Schieb Report

Ausgabe 2024.30

Passkeys: Auch auf dem Smartphone sicher

Immer mehr Internetverkehr wandert von PC auf das Smartphone. Klar, schließlich habt ihr das immer dabei und werdet immer mobiler. Android und iOS unterstützen beide die native Verwendung von Passkeys.

Passkeys unter Android

Passkeys auf Android passen sich nahtlos in die ohnehin schon vorhandene Integration aller Google-Dienste ein. Um einen neuen Passkey anzulegen, ruft einfach die Webseite des Dienstes auf und meldet euch an.

Um Passkeys nutzen zu können, müsst ihr den Google-Passwortmanager aktivieren:

- Streicht von oben nach unten über den Bildschirm und tippt dann auf das Zahnrad. Alternativ öffnet sie Einstellungen über die App-Übersicht.

- Der Weg zu den Passworteinstellungen unterscheidet sich zwischen den einzelnen Android-Versionen. Bei Android 14 tippt auf **Passwörter und Konten**.

- Aktiviert dann den Schalter neben **Google**.

Das Anlegen eines neuen Passkeys funktioniert wieder über die Webseite des Anbieters oder Dienstes:

- Entweder findet ihr schon direkt auf dem Anmeldebildschirm die Option, einen Passkey anzulegen, oder sie wird euch nach der Anmeldung angeboten.

- Ist das nicht der Fall, dann sucht sie in eurem Konto unter **Passwörter und Sicherheit**.

- Tippt auf **Weiter**, um den Passkey anzulegen.

- Meldet euch per Fingerabdruck oder Gesichtsscan (je nach Gerät) an eurem Smartphone an.

- Der Passkey wird automatisch gespeichert. Da Google automatisch die Synchronisation mit den Passwörtern im Google-Account aktiviert, findet ihr den neuen Passkey dann unter „Google Passwort Manager“.

-

Passkeys unter iOS

Die Voraussetzung für die Nutzung von Passkeys auf einem iPhone oder iPad sind gering. Ihr benötigt:

- Mindestens iOS/iPadOS 16

- Der iCloud-Schlüsselbund muss aktiviert sein.

- Die Zwei-Faktor-Authentifizierung muss ebenfalls aktiviert sein.

Der iCloud-Schlüsselbund aktiviert ihr so:

- Öffnet die Einstellungen des iPhones.
- Tippt auf euer Kontobild ganz oben, um die iCloud-Einstellungen zu öffnen.
- Tippt auf **iCloud** > **Passwörter & Schlüsselbund**.
- Tippt auf den Schalter neben **iPhone synchronisieren**, wenn dieser nicht bereits aktiviert ist. Der iCloud Schlüsselbund wird aktiviert.

Die Zwei-Faktor-Authentifizierung (bei der ihr bei der Anmeldung mit der Apple ID ein anderes Apple-Gerät oder ein Telefon zum Empfang eines Codes als zweiten Faktor benötigt, aktiviert ihr so:

- Tippt in den iCloud-Einstellungen auf **Anmeldung und Sicherheit**.
- Dann könnt ihr – so das nötig ist – noch die vertrauenswürdigen Nummern bearbeiten.

Das Erzeugen eines Passkeys für eine Webseite oder Dienst wird meist automatisch angestoßen, wenn Passkeys unterstützt werden:

- Meldet euch bei dem Dienst an.
- Dieser fragt euch nach erfolgreicher Anmeldung, ob ihr einen Passkey erzeugen wollt, wenn das bis jetzt nicht geschehen ist, bestätigt das.
- Das iPhone fordert euch nun auf, euch mit Gesichtserkennung, Fingerabdruck oder PIN anzumelden, um eure Identität zu bestätigen.

- Habt ihr das erfolgreich gemacht, dann wird der Passkey auf dem iPhone gespeichert und lässt sich bei den folgenden Anmeldungen direkt nutzen.

- Bietet die Seite das Anlegen eines Passkeys nicht direkt an, dann hilft es oft, in den Kontoeinstellungen nachzusehen und dann – wie oben am Beispiel Google beschrieben – die Erstellung des Passkeys manuell zu starten.

- Die Passkeys findet ihr wie die Passwörter unter **Einstellungen** > **Passwörter** unter der jeweiligen Webseite. Dort könnt ihr sie auch entfernen, wenn sie nicht mehr benötigt werden.

Wenn Outlook falsche Temperaturen anzeigt

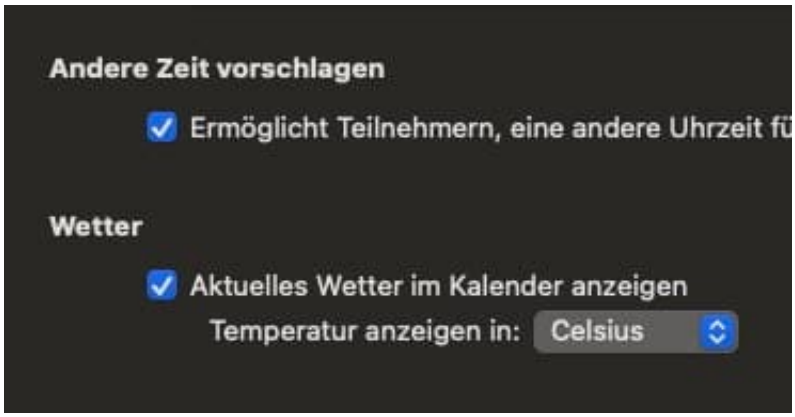
Ihr habt einen Termin draußen und seid euch unsicher, was ihr anziehen sollt. Spart euch die Wetterapp, Outlook kann euch da ebenfalls helfen. Und das sogar direkt bei den Terminen!

Aktivieren von Wetter in Outlook

Outlook hat nun auf den ersten Blick nichts mit der Wettervorhersage zu tun, allerdings hat es natürlich als Microsoft-Programm Zugriff auf viele Windows-Funktionen, so auch die Wetter-App. Und was da funktioniert, lässt sich schnell auch auf andere Betriebssysteme spiegeln. Die aktuellen Outlook-Versionen unterstützen durch die Bank weg die Anzeige des aktuellen Wetters am Datum

eines Termins. So aktiviert ihr es:

- Geht auf dem Gerät eurer Wahl in die Einstellungen von Outlook, dann klickt in der Seitenleiste auf **Kalender**.
- Aktiviert die Option **Wetter** bzw. **Aktuelles Wetter im Kalender anzeigen**.
- Startet Outlook neu.
- Die mobilen Versionen von Outlook verwenden automatisch immer die aktuelle Position des Gerätes für die Wettervorhersage.
- In den Desktop-Versionen klickt einfach auf die Wetterleiste über der Terminübersicht und legt dort Orte an, für die ihr das Wetter angezeigt haben möchtet. Die Option der automatischen Ortsbestimmung per GPS gibt es da auch, die wird aber bei einem stationären Gerät eher weniger gewünscht sein.



Wenn die Temperatur in Fahrenheit ist

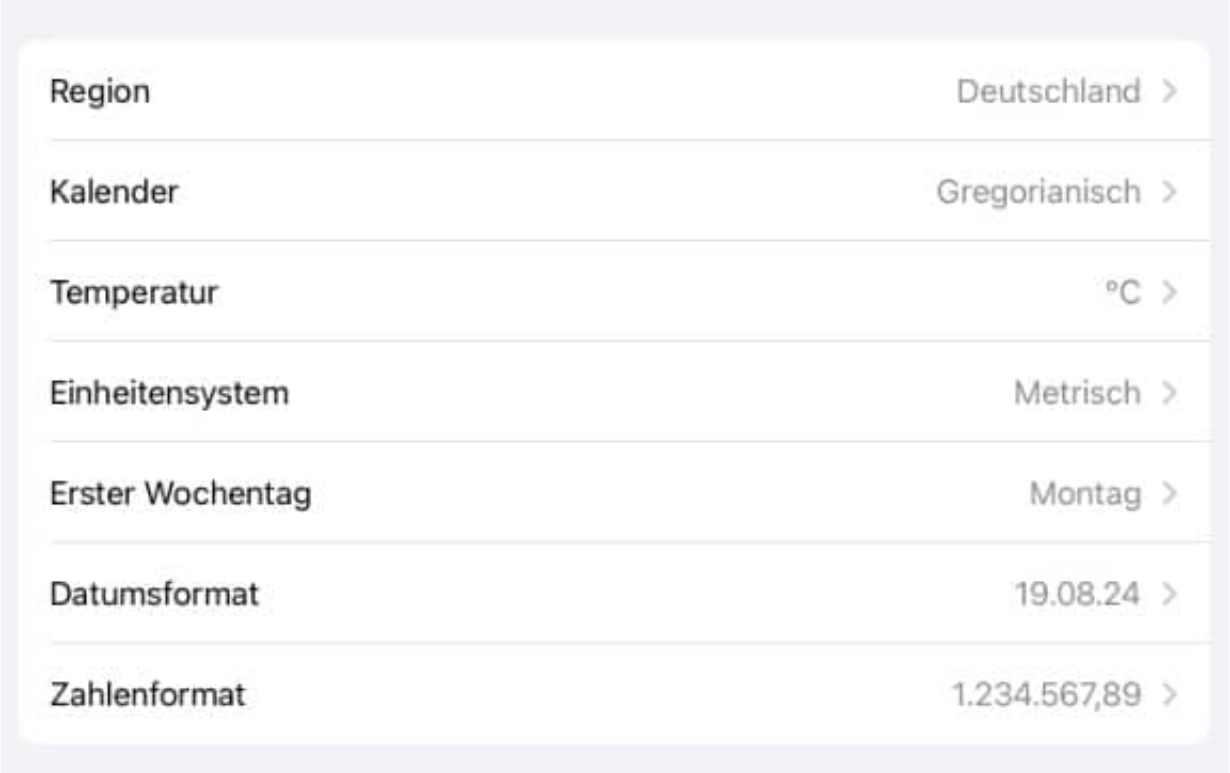
Ein besonders ungünstiger Fehler ist die Anzeige der falschen Einheit für die Temperatur: Alle Versionen von Outlook unterstützen sowohl Celsius (was in unseren Breitengraden gebräuchlich ist) als auch Fahrenheit. Letzteres lässt sich nicht so einfach in Celsius umrechnen. Wenn die Temperatur also ein F hintenan gestellt hat und unlogisch erscheint, dann korrigiert das:

- Geht auf dem Gerät eurer Wahl in die Einstellungen von Outlook, dann klickt in der Seitenleiste auf **Kalender**.
- Wählt in der Auswahlliste **Celsius** als Einheit aus.
- Bei einem iPhone oder iPad kann das ein wenig kniffliger sein: iOS verwendet im Standard die Systemeinstellung für die Einheiten, die unter anderem auch die Temperatureinheit beinhaltet.

- Manchmal geht die Übergabe von den Einstellungen an die nutzenden Apps schief. Dann ist zwar "eigentlich" Celsius eingestellt, die Apps zeigen aber trotzdem Fahrenheit an.

- Geht dann in die Einstellungen von iOS, auf **Allgemein** > **Sprache & Region**.

- Tippt auf **Temperatur**, dann wählt einmal **F** aus, tippt noch einmal auf Temperatur und dann wählt wieder **C**elsius aus. Startet dann auch die App, die die falsche Temperatureinheit angezeigt hat, neu!



Digitales Geld: Sicherer als Bargeld?

Wir bezahlen immer häufiger mit dem Smartphone, manche investieren sogar in Kryptowährungen. Da stellt sich die Frage: Ist das digitale Geld auch sicher?

Deutsche sind keine Bargeldzahler mehr

Lange Zeit waren wir Deutschen ein Volk der Bargeldzahler. Überall um uns herum haben die Menschen an den Kassen Kreditkarten und Smartphones gezückt, wir haben aber lieber mit Bargeld gezahlt.

Das hat sich erst nach und nach und sehr allmählich geändert. Doch mit Corona kam der Switch: Plötzlich haben selbst Bäckereien und Marktstände bargeldloses Bezahlen akzeptiert – und die Deutschen haben angefangen, selbst kleine Beträge mit Karte oder Smartphone zu begleichen.

In der Online-Welt herrschen sowieso Zahlmethoden wie Paypal vor. Und mit Wero haben einige europäische Banken nun sogar eine Konkurrenz zu Paypal auf den Weg gebracht.

Und wer Geld anlegen will, der macht das heute oft auch in Kryptowährungen, allen voran Bitcoin. Die Welt des Geldes ist digital geworden: Wir nehmen kaum noch Papier und Münzen in die Hand. Wie sieht das bei Euch aus?

Vielleicht stellt Ihr Euch auch die Frage: Bequem ist dieses digitale Geld ja auf jeden Fall. Aber wie sieht es eigentlich mit der Sicherheit aus? Ist Bargeld sicherer als digitales Geld, oder eher umgekehrt? Wenn ich meine Brieftasche verliere, ist das Bargeld darin weg. Digitales Geld kann man aber auch verlieren: durch Hackattacken oder Betrügereien.

Bargeld lacht: Auch in Deutschland wird Bargeld allmählich unwichtiger

Was ist sicherer: Bargeld oder digitales Geld?

Wie so oft im Leben lassen sich solche Fragen nicht eindeutig mit A oder B beantworten. Beide Geldsysteme haben ihre klaren Vor- und Nachteile, auch individuelle Risiken. Bargeld kann ich verlieren oder es kann geklaut werden, doch in digitale Wallets – also Konten oder Brieftaschen – können Hacker eindringen und mich beklauen oder betrügen.

Es gibt diverse Studien, die die Sicherheit von Bargeld und digitalen Zahlsystemen untersucht haben. Eine Studie der Deutschen Bundesbank zum Beispiel zeigt, dass der direkte Bargelddiebstahl in Deutschland rückläufig ist. Nur etwa 0,3% der Befragten gaben an, in den letzten 12 Monaten Opfer eines Bargelddiebstahls geworden zu sein.

Im Gegensatz dazu nahmen Betrugsdelikte im Bereich des digitalen Zahlungsverkehrs zu. Laut dem Bundeskriminalamt (BKA) stieg die Zahl der erfassten Fälle von Cybercrime im Jahr 2020 um 7,9% im Vergleich zum Vorjahr.

Du siehst: Die Frage lässt sich nicht einfach oder eindeutig beantworten, wir müssen also differenzieren und genauer hinschauen.

Die Unterschiede der Zahlungssysteme

Und das wollen wir auch machen. Fangen wir doch mal mit der generellen Frage an: Wo liegen die prinzipiellen Vor- und Nachteile von Bargeld und digitalen Zahlsystemen?

Bargeld zum Beispiel hat eindeutige Vorteile: Es ist greifbar, man kann es fühlen, unter das Kopfkissen packen, verstecken oder bei sich führen. Bargeld ist von keiner Technologie abhängig. Bargeld ist anonym nutzbar, kann nicht gehackt werden.

Bargeld kann aber gestohlen werden oder verloren gehen. Das haben wir doch alle schon erlebt. Und weil es anonym ist, kann ich nie beweisen, den 100er, den Du da gerade in der Hand hältst ist der, den ich gerade verloren habe.

Auch ist Bargeld unpraktisch: Große Summen will man nicht mit Bargeld bezahlen, und viel Kleingeld beult das Portemonnaie aus.

Digitales Geld – ist eindeutig bequem und praktisch im Alltag. Ich kann nachvollziehen, wann ich was an wen bezahlt habe. Manchmal sind digitale Zahlungssysteme sogar vom Anbieter abgesichert. Also transparenter und sicherer als Bargeld.

Doch dafür sind digitale Zahlungssysteme anfällig für Hack-Angriffe. Heerscharen von Hackern und Betrügern stürzen sich drauf und versuchen uns zu beklauen: Bankkonto, Paypal, Kryptowährungen. Kein System ist 100% sicher.

Außerdem ist man abhängig von funktionierender Technologie: Wenn Zahl-Terminals im großen Stil ausfallen – das hatten wir schon –, stehen wir da.

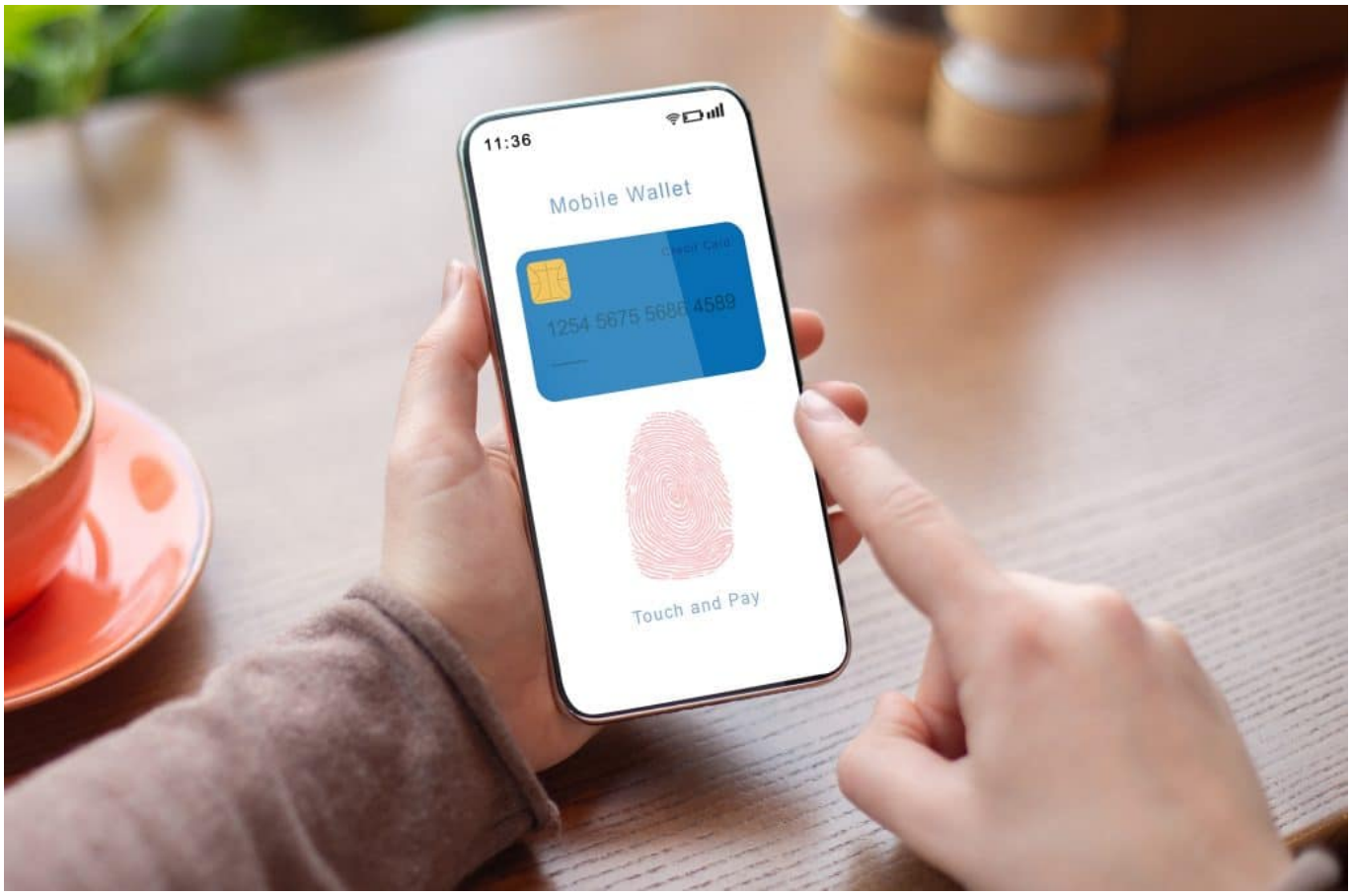
Diese Risiken drohen beim digitalen Geld

Die Zahlen für echten Bargelddiebstahl gehen zurück. Wie sieht es denn in der Welt der digitalen Bezahlung aus: Welche Risiken drohen hier konkret – kann sich jemand meinen Apple Pay oder Google Pay Account schnappen und damit bezahlen?

Google Pay und Apple Pay sind sehr gut abgesicherte Zahlsysteme. Eine Studie von „Javelin Strategy & Research“ aus 2021 hat gezeigt: Nur 2% der Identitätsdiebstähle betrafen mobile Wallets wie Apple Pay oder Google Pay. Im Vergleich dazu waren 40% der Fälle mit Kreditkartenbetrug verbunden

Es ist also klug, seine Kreditkarte zu Hause zu lassen und sie lieber bei Apple Pay oder Google Pay zu hinterlegen. Denn man muss sagen: Beide Systeme verfügen über eine hervorragende Absicherung. Die Zahlvorgänge erfolgen token-basiert und verschlüsselt, das bedeutet, niemals werden Kreditkartendaten oder persönliche Daten übertragen. Da lässt sich auch nichts ausspionieren, etwa mit einem manipulierten Lesegerät. Unmöglich.

Einziges Risiko: Jemand stiehlt mein Smartphone oder die Watch, mit manchen Smartwatches kann man auch mit einer digitalen Wallet bezahlen. Aber hier gibt es meist eine doppelte Absicherung: Einmal beim Freischalten des Smartphones, und dann noch mal beim Öffnen der Wallet. Man müsste also die PIN kennen und/oder den Gesichts- oder Fingerabdruck-Scan überlisten. Das ist sehr schwer.



Per Fingerabdruck im Smartphone anmeden

Betrug per Skimming

Einige erinnern sich vielleicht, dass mal davor gewarnt wurde, dass Betrüger mit einem Lesegerät nah an mein Smartphone oder Karten kommen und sie so auslesen oder sogar belasten könnten…

Das gibt es tatsächlich und wird „Skimming“ genannt. Durch NFC (Near Field Communications) nimmt ein Smartphone Kontakt zu einem Lesegerät auf und tauscht Daten aus. Doch durch die enorm aufwändige Verschlüsselung durch Google und Apple Pay und die Datensparsamkeit ist es bislang nicht gelungen, diese Zahlsysteme auf diese Weise austricksen. Das funktioniert nur bei

schlechter abgesicherten Zahlsystemen.

Wie sicher ist Paypal eigentlich?

Wir müssen wir wohl auch mal über Paypal sprechen. Es soll rund 33 Mio. aktive Paypal-Konten in Deutschland geben. Wie sicher oder unsicher ist Paypal?

Paypal-Nutzer sind durchaus gefährdet, denn da Paypal so weit verbreitet ist, versuchen auch viele Betrüger hier erfolgreich zu sein. Ich möchte vorweg schicken, dass die Absicherungsmechanismen bei Paypal, aber auch bei Kreditkarten viel besser geworden ist. Nutzer müssen bei praktisch allen Kreditkarten bei relevanten Belastungen einen zweiten Faktor eingeben, selbst wenn sie über Paypal bezahlen. Man kennt das: Da meldet sich dann die Bank oder Kreditkartenfirma, und sendet eine SMS oder erwartet, dass man in der Banking App – die auch nochmal abgesichert ist – den Zahlvorgang bestätigt.

Das macht Paypal heute deutlich sicherer als noch vor wenigen Jahren.

Trotzdem ist Paypal nicht komplett sicher: Betrüger versuchen durch Phishing-Mails, die aussehen wie die von Paypal, Opfern die Zugangsdaten zu entlocken. Wenn sie dann so ins Paypal-Konto kommen, können sie zumindest schon mal das aktuelle Guthaben ausgeben. Mit weiteren Tricksereien können sie es auch auf ein anderes Konto überweisen oder Lastschriften erzeugen.

Das Risiko lässt sich aber deutlich reduzieren, indem man auch bei Paypal selbst die Zwei-Faktor-Authentifizierung aktiviert. Das ist nicht standardmäßig der Fall. Einfach aktivieren – dann muss man beim Login auf einem neuen Geräten einen

weiteren Code eingeben, entweder per SMS oder im Smartphone zu erzeugen. Das erhöht die Sicherheit enorm.

Paypal ist beliebtes Ziel für Phishing-Attacken

Keine Angaben zu Betrugsfällen

Wie oft kommt es denn die Betrugsfällen bei Paypal, Google und Apple Pay?

Leider machen die Unternehmen dazu keine konkreten Angaben. Es gibt nur wenige offizielle Studien, die den digitalen Zahlsystemen aber ein vergleichsweise geringes Risiko zusprechen, wie etwa die „Bank of international Settlements“. Deutlich weniger als beim Bargeld. Allerdings weise eine Studie von McKinsey auf die Risiken durch Phishing und Malware hin.

Sicherheit von Bitcoin und Bitcoin Wallets

Kommen wir noch zu einem anderen Aspekt: Gespartes Geld. Sparbuch oder zum Beispiel Bitcoin, wer sich darauf einlassen will. Mir ist das schon passiert: Geldbörse im Restaurant liegengelassen. Weg. Bargeld kann ich verlieren. Bitcoin auch?

Sagen wir mal so: Das hängt davon ab, wo ich meine Bitcoin lagere. Ich kann sie in einem Konto lagern, bei einem Verwahrer sozusagen, der meine Bitcoin für mich verwahrt. Das ist vergleichsweise sicher.

Man kann seine Bitcoin aber auch auf einer externen Festplatte speichern – oder einer speziellen „Wallet“, ein kleines Gerät, das mir sogar anzeigt, wie viel Bitcoin darin gespeichert sind. Wenn ich die verliere, die Festplatte oder die Hardware-Wallet, sind die Bitcoin futsch – wie beim Bargeld, auf das ich nicht aufpasse.

Es kommt aber noch was dazu: Wenn ich meinen Schlüssel zur Wallet verliere, mein Passwort vergesse zB, dann sind der Bitcoin da, aber ich komme nicht dran. Ich kenne jemanden, der hat in den Anfangszeiten des Bitcoins, als der noch 1 EUR gekostet hat, Hunderte, Tausende von Bitcoin auf einer externen Festplatte gespeichert – und kommt nicht dran, weil er das Passwort nicht mehr weiß. Das hätte heute einen Wert von etlichen Mio. EUR. Das kann einem mit Bargeld und Aktien nicht passieren.

Sicherheit von Bitcoin und Co.

Bitcoin und andere Kryptowährungen sind also sicher. Man hört und liest doch aber auch immer wieder, dass Bitcoin geklaut werden – und sogar im großen Stil.

Die Sicherheit von Bitcoin und anderen Kryptowährungen hängt hauptsächlich von der sicheren Verwahrung der privaten Schlüssel ab, die den Zugriff auf die einzelnen digitalen „Coins“ ermöglichen. Meist ist das ein Passwort, technisch ein digitaler Schlüssel.

Es gibt bei Kryptowährungen verschiedene Risiken. Wenn sich jemand Zugriff auf die privaten Schlüssel eines Benutzers verschafft, kann er die damit verbundenen Bitcoins stehlen. Das kann passieren, wenn Benutzer ihre Schlüssel nicht sicher aufbewahren, z.B. auf einem mit dem Internet verbundenen Computer oder in einem unverschlüsselten Format.

Es gibt aber auch betrügerische Börsen: Einige Benutzer verlieren ihre Bitcoins durch betrügerische Kryptowährungsbörsen. Diese Plattformen geben vor, seriös und legitim zu sein, aber plötzlich schließen und mit den Geldern der Benutzer verschwinden, wie im Fall von Mt. Gox im Jahr 2014.

Betrüger können aber auch versuchen, Benutzer dazu zu bringen, ihre privaten Schlüssel oder Anmeldedaten für Kryptowährungsbörsen preiszugeben, indem sie gefälschte Websites oder E-Mails verwenden (etwa durch Phishing). Es gibt auch Malware, die speziell entwickelt wurde, um Kryptowährungen von infizierten Computern zu stehlen.

Es gibt also diverse Betrugsmaschen. Da wo Geld ist, sind auch Betrüger.

Manchmal ist Bargeld Trumpf

Ich habe immer Bargeld dabei, aber nicht mehr so viel wie früher. Für Trinkgelder oder kleinere Ausgaben. Ansonsten bezahle ich mit dem Smartphone, per Apple Pay zum Beispiel. Damit habe ich gute Erfahrungen gemacht. Ich lasse die echten Kreditkarten in der Regel zu Hause; man braucht sie fast nicht mehr. Dasselbe gilt für EC-Karten, außer zum Abheben von Bargeld.

Aber trotzdem wachsam sein: Es vergeht kein Tag, an dem ich keine Mail, WhatsApp Nachricht oder SMS erhalte, die auf die ein oder andere Weise versucht, mich auszutricksen. Angeblich hätte ich etwas zu viel bezahlt, oder mein Konto würde gesperrt, wenn ich nicht sofort reagiere. So was.

Aber das sind alles Versucht, mich auf Fake-Seiten zu lotsen oder mir Malware unterzujubeln, die vielleicht meine 2-Faktor-Authentifizierung mitlesen will. Man sollte also dennoch immer vorsichtig und umsichtig sein.

Studien

Deutsche Bundesbank:
https://www.bundesbank.de/de/presse/pressenotizen/zahlungsverhalten-in-deutschland-2021-894082

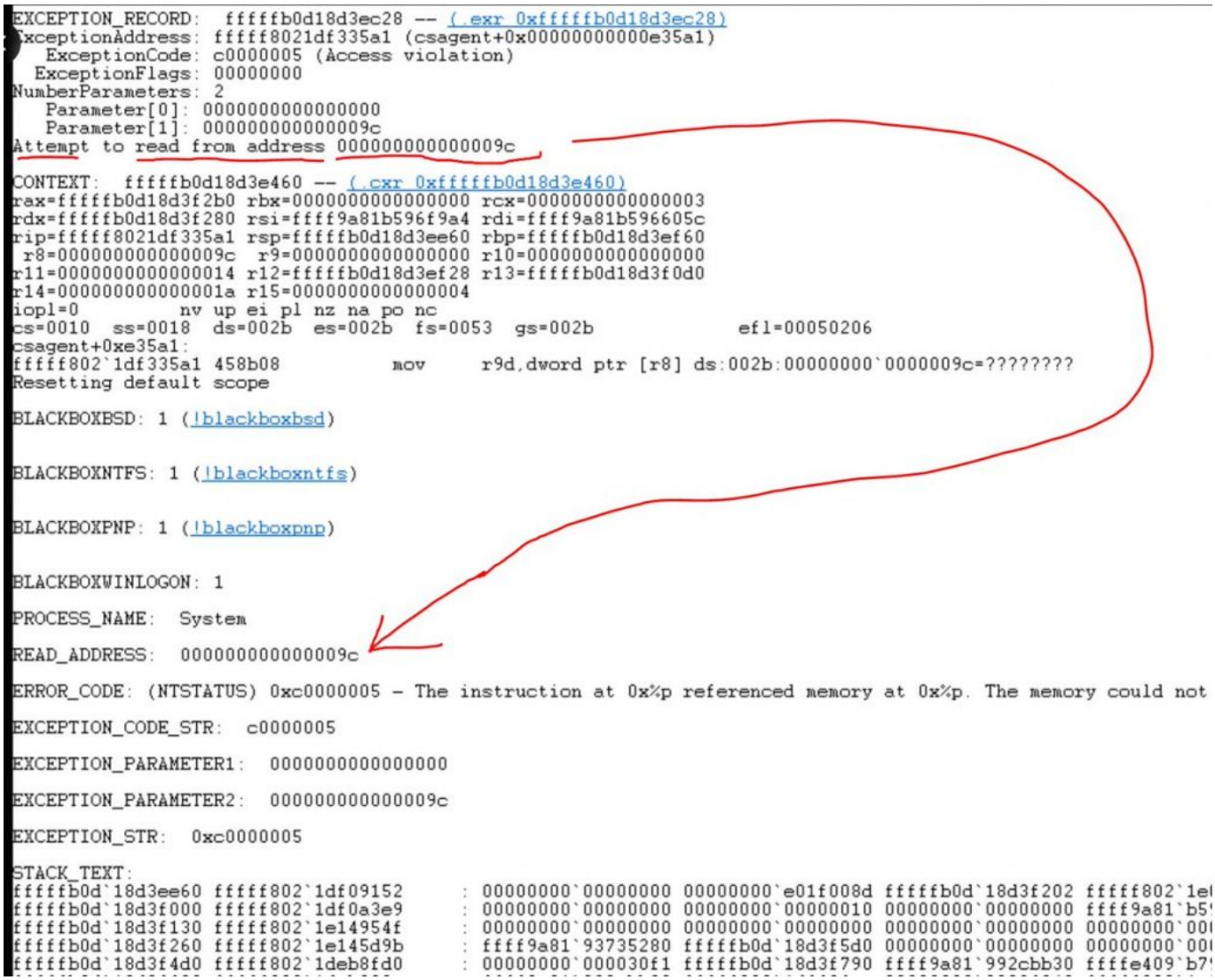
McKinsey: Sicherheit von digitalen Zahlungsmitteln
https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/consumer-trends-in-digital-payments

Digital payments make gains but cash remains
https://www.bis.org/statistics/payment_stats/commentary2301.htm

Gründe für den globalen IT-Ausfall

Weltweit sind Windows-Rechner ausgefallen: Ein zeitgleich an unzählige Rechner verteiltes fehlerhaftes Update hat das Chaos verursacht. Hier die genauen Hintergründe und Ursachen.

Grund für die massenhaften Ausfälle waren nach bisherigen Erkenntnissen keine Fehler in Windows – auch wenn die auf den betroffenen Rechner angezeigte Fehlerseite das vermuten lässt –, auch nicht in der Infrastruktur von Microsoft. Lahmgelegt hat die Rechner ein „Falcon Sensor“ genanntes Sicherheitssystem des auf IT-Sicherheit spezialisierten Unternehmens CrowdStrike.



Das genau ist der technische Fehler, der zum Chaos führte

Eine Art Virenschutz ist Ursache des Problems

Man darf sich den „Falcon Sensor“ wie eine Art Deluxe-Version einer ganz normalen Antiviren-Software vorstellen: Ein Schutzsystem, das Rechner vor Bedrohungen aus dem Netz, aber auch auf dem Rechner beschützt. Mit dem Unterschied allerdings, dass es sich um eine hoch professionelle Anwendung handelt, die eine kontinuierliche Überwachung vor Eindringlingen, Hackangriffen, Viren und Würmern bietet.

Vor allem größere Unternehmen, Betriebe und Institutionen setzen „Falcon Sensor“ von einem Unternehmen namens CrowdStrike ein, um ihre IT-Infrastruktur und auch die einzelnen Geräte im Netz vor Bedrohungen jeder Art zu schützen. Es gibt noch andere Hersteller, die ähnliche Lösungen anbieten – die Software von CrowdStrike ist weit verbreitet.

Keine Privatleute betroffen

Allerdings setzt kein Privathaushalt eine solche Lösung ein – das wäre überdimensioniert und auch viel zu kostspielig. Das ist auch schon der Grund, weshalb – zumindest in diesem Fall! – keine Privatleute betroffen waren, sondern nur Unternehmen. Insbesondere solche, die sich aus gutem Grund mit einer eigentlich hochwertigen Anwendung vor Bedrohungen schützen.

Diesmal jedoch war also der eigentliche Schutz das Problem: Schutzsysteme wie „Falcon Sensor“ versorgen ihre Kundschaft regelmäßig, mitunter sogar mehrmals am Tag, vollkommen automatisch mit Updates, etwa um Rechner und Systeme vor neuen bekannt gewordenen Bedrohungen zu schützen. Bei einem solchen Update wurde ein folgenreicher Fehler gemacht: Ungezählte Rechner überall auf der Welt wurden lahmgelegt.

Nur Windiws-Rechner betroffen

Reset aufwändiger als gedacht

Weil die Windows-PCs sofort abgestürzt sind und selbst ein Neustart (Reboot) keine Lösung gebracht hat, konnten auch keine Korrekturen vorgenommen werden – erst recht lassen sich in einem solchen Fall nicht automatisiert Updates einspielen, die alle Probleme lösen.

Es ist aufwändig, denn nun muss jeder betroffen Rechner manuell im „Safe Modus“ gestartet, einige Dateien entfernt und dann ein Update geladen werden, damit alles wieder läuft.

Domino-Effekt durch globale Vernetzung

Der Fall zeigt allerdings auch, wie zerbrechlich die Welt heute durch die zunehmende Digitalisierung ist: Moderne Software und auch Cloud-Anwendungen sind oft unsichtbar mit unzähligen anderen Komponenten, Programmen, Bibliotheken und Cloud-Diensten verknüpft. Fällt eine aus oder ist sogar gestört, entsteht ein unheilvoller Domino-Effekt.

In diesem Fall war die Ursache schnell gefunden. Es gibt aber vergleichbare Fälle, da muss erst nach der Ursache gefahndet werden. Manchmal ist eine „Bibliothek“, ein kleines Programm mit nützlichen Funktionen das Problem, das unzählige Unternehmen wie selbstverständlich einsetzen.

Domino-Effekt durch globale Vernetzung

Es mangelt an entsprechender Transparenz und Dokumentation. Jeder, der Software einsetzt (zumindest in Unternehmen), müsste sofort wissen, welche Komponenten in der Software enthalten sind.

Und noch etwas ist wichtig: Der aktuelle Fall zeigt, dass auch Infrastruktur von solchen Ausfällen betroffen sein kann. Es braucht Resilienz: Notfallsysteme, die im Fall der Fälle anspringen, um wenigstens eine Basisfunktionalität bieten zu können, bis das eigentliche System repariert ist. Das ist allerdings kostspielig, angesichts der zunehmenden Digitalisierung und Verzahnung unerlässlich.