht zum Massenthema. Zu teuer, zu wenig sinnvolle Einsatzmöglichkeiten – es sei denn, man spielt gerne Spiele. Was aber groß im Kommen ist, ist Augmented Reality (AR). Hier verschmelzen echte und virtuelle Welt. Wir kennen das von Spielen wie Pokemon: Im Display des Handys sehen wir die echte Welt – und rein montierte Monster.

Das Konzept wird ausgebaut. Aber im sinnvollen Bereich: Google Maps zum Beispiel kommt in einer AR-Version. Da können wir uns mit dem Smartphone umschauen und bekommen Erläuterungen zu Gebäuden, Brücken oder Straßen, die wir gerade sehen. Und die App zeigt uns den Weg: Da musst Du lang... Auch im Arbeitsbereich wird AR zum Einsatz kommen. Hier aber mit speziellen Brillen: Wir sehen die Umwelt – und es werden Extrainfos eingeblendet. Diesen Hebel umlegen. Oder Ärzte schauen sich gemeinsam 3D-Modelle an.

"Smarte" Westen überwachen chinesische Schüler

In Sachen Überwachung gibt es einen ungekürten Weltmeister: China. Hier werden nicht nur mit Hochdruck neue Technologien zur Überwachung entwickelt, sondern auch gleich eingesetzt. Widerstand aus der Bevölerung ist nicht zu befürchten. In einigen Schulen müssen die Schüler jetzt spezielle Westen tragen, die mit Überwachungs-Chips ausgestattet sind.

China zeigt der Welt, was in puncto Überwachung alles möglich ist. Nicht nur technisch, sondern generell. Von komplett überwachten Innenstädten, in denen Wohl- und Fehlverhalten aller Bürger registriert und durch Gesichtserkennung auch gleich entsprechend verbucht werden kann, haben wir schon gehört – ein erster erkennbarer Auswuchs von Künstlicher Intelligenz (KI).

Doch die Überwachung geht munter weiter: In einigen chinesischen Provinzen tragen Schüler mittlerweile mit speziellen Chips ausgestattete Jacken. Damit lassen sich die Schüler stets genau orten. Angeblich nur, wenn sie sich auf dem Schulgelände befinden. Kommen sie pünktlich? Befinden sie sich in den richtigen Räumen? Stehen sie aufrecht oder liegen sie faul herum? Die Jacke verrät's ...

[caption id="attachment_760984" align="alignnone" width="500"]


Chinesische Schüler müssen spezielle Schuluniform tragen[/caption]

In jeder "intelligenten Uniform" ein Chip

Jeder muss seine "intelligente Uniforn" auf dem Schulgelände tragen. Die Jacken sollen den Schülerinnen und Schülern angeblich den Alltag erleichtern und ihr Lernverhalten verbessern. Ist das nicht fürsorglich? Gezieltes Dauer-Tracking durch Zauberjacke statt Gesichtserkennung

auf dem Schulgelände. Doch der angebliche Komfort ist nur vorgeschoben. In Wahrheit geht es um Überwachung total.

Das Ziel: Artige Mitbürger. Denn wer ständig überwacht wird und sich darüber im Klaren ist, der verhält sich anders. Angepasster. Das weiß jeder, der "The Circle" gelesen hat - oder die Macht der Sozialen Netzwerke zu Ende denkt und die Enthüllungen von Edward Snowden noch nicht völlig vergessen hat.

KI wird in China im Eiltempo weiter entwickelt. Vor allem dort, wo sie zur Überwachung eingesetzt werden kann. Aus Cities werden "Smart Cities". Aus einem Campus ein "Smart Campus". Zwar werden weder Städte noch Universitäten smart, nur weil jeder jederzeit überwacht wird. Aber der Staat ist besser im Bilde. Er weiß viel mehr – smart ist das nicht.

https://vimeo.com/228465945

KI kann nicht nur überwachen, sondern sogar schon selbst Fotos erstellen

Wer an smart glaubt, ist alles andere als smart

"Smart" ist natürlich nur das Verkaufsargument für die Überwachungsapparatur. Denn wer will sich schon wehren, wenn etwas "smart" werden soll? Eben! Künstliche Intelligenz verarbeitet die ungeheuren Datenmengen, die durch Gesichtserkennung oder getrackte Chip-Jacken anfallen, ohne mit der virtuellen Wimper zu zucken. Was dabei herauskommt? Wem das alles dient? Das erfahren die Überwachten nicht. Sie sollen sich freuen, dass sie in einer "smarten" Welt leben. Klasse.

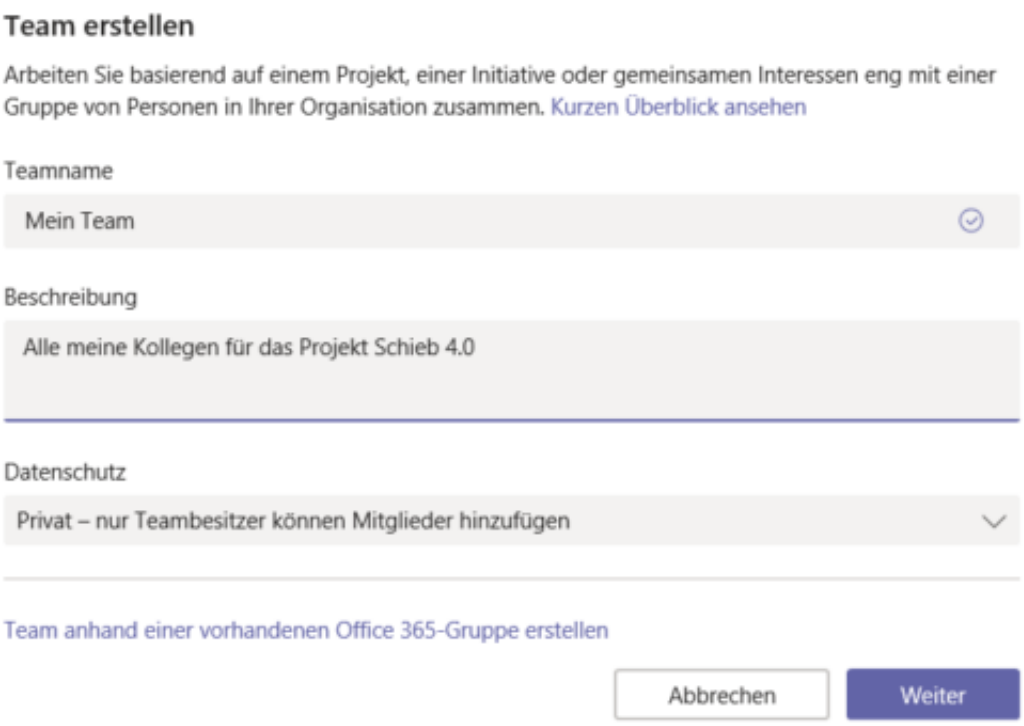
Wir sollten von China lernen. China macht vor, welche Konsequenzen es haben kann, wenn alles gemacht wird, was technisch möglich ist - ohne jede Debatte über Chancen, Risiken und gesellschaftliche Folgen. Wir sollten hier bei uns nicht denselben Fehler machen. Es empfiehlt sich jedenfalls nicht, den Chinesen alles nachzumachen, nur um "nicht den Anschluss zu verlieren", wie es gerne heißt.

Willkommen im Team! Ein neues Team anlegen

Skype for Business wird von Microsoft auf das virtuelle Abstellgleis geschoben und durch Microsoft Teams ersetzt. Was auf den ersten Blick als nur für Firmen interessante Lösung erscheint, hat für den Privatnutzer von Office 365, der mehrere Benutzer (beispielsweise die Familienmitglieder) verwaltet, durchaus interessant. Und ein neues Team ist schnell angelegt.

Verantwortlich für diese Aufgabe ist derjenige, der Administrationsrechte für die Office 365-Installation hat. Dieser kann über die App-Auswahl oben links auf **Teams** klicken und unter **Einem Team beitreten oder ein Team** erstellen den Prozess starten.

Der **Teamname** sollte schon sprechend sein, zusätzlich kann aber noch eine **Beschreibung** angegeben werden, die noch weitere Informationen zur Unterscheidung von unterschiedlichen Teams enthält.



Unter **Datenschutz** kann festgelegt werden, ob das neue Team noch erweitert werden kann und wer das darf: Im Standard ist diese Berechtigung auf den Teambesitzer (also Sie) eingeschränkt, auf Wunsch kann sie aber auch an jedes Mitglied der Organisation (im Besipiel der Familie) freigegeben werden.

Im nächsten Schritt können nun die Mitglieder des Teams aus der Organisation hinzugefügt werden.

Jedes Mitglied des neuen Teams bekommt nun automatisch eine E-Mail zugesendet, dass es einem Team hinzugefügt wurde und kann direkt mit der Arbeit loslegen.

Erster Patchday 2019: Updates für alle Windows-Versionen

Der erste offizielle Patchday für Microsoft Produkte des Jahres 2019 ist verstrichen, und so hat Microsoft am 8.1.2019 für alle Windows-Versionen Patches und Updates herausgebracht. Der Fokus lag hier weniger auf neuen Funktionen, sondern vor allem 49 Sicherheitslücken. Gerade im Angesicht der letzten Sicherheitsvorfälle ein wichtiger Schritt.

[caption id="attachment_761021" align="alignnone" width="500"]

geralt / Pixabay[/caption]

Das kumulative Update enthält alle vorigen Updates plus die neuen Patches und kann manuell hier herintergeladen werden. Ist die automatische Update-Funktion von Windows 10 aktiv und das Gerät eingeschaltet und mit dem Internet verbunden, dann findet die Installation in den nächsten Tagen auch automatisch statt.

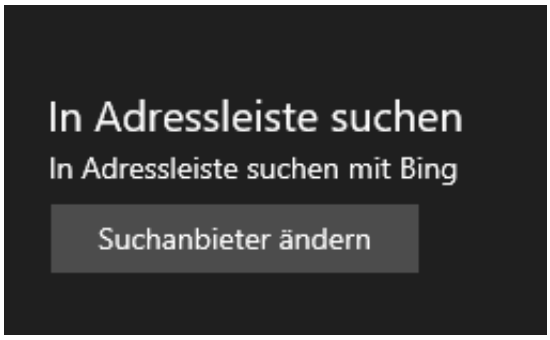
Vielzahl von Sicherheitsupdates

Unter anderem wird mit dem Update die bisher konfigurierbare Ausführung der PowerShell mit nicht administrativen Accounts über eine Remote-Verbindung verhindert.

Weiterhin bekommen Edge und der Internet Explorer, die App-Verwaltung, die Windows WLAN-Implementierung, die JET Database Engine, die Virtualisierungsplattform und die Scripting Engine Sicherheitsupdates.

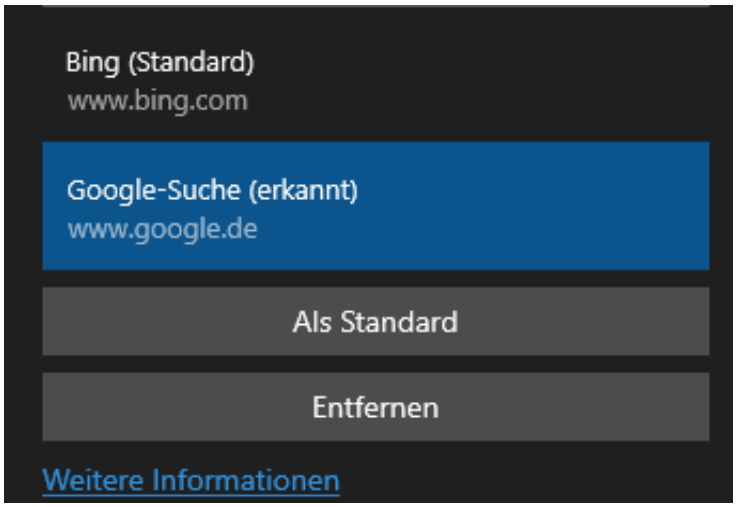
Ändern des Suchanbieters in Microsoft Edge

Die Suche im Internet ist eine der meist verwendeten Funktionen unter Windows. Lange sind die Zeiten vorbei, in denen man erst die Webseite der Suchmaschine (z. B. bing.com) aufrufen musste und dann erst den Suchbegriff eingeben konnte. Microsoft Edge (und auch andere Browser) erlauben die Eingabe des Suchbegriffs direkt in die Adresszeile. Sie führen dann die Suche mit der konfigurierten Standardsuchmaschine aus. Im Standard ist das Microsofts eigener Suchdienst bing. Das Umstellen auf eine andere Suchmaschine geht problemlos:



Rufen Sie zuerst die Webseite der Suchmaschine auf, die Sie als Standard verwenden möchten, zum Beispiel google.de oder startpage.com. In Edge führt der Weg dann über **Einstellungen**, **Erweitert**, **In Adressleiste suchen**, wo Sie mit einem Klick auf **Suchanbieter ändern** aus der Liste der erkannten Suchmaschinen diejenige bestimmen können, die Sie für die Suche über die Adresszeile des Browsers nutzen möchten.

Webseiten von Suchmaschinen, die bereits aufgerufen werden, zeigt Edge als "erkannt" an. Wenn Sie einen der Einträge **als Standard** setzen wollen. klicken Sie diese Option an. Sie können ebenfalls bereits erkannte Suchmaschinen **entfernen**.



Andere Suchmaschine, anderes Ergebnis

Je nachdem. welche Suchmaschine sie auswählen, werden Sie unterschiedliche Ergebnisse zu Ihren Suchbegriffen bekommen. Das liegt nicht nur an der Qualität der unterschiedlichen

Algorithmen, sondern auch an der Ausrichtung der Anbieter: Kommerzielle Anbieter wie Google und Bing wollen Geld verdienen und personalisieren und ordnen die Suchergebnisse so, wie es gerade passt. Ein interessanter Artikel zum Thema findet sich hier.

Google Assistant wird zum Übersetzer

Das Wettrennen der Sprachassistenten geht in die nächste Runde. Amazons Alexa (Amazon), Cortana (Microsoft), Siri (Apple), Bixby (Samsung) und der Google Assistant (Google) versuchen sich immer weiter in die Herzen und Haushalte der Anwender zu bringen. Je mehr Funktionen sie haben, desto eher gelingt dies. Auf der CES hat Google jetzt einen weiteren Schritt eingeleitet.

Über die neue Übersetzerfunktion können sich Anwender mit Hilfe des Assistant in zwei Dutzend Sprachen (darunter auch Deutsch) verständigen. Gesprochene Sätze hört der smarte Assistent sich an und gibt sie in der gewünschten Zielsprache wieder.

Ein erster Anwendungsfall findet sich passend zur CES in Las Vegas im dortigen Caesars Palace-Hotel, wo das System an der Rezeption eingesetzt wird und Gäste und Rezeptionisten zusammenbringt.

Google Assistant Connect für Entwickler

Um nicht nur auf eigene Hardware setzen zu müssen, hat Google auf der CES die Plattform Google Assistant Connect vorgestellt. Diese soll die Integration des Assistant in die Hardware anderer Hersteller vereinfachen. Ein Weg, mit dem sowohl Amazon als auch Microsoft gute Erfahrungen gemacht haben, indem sie unter anderem Hersteller wie Harman Kardon und Sonos überzeugten, Lautsprecher mit ihren Sprachassistenten auf den Markt zu bringen.

Aus dem iPad Pro zum Macbook: Brydge Keyboard für neue iPad Pros vorbestellbar

Apple positioniert die neuen iPad Pros, die Ende 2018 erschienen sind, noch mehr als Notebook-Ersatz, als es bisher schon der Fall war. Wer diese Nutzung allerdings ernsthaft anstrebt, der vermisst eine Tastatur, die das iPad bequem und sicher auf dem Schoß balancieren lässt und dazu noch einen verstellbaren Winkel bietet, quasi also aus dem iPad ein Macbook macht. Für die älteren iPads gibt es diese bereits, für das iPad Pro 11 und 12.9 hat können diese seit heute in deutlich überarbeiteter Form beim Hersteller Brydge vorbestellt werden.

Das iPad wird in zwei kleine Halterungen eingelegt, die trotz der geringen Bildschirmränder der neuen iPads das Gerät fest und sicher halten. Die Farbgebung und die Rundungen entsprechen hier 1:1 denen des iPads, sodass das "zugeklappte" Gerät einem Macbook zum Verwechseln ähnlich sieht.

Die Tastatur ist hintergrundbeleuchtet und damit auch im Dunkeln gut lesbar. Vom Tastenweg entspricht sie ersten Testberichten nach der hochgelobten Tastatur der älterern Macbooks.

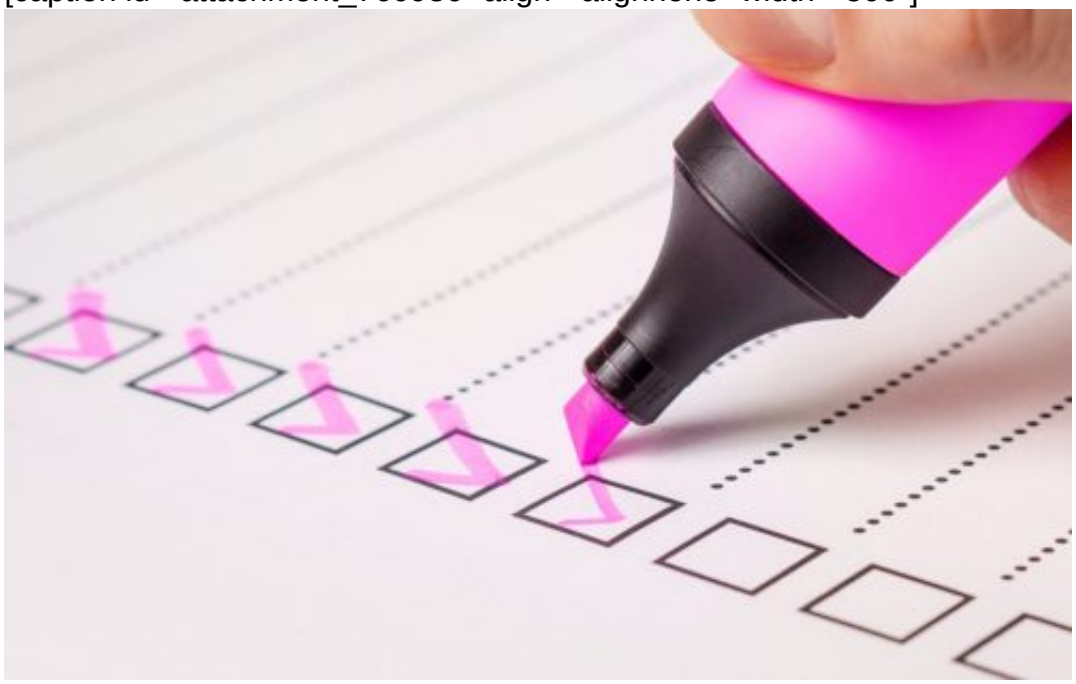
Tablet-Modus und iPad-Schutz

Neu vor allem: Bisher hatten die Brydge-Tastaturen immer einen maximalen Kippwinkel. die neuen Modelle erlauben es, das iPad komplett umzuklappen und so einen "Tablet-Modus" zu nutzen, bei dem das Display oben ist und die Tastatur angebracht, aber versteckt ist.

Ob man es will oder nicht: Brydge liefert dem empfindlichen Rücken des iPads ein magentisches Aluminium-Cover mit, das aber natürlich nicht zwingend verwendet werden muss. Positiv betrachtet: Zusätzlicher Schutz unterwegs kann nicht schaden, vor allem, wenn er nichts kostet.

Autovervollständigung für Formulare in Microsoft Edge einstellen

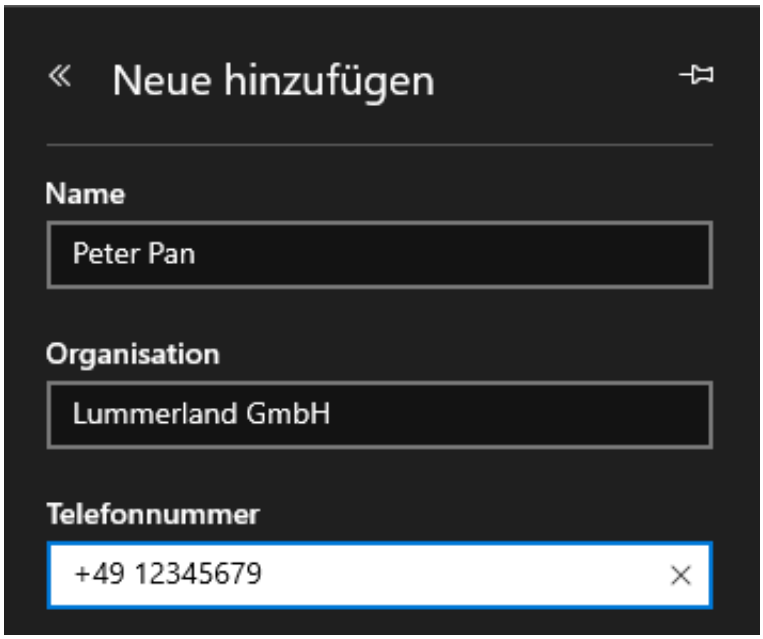
Sie kennen die Situation: Wann immer Sie im Internet etwas bestellen. müssen Sie Ihre Adresse eingeben. Immer und immer und immer wieder, für jede Webseite neu. Der Windows 10-Browser Microsoft Edge kennt Ihre Sorgen und bietet die so genannten Formulare, feste Bausteine, die Sie automatisch füllen lassen können oder gar manuell anlegen können.

[caption id="attachment_760986" align="alignnone" width="500"]

TeroVesalainen / Pixabay[/caption]

Unter **Einstellungen**, **Kennwörter & AutoAusfüllen** können Sie unter **AutoAusfüllen** einschalten, dass Formulardaten gespeichert werden. Edge erkennt dann, wenn Sie Informationen in ein Formular auf einer Webseite eingeben und speichert Ihre Eingaben ab. Fordert eine andere Webseite dann ähnliche Informationen an, dann kann Edge diese automatisch eintragen.

Erstellen manueller Formulare

Wenn sie nicht warten möchten, bis Sie eine Webseite aufrufen, die Ihre Formulardaten abfragt, dann geben Sie diese doch einfach manuell ein: Unter **Formulare verwalten** können Sie nicht nur die bereits gespeicherten ansehen, ändern und löschen, sondern auch ganz neue direkt eingeben!

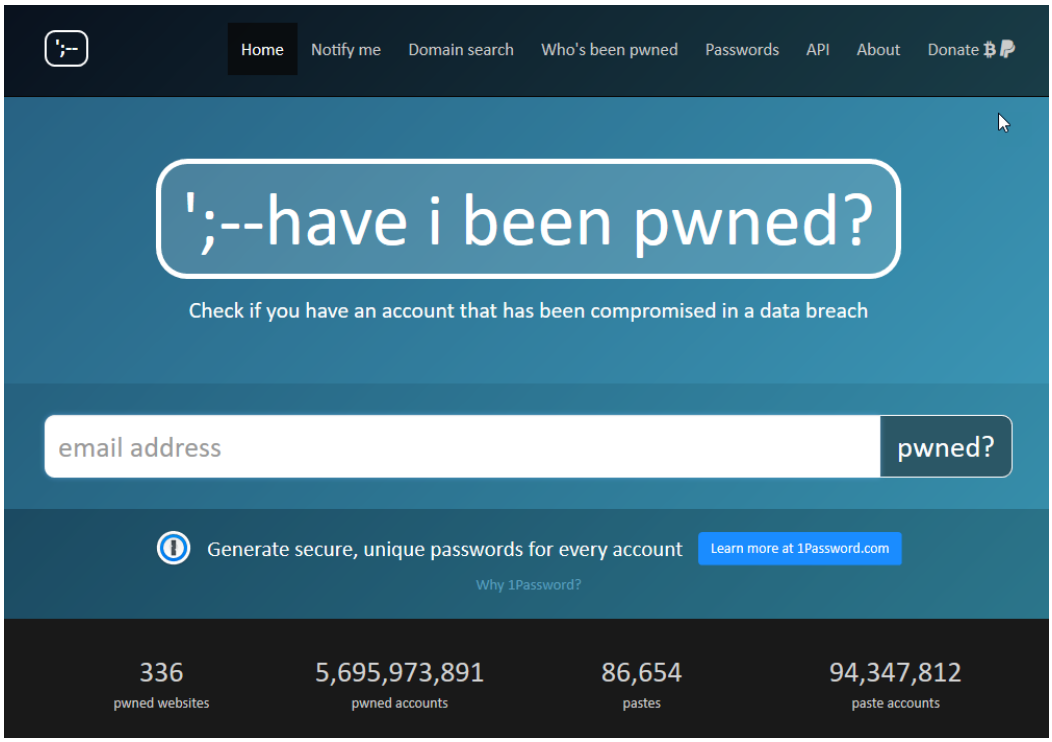


Kreditkarteninformationen finden sich übrigens nicht unter den Formularen, sondern unter Karten speichern. Diese Option finden Sie aber an der selben Stelle in den Einstellungen von Microsoft Edge. Es macht durchaus Sinn, diese auszuschalten!

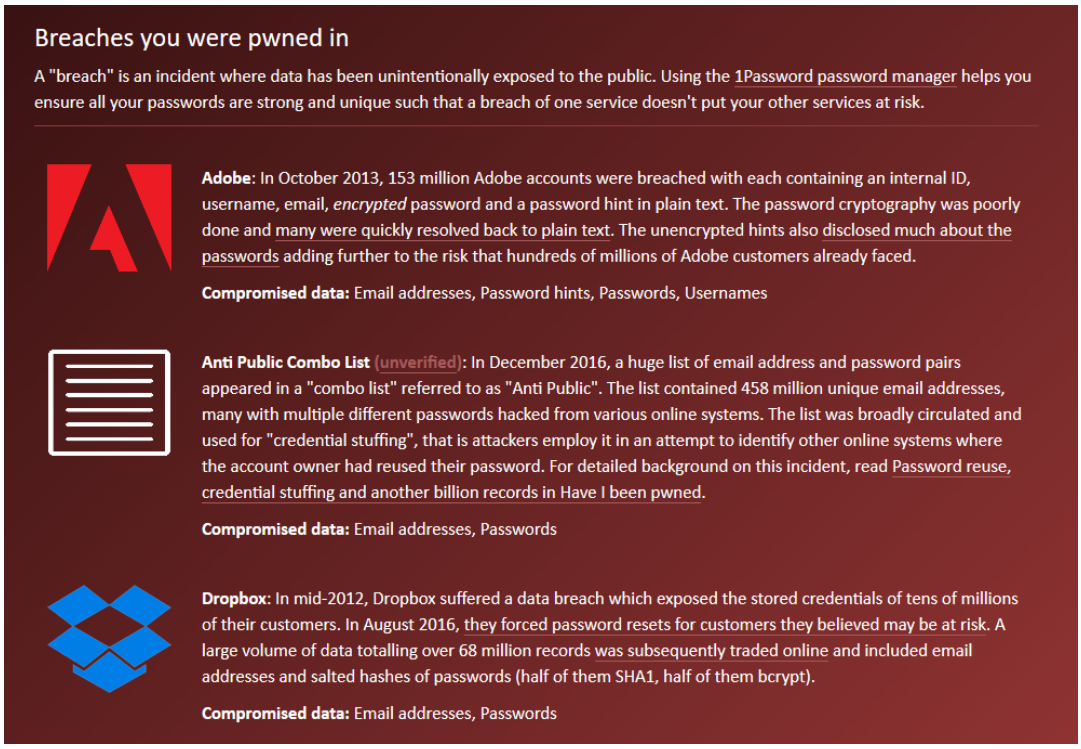
Schnell prüfen, ob der eigene E-Mail-Account kompromittiert wurde

Nicht erst seit dem "Adventkalender" des Hackers G0D, der eine Vielzahl teilweise sehr sensibler Daten vieler Prominenter und Politiker ins Netz gestellt hat, sind viele Anwender besorgt, ob sie vielleicht auch schon mal Ziel eines Angriffes waren. Das lässt sich durchaus herausfinden, denn die Daten der Opfer vieler Hackaktionen sind bekannt. Jeder kann unverbindlich nachschauen, ob er dabei ist.

Es gibt verschiedene Arten, Opfer von Hackaktionen zu werden. Direkt das Ziel zu sein, also ausspioniert zu werden, kommt vor - aber eher selten. Häufiger wird man zum Opfer, weil Hacker sich Zugriff auf Datenbanken von Onlinediensten verschaffen und dort im großen Stil Login-Daten und Passwörter "entwenden".



Die Webseite HaveIBeenPwned.com (zu Deutsch etwa "Bin ich haushoch besiegt worden?") erlaubt die Prüfung, ob die eigene E-Mail-Adresse von einem der bekannten Hacks betroffen war. Zu wünschen ist Ihnen, dass die Anzeige grün bleibt und dies nicht der Fall war. Wenn sie allerdings rot wird, dann tut Eile Not!



Ändern Sie auf allen Webseiten und in allen Systemen, in denen Sie diese E-Mail-Adresse nutzen, schnellstens das Passwort!

Sicherheit kann trügerisch sein

Dass Ihre E-Mail-Adresse hier nicht als betroffen gelistet ist, heißt keinesfalls, dass sie nicht doch irgendwo abgegriffen wurde und jemand das zugehörige Passwort kennt. In sofern: Ändern Sie Ihre Passwörter regelmäßig und in geringem Abstand.

Wenn Sie unsicher sind, wie ein Passwort beschaffen sein sollte, dann ist diese Seite des Bundesamtes für Sicherheit in der Informationstechnik (BSI) genau die richtige. Hier finden Sie viele Empfehlungen rund um ein "sicheres" Passwort.

Hinzufügen einer Kreditkarte für Apple Pay am iPhone

Mit Apple Pay wird eine Kreditkarte quasi ins iPhone hineintransportiert: Für den Bezahlvorgang ist dann nicht mehr die Plastikkarte nötig, sondern nur noch das iPhone. In diesem sind alle Daten der Kreditkarte vorhanden und es überträgt die zur Zahlung nötigen Daten dann kontaktlos an den Kartenleser im Geschäft. Das Hinzufügen einer Kreditkarte ist extrem einfach, ob nun die Kamera des iPhones oder die manuelle Eingabe verwendet wird.

Pay

Füge eine Kredit-, Debit- oder Kundenkarte zu Apple Pay hinzu, um sichere Käufe in Geschäften, Apps und im Internet zu tätigen.

In der iOS-internen Wallet-App kann eine neue Kreditkarte für Apple Pay durch Tippen auf das "+"-Zeichen oben rechts eingeleitet werden. Am einfachsten ist dann ohne Frage die Verwendung der Kamera des iPhones: Nach Auswahl des Herausgebers der Kreditkarte öffnet sich die Kamera-App im Hintergrund und lässt Sie die Kreditkarte scannen. Das iPhone erkennt die Kartennummer und trägt sie dann automatisch ein.

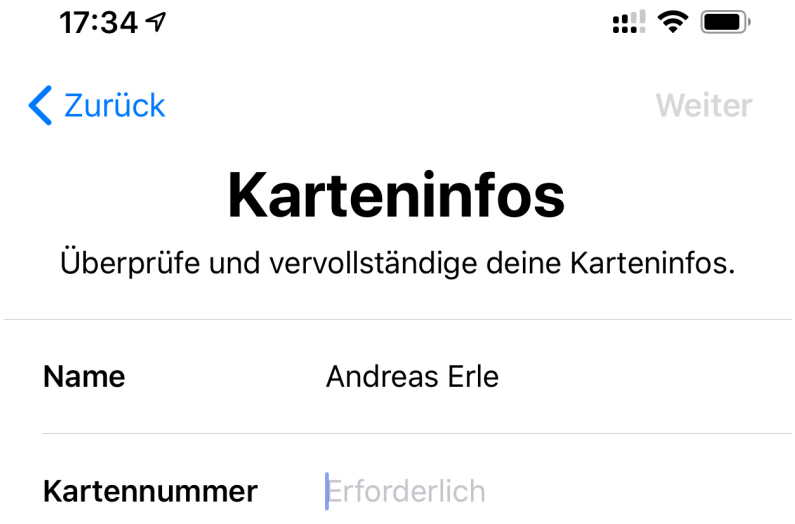
Das Ablaufdatum der Karte muss dann meist manuell eingegeben werden, ebenso die Prüfziffer (die drei- bzw. vierstellige Zahl, die sich meist auf der Rückseite der Karte befindet.

Karte hinzufügen

Richte die Karte im Rahmen aus.

Manuelle Eingabe ist ebenfalls möglich

Wenn das Scannen der Kartennummer nicht automatisch funktioniert (beispielsweise, weil diese sich von der Farbgebung nicht deutlich genug von der Farbe der Karte abhebt), dann können diese Daten auch manuell über die Softtastatur des iPhones eingegeben werden.



Sind die Daten korrekt eingegeben und gespeichert worden, dann kann die neu konfigurierte Karte direkt über Apple Pay genutzt werden.

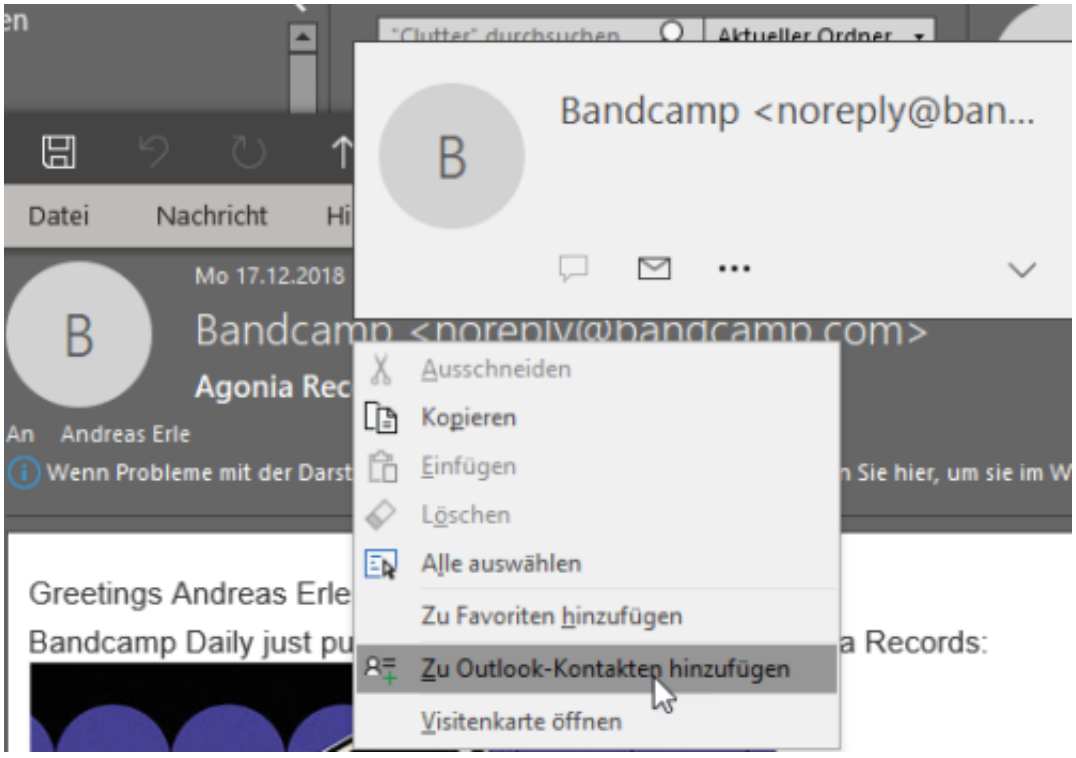
Unbekannten Absender als Outlook-Kontakt anlegen

Die Zahl der E-Mails, die am Tag im Posteingang ankommen, nimmt stetig zu. Keine Frage, viele davon sind SPAM und damit nicht interessant. Neben unerwünschten Werbemails aber kommt durchaus die eine oder andere Nachricht von einem neuen Absender an, die wichtig ist und deren Absender man speichern möchte. Es ist nicht nötig, dies manuell zu machen, Outlook bietet eine schnelle Möglichkeit, einen neuen Kontakt direkt aus der E-Mail heraus anlegen zu lassen.

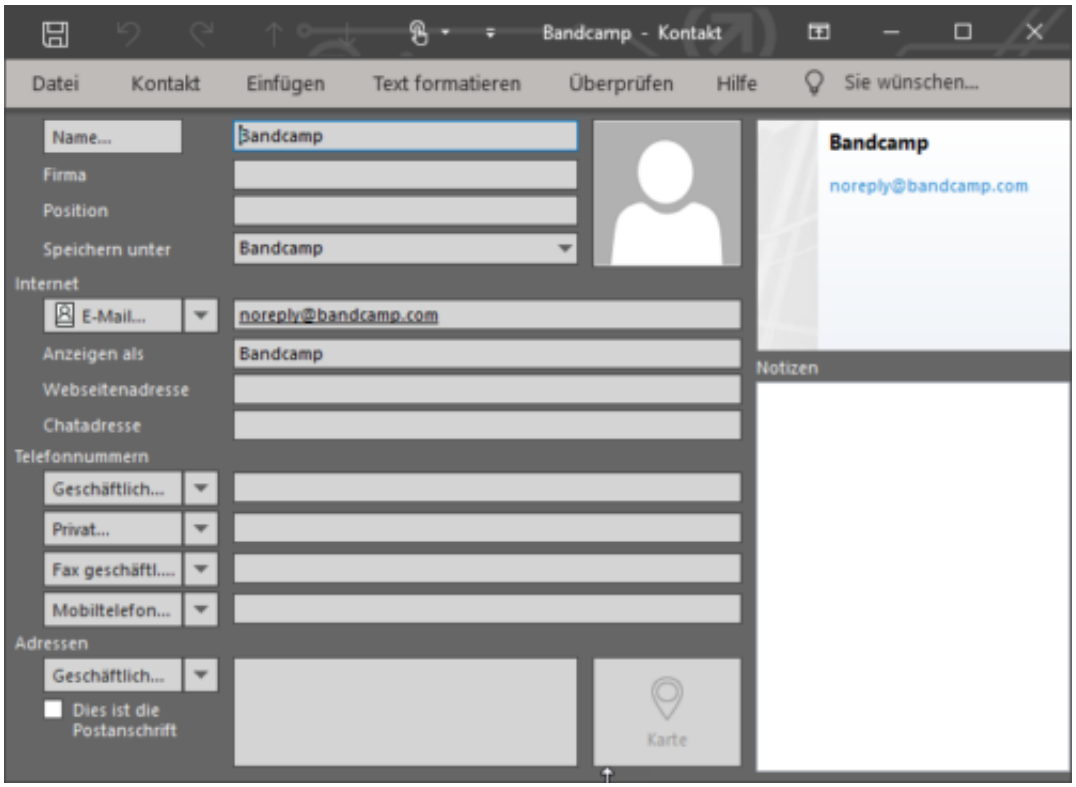
Wichtig ist, dass die E-Mail nicht im Clutter oder in den Junk-Emails steckt, weil Outlook in diesem Fall viele Funktionen per se deaktiviert. Wie Sie eine E-Mail von dort in den Posteingang bekommen, lesen Sie hier.

Aus der Absenderadresse in die Kontakte

Zum Anlegen des Kontaktes klicken Sie mit der rechten Maustaste in die Absenderadresse der E-Mail. Im sich öffnenden Menü klicken Sie dann auf **Zu Outlook-Kontakten hinzufügen**.



Outlook öffnet nun einen neuen Kontakt und trägt die aus der E-Mail zu identifizierenden Felder wie den Namen und die E-Mail-Adresse bereits ein.



Wenn Sie noch weitere Informationen zum Absender haben, tragen Sie diese ein und speichern Sie den Kontakt dann ab.