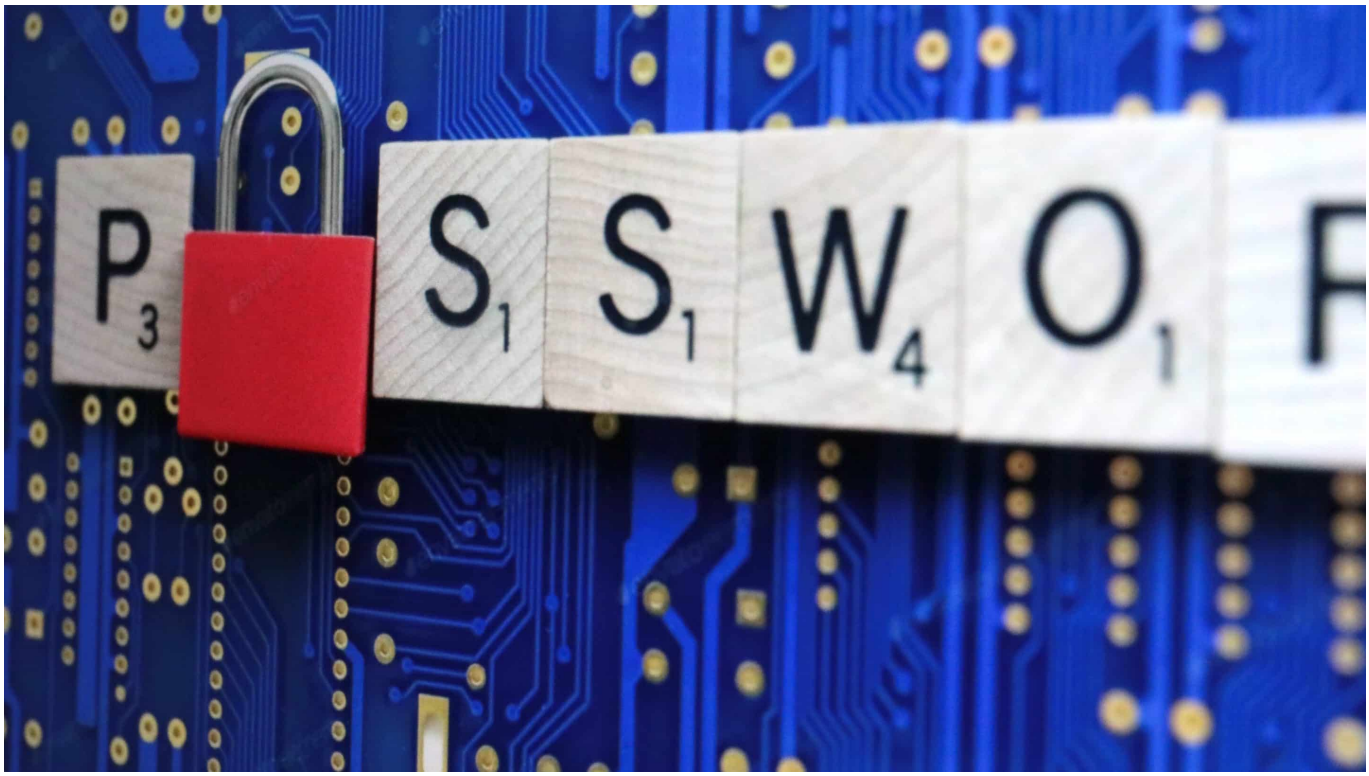
Schieb Report

Ausgabe 2024.18

Briten verbieten leicht zu knackende Default-Passwörter wie "passwort"



Hacker sind wie Einbrecher: Sie nehmen sich die Objekte vor, bei denen es besonders einfach ist. Großbritannien verbietet jetzt schlichte Default-Passwörter in vernetzten Geräten.

Hintergrund: Viele Hersteller liefern ihre Geräte mit Standardpasswörtern wie „admin“ oder „12345“ an alle Kunden aus. Das stellt ein erhebliches Sicherheitsrisiko dar.

Default-Passwörter in ausgelieferter Hardware stellen aus mehreren Gründen ein großes Sicherheitsrisiko dar:

-

1. Leichte Angreifbarkeit: Default-Passwörter sind oft einfach zu erraten oder werden sogar in Handbüchern oder online veröffentlicht. Hacker können so leicht auf das Gerät zugreifen und sensible Daten stehlen oder das Gerät für Angriffe missbrauchen.

2. Weite Verbreitung: Da viele Geräte eines Modells das gleiche Default-Passwort haben, können Angreifer mit einem kompromittierten Passwort potenziell auf Tausende Geräte zugreifen. Das ermöglicht großflächige Angriffe.

3. Mangelndes Sicherheitsbewusstsein: Viele Nutzer ändern Default-Passwörter nicht, weil sie sich der Risiken nicht bewusst sind oder es als zu umständlich empfinden. Die Passwörter bleiben dann ein permanentes Einfallstor.

4. Gefährdung ganzer Netzwerke: Unverändertes Default-Passwörter gefährden nicht nur das einzelne Gerät, sondern oftmals ganze Netzwerke, in die das Gerät eingebunden ist. Hacker können sich so lateral im Netzwerk bewegen.

5. Rechtliche Haftung: Bleiben Default-Credentials unverändert, kann das rechtliche und finanzielle Folgen haben, wenn es zu einem Angriff oder Datenleck kommt. Unternehmen verstoßen so gegen Compliance-Vorgaben.

Lästig: Passwörter sind leicht angreifbar und die guten schwer zu merken

Es ist daher unerlässlich, dass Hersteller ihre Kunden prominent auf die Notwendigkeit einer sofortigen Passwortänderung hinweisen. Idealerweise sollten Geräte Nutzer bei Inbetriebnahme zu einer Änderung zwingen.

Machen die Hersteller aber nicht. Die Folge: Viel zu viele Geräte wie Router, WLAN-Access-Points, Haushaltsgeräte, Smart-TV oder Rauchmelder lassen sich von Hackern leicht knacken.

Rund 12.000 Attacke in einer Woche

Die meisten installieren Geräte oder stellen sie auf – und denken dann nieder

daran. Die unbemerkten Angriffe auf die Geräte aus dem Netz realisiert niemand.

Die britische Verbraucherschutzorganisation „Which?“ hat bei einer einwöchigen Messung eines Test-Haushalts 12.000 Attacken auf Smarthome-Geräte gemessen. Ganze 2.500 Mal wurde dabei versucht, die zumeist schwachen Passwörter der Geräte zu „erraten“.

Die Angriffe sind real, der Widerstand der vernetzten Geräte niedrig. Viele Hersteller haben es sich und den Konsumenten in der Vergangenheit zu leicht gemacht: Sie haben ihre Geräte mit einem Standardpasswort wie „admin“, „passwort“ oder „12345“ ausgeliefert.

Das Passwort steht im Handbuch und die Geräte müssen nicht aufwändig mit unterschiedlichen Passwörtern konfiguriert ausgeliefert werden, die man auch noch dem Kunden mitteilen muss.

Selbst der Wechsel eines Passwortes macht keinen Unterschied

Standard-Passwort erhebliches Sicherheitsrisiko

Doch alle Geräte eines Herstellers oder Modells im Auslieferungszustand mit demselben Passwort auszustatten, ist ein enormes Sicherheitsrisiko.

Denn die meisten Kunden machen sich nicht die Mühe, das voreingestellte Passwort zu ändern. Warum auch: Das Gerät funktioniert schließlich – und ein Standardpasswort gaukelt Sicherheit vor.

Doch genau diese Praxis ist ein Leckerbissen für Hacker: Sie durchforsten mit Hilfe von automatisierten Scans rund um die Uhr das gesamte Netz nach aktiven Geräten – ob Router, Smart-TV oder Web-Cam – und übernehmen dann die

Kontrolle. Denn wenn das Passwort bei nahezu allen Geräten identisch ist, bedarf das keinen großen Aufwand.

Hacker können viel zu leicht Kontrolle übernehmen

Die Folge: Hacker können sich in fremde Wohnzimmer einklinken, Gespräche belauschen, unbemerkt die Web-Cam aktivieren und Schlimmeres. Besonders gefährlich für die Allgemeinheit ist das Zusammenschließen von gekaperten Geräten in den Privathaushalten zu sogenannten „Botnets“, um damit in konzertierten Aktionen Server zu attackieren und lahmzulegen („DDoS-Attacke“). Teilweise mit enormem Schaden,

Aus diesem Grund verbietet die britische Regierung es den Herstellern jetzt, Geräte mit einfachen Standard-Passwörtern wie „admin“ oder „password“ auszuliefern. Ab sofort müssen erhöhte Sicherheitsstandards beachtet werden.

Weitere sinnvolle Maßnahme: Die Hersteller müssen angeben, wie lange sie ihre Geräte mindestens mit Sicherheits-Updates versorgen; etwa um entdeckte Sicherheitslücken in der Software der Geräte zu stopfen. Außerdem müssen die Hersteller den Kunden ermöglichen, Probleme und Sicherheitslücken zu melden.

Ein Magier war offiziell der erste Hacker der Geschichte

Auch EU plant Maßnahmen – allerdings erst ab 2027

Die britische Regierung sei damit die weltweit erste, die solche Regeln umgesetzt hat, so das britische Parlament. Auch das Europaparlament hat sich im März dieses Jahres auf den „Cyber Resilience Act“ geeinigt, der ähnliche Sicherheitsanforderungen vorsieht. Solche Maßnahmen werden von IT-Sicherheitsexperten schon lange gefordert.

Allerdings bekommen Hersteller und Handel in der EU eine großzügige Übergangszeit: Geplant ist, dass die europäischen Regeln erst ab 2027 greifen.

Darauf sollte man aber nicht warten. Wer ein Gerät installiert und benutzt, das online geht, sollte darauf achten, gleich am Anfang das Standard-Passwort durch

ein eigenes zu ersetzen. Das erschwert es Hackern, sich in die Geräte einzuklinken.

Diebstahlschutz bei iOS

Euer Smartphone, euer Datenschatz. Nahezu euer ganzes Leben ist darauf gespeichert, und ein Verlust ist eine Katastrophe. Sichert euer Gerät so ab, das niemand sonst an eure Daten kommt!

PIN und Biometrie

Jedes Smartphone bietet zumindest einen Basisschutz an, mit dem ihr das Gerät vor ungewolltem Zugriff schützen könnt und solltet. Ob es einen Moment unbeobachtet auf dem Schreibtisch liegt, aus der Handtasche entwendet wird oder tatsächlich abhanden kommt: Die Sicherung mit PIN und/oder biometrischen

Zugangsdaten wie Fingerabdruck oder Gesichtserkennung ist schnell eingerichtet:

- Beim iPhone tippt auf **Einstellungen** > **Face ID & Code** (bei älteren

Modellen mag hier auch Touch ID stehen).

- Wenn ihr bereits einen Gerätecode vergeben habt, dann müsst ihr diesen eingeben.

- Fehlt die Sicherung durch einen Code noch, dann könnt und solltet ihr diesen jetzt vergeben.

- Unter Code anfordern könnt ihr die Zeit einstellen, nach der automatisch der Code abgefragt wird. Diese Zeitspanne ist sehr subjektiv und hängt von eurem Nutzungsverhalten ab. Probiert hier gegebenenfalls ein wenig aus.

- Unter Face ID könnt ihr die Gesichtserkennung aktivieren. Diese muss trainiert werden, indem ihr auf Aufforderung des Geräts euer Gesicht in einem Rahmen positioniert und bewegt. Als Brillenträger müsst ihr das sogar doppelt machen, einmal mit, einmal ohne Brille.

- Ganz unten auf diesem Bildschirm findet ihr die Option **Daten löschen**. Ist diese aktiviert, dann wird das Gerät nach 10 fehlgeschlagenen Anmeldeversuchen automatisch gelöscht. Seid nur vorsichtig, wenn ihr kleine Kinder habt, die das Gerät gegebenenfalls in die Finger bekommen könnten. Da sind versehentliche Anmeldungen an der Tagesordnung!

Der erweiterte Diebstahlschutz

iOS hat seit iOS 17.3 eine weitere Funktion, die die Sicherheitseinstellungen schützen soll. Denn was nützen die, wenn jemand sie aktivieren kann. Beispielsweise, weil er euren Code kennt?

Die Idee dahinter: Ein Dieb wird sich erst einmal mit dem Gerät vom Ort seiner Tat entfernen und erst dann Einstellungen ändern. Prüft das iPhone vor der Veränderung von Einstellungen, ob ihr an einem für euch normalen Ort seid, dann wird das den Dieb vermutlich ausbremsen. Der wird eher nicht bei euch zuhause oder auf der Arbeit sein!

img 1411

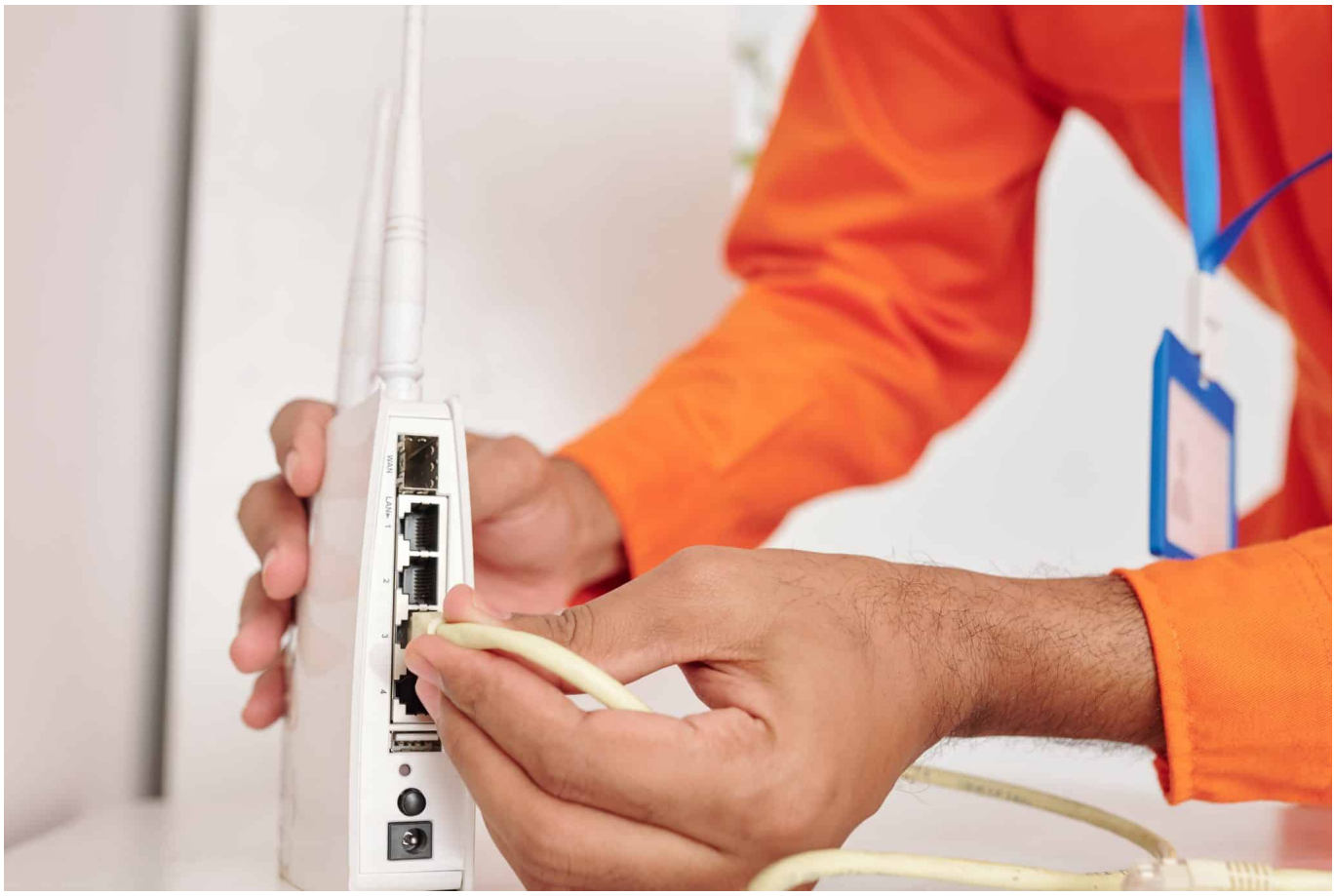
- Beim iPhone tippt auf **Einstellungen** > **Face ID & Code** (bei älteren Modellen mag hier auch Touch ID stehen).

- Rollt nach unten auf **Schutz für gestohlene Geräte**.

- Aktiviert diesen, dann wählt unter **Sicherheitsverzögerung erforderlich** die Option **An keinem vertrauten Ort**, damit eine Verzögerung von einer Stunde und eine weitere Authentifizierung durch Code/Gesichtserkennung eingeschaltet wird, sobald ihr Sicherheitseinstellungen ändern wollt.

- Aktiviert **Immer**, damit diese Verzögerung immer aktiviert wird, sobald ihr Sicherheitseinstellungen ändern wollt.

Probleme im WLAN lösen



Ohne WLAN geht zu Hause und oft auch unterwegs kaum etwas. Prima, wenn es funktioniert, was aber, wenn das nicht der Fall ist? Die Ursachen sind vielfältig.

WLAN vs. LAN

WLAN und LAN unterscheiden sich um einen Buchstaben, und der ist entscheidend: Das **L**ocal **A**rea **N**etwork ist eine lokale Vernetzung von Geräten, die im Normalfall per Kabel stattfindet. Auch wenn der eine oder andere Anwender LAN und Netzwerk gleichsetzt, ist verwendet das LAN klassischerweise Kabel und schließt damit den ein oder anderen Gerätetypen

aus: Tablets und Smartphones haben keinen Anschluss für ein Netzwerkkabel.

Hier kommt nun das W in WLAN ins Spiel: ein WLAN ist ein **W**ireless **L**ocal **A**rea **N**etwork, also ein kabelloses Netzwerk. Der Vorteil: Es ist ach da verwendbar, wo ihr mit einem Netzwerkkabel nicht hinkämt und mit Geräten, die keinen Kabelanschluss haben.

WLAN-Probleme lösen

Die ersten Schritte bei WLAN-Problemen: Kontrolliert die Internetverbindung.

Danach kontrolliert die Funkkanäle.

Wenn das nicht reicht, dann helfen Euch Tools wie InSSIDler weiter. Der Aufwand ist allerdings nicht zu unterschätzen, denn die Programme sind, wie die Probleme, die sie lösen sollen - komplex. Wenn es sich um ein 5GHz WLAN handelt, mit dem Ihr Probleme habt, dann ist die Lösung oft viel einfacher:

Die verwendeten Funkfrequenzen kollidieren manchmal mit den Radarsignalen nahegelegener Flughäfen, Krankenhäuser und anderer Organisationen. Die sind aber "bevorrechtigt", wie es im Beamtendeutsch heißt: Sobald Euer Router ein solches Signal erkennt, muss er entweder den WLAN-Kanal wechseln oder gar das komplette WLAN zeitweise ausschalten.

06.12.22	18:55:41	Internetverbindung IPv6 wurde getrennt, Präfix nicht mehr gültig.
06.12.22	18:55:41	Internetverbindung wurde getrennt.
06.12.22	18:55:36	DSL antwortet nicht (Keine DSL-Synchronisierung).
06.12.22	16:03:02	[Buero] 5-GHz-Band für 10 Min. auf dem gewählten Kanal 116 (Frequenz 5.580 GHz) nicht nutzbar wegen Prüfung auf bevorrechtigten Nutzer (z.B.RADAR).
06.12.22	16:02:42	RADAR wurde auf Kanal 116 (Frequenz 5.580 GHz) erkannt, automatischer Kanalwechsel wegen bevorrechtigtem Nutzer ausgeführt.
05.12.22	17:00:23	Internettelefonie mit AnddPro12.9_eSHGs2.I über 192 war nicht erfolgreich. Ursache: (408)
04.12.22	21:53:16	[Buero] 5-GHz-Band für 10 Min. auf dem gewählten Kanal 116 (Frequenz 5.580 GHz) nicht nutzbar wegen Prüfung auf bevorrechtigten Nutzer (z.B.RADAR).
04.12.22	21:53:03	[Buero] Repeater-Anmeldung an der Basis gescheitert: Authentifizierungsfehler. MAC-Adresse: [2 Meldungen seit 04.12.22 21:23:05]
04.12.22	21:22:43	[Buero] RADAR wurde auf Kanal 116 (Frequenz 5.580 GHz) erkannt, automatischer Kanalwechsel wegen bevorrechtigtem Nutzer ausgeführt.
03.12.22	04:18:53	IPv6-Präfix wurde erfolgreich aktualisiert. Neues Präfix: 2003:c5:cf2b:e200::/56
03.12.22	04:11:57	DynDNS-Fehler: Der angegebene Domainname kann trotz erfolgreicher Aktualisierung nicht aufgelöst werden.
03.12.22	04:03:53	IPv6-Präfix wurde erfolgreich bezogen. Neues Präfix: 2003:c5:cf2b:e200::/56
03.12.22	04:03:52	Internetverbindung IPv6 wurde erfolgreich hergestellt. IP-Adresse: 2003:c5:cfff:2c1a:3ea6:2fff:fe3c:6b21
03.12.22	04:03:52	Internetverbindung wurde erfolgreich hergestellt. IP-Adresse: 80. 01, DNS-Server: 217. 0 und 217.237.150.115, Gateway: 62. 2, Br
03.12.22	04:03:52	Information des Anbieters über die Geschwindigkeit des Internetzugangs (verfügbare Bitrate): 249881/43976 kbit/s
03.12.22	04:03:49	DSL ist verfügbar (DSL-Synchronisierung besteht mit 265461/46719 kbit/s).
03.12.22	04:00:57	DSL-Synchronisierung beginnt (Training).
03.12.22	03:59:55	Zeitüberschreitung bei der PPP-Aushandlung.
03.12.22	03:59:55	Internetverbindung IPv6 wurde getrennt, Präfix nicht mehr gültig.
03.12.22	03:59:55	Internetverbindung wurde getrennt.

- Meldet Euch an der Verwaltungsoberfläche Eures Routers an.

- Wechselt in die **Systemeinstellungen**. Dort findet Ihr einen Eintrag für die **Systemereignisse**.

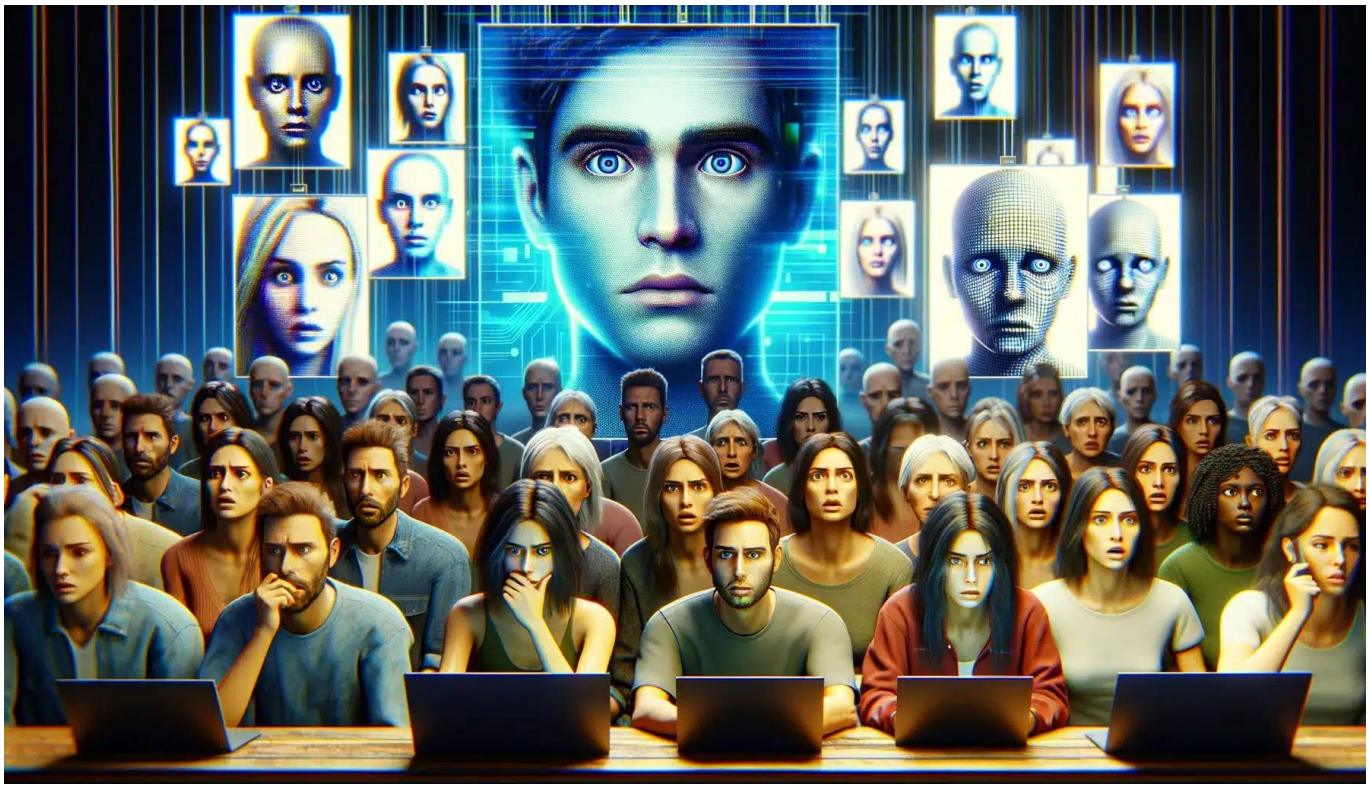
- Klickt darauf, dann zeigt Euch der Router eine Übersicht der wichtigen Ereignisse an inkl. eines Zeitstempels.

- Sucht nach Einträgen "RADAR wurde erkannt" oder "5GHz-Band wurde deaktiviert" und vergleicht den Zeitstempel mit der Zeit, zu der Ihr mit dem WLAN Probleme hattet.

- Stimmen die Zeiten überein, dann habt Ihr die Ursache für die Störung gefunden.

Die einzige Alternative, die Ihr hier habt: Verbindet Euch statt mit dem 5GHz-WLAN mit dem 2.4 GHz WLAN, wenn das verfügbar ist. Für dieses gibt es diese automatische Prüfung nicht. Viele Router bieten an, die beiden WLANs unterschiedlich zu benennen, sodass Ihr die Möglichkeit habt, Euch gezielt mit dem einen oder dem anderen zu verbinden.

Das Zeitalter von KI und Deepfakes – Chancen und Gefahren



KI bietet viele interessante Möglichkeiten und ist auch oft sehr nützlich. Doch KI kann auch missbraucht werden, etwa in Form von Deepfakes.

Die Entwicklung von Künstlicher Intelligenz (KI) schreitet weiter voran.

Und während diese Technologie ohne Frage viele neue Möglichkeiten mit sich bringt, kann KI – in den falschen Händen – durchaus auch eine Gefahr darstellen. KI kann zum Beispiel die Gefahr durch Cyber-Angriffe drastisch erhöhen.

Dazu gehören vor allem sogenannte **Deepfakes**, durch künstliche Intelligenz veränderte Medieninhalte, die Fälschungen ermöglichen, die täuschend echt

erscheinen.

Ein brennendes Pentagon oder Weißes Haus (hier ein Deepfake) kann Unruhe auslösen

Gefahren durch Deepfakes

Mit Deepfakes lassen sich Gesichter auf vorhandene Videos legen und der Ton so manipulieren, dass Betrachter das Gefühl haben, dass das Video authentisch ist.

Das mag Spielereien ermöglichen, die – wenn nicht weiter geteilt oder entsprechend gekennzeichnet – harmlos sind.

Doch im Zuge von Cyberbetrug handelt es sich um eine mächtige Waffe, die effiziente **Cyberangriffe und Manipulation ermöglicht**.

Mögliche Folgen können sein: Verbreitung von Fehlinformationen, Social-Engineering-Angriffe oder Diffamierung von Personen oder Organisationen. Für private Online-Nutzer besteht insbesondere die Gefahr, dass Deepfakes die **Gefahr durch Phishing-Angriffe erhöhen**.

Phishing-Attacken mithilfe von Deepfakes lassen sich in zwei Kategorien unterteilen: Angriffe in Echtzeit und Nicht-Echtzeit-Angriffe.

Bei Angriffen in Echtzeit könnten die Kriminellen das Opfer mit gefälschten Video- oder Audiodaten davon überzeugen, dass die Person am anderen Ende ein vermeintlicher Kollege, Vorgesetzter oder Kunde ist.

Das ist vor allem bei **Spear-Phishing** effektiv, wenn das Opfer zuvor gezielt ausgesucht wurde und mithilfe vorab gesammelter Informationen ein Phishing-Angriff erfolgt.

Nicht-Echtzeit-Angriffe hingegen basieren darauf, dass der Täter ebenfalls eine Video- oder Audiodatei fälscht und sich als eine bestimmte Person ausgibt, wie zum Beispiel einen Prominenten.

Diese Datei teilt er dann über E-Mail, soziale Medien oder Chats, um die Empfänger zur Preisgabe von Informationen zu drängen oder bestimmte Handlungen ausführen zu lassen. Diese Angriffe, die nicht in Echtzeit erfolgen,

ermöglichen es, **mehrere Personen gleichzeitig** zu attackieren.

Passwort Manager sorgen für ein sichereres Internet

So kannst du dich schützen

Es gibt mehrere Möglichkeiten, sich gegen Cyberangriffen mithilfe von KI und Deepfakes zu schützen:

Bleibe informiert: Informiere dich ausgiebig und regelmäßig über Deepfakes und Cyberbedrohungen durch KI, um Angriffe frühzeitig erkennen zu können. **Sei außerdem skeptisch**, wenn du Nachrichten oder Anrufe von scheinbar bekannten Personen erhältst, dessen Inhalte aber **widersprüchlich** zum gewöhnlichen Verhalten oder Inhalten der Person sind.

Sichere deine Konten: Cyberkriminelle haben es oft auf Kontodaten und andere persönliche Informationen abgesehen.

Sichere deine Accounts daher **mit starken und individuellen Passwörtern**. Ein Passwort-Manager kann dir helfen, deine Logindaten zu speichern und zu verwalten und starke Kennwörter zu erstellen.

Aktiviere eine Zwei-Faktor-Authentifizierung (2FA): Zusätzlich zu starken Kennwörtern solltest du deinen Konten mit einer 2FA **eine zusätzliche Sicherheitsschicht** hinzufügen. Das bedeutet, um dich in dein Konto einzuloggen, benötigst du neben den Logindaten einen Code, der per App oder SMS generiert wird.

Schulungen innerhalb von Unternehmen: Da solche Deepfakes für Spear-Phishing-Attacken genutzt werden können, die gezielt Unternehmen treffen, sollten **regelmäßige Schulungen** stattfinden, um die Mitarbeiter über die Gefahren von KI und Deepfakes für Cyberattacken aufzuklären.

Call ID Spoofing: Wie Betrüger Ihre Telefonnummer fälschen und was Sie dagegen tun können

Die Rufnummer, die bei einem Anruf im Display des Handys oder Telefons erscheint, lässt sich manipulieren – und Betrüger nutzen das aus.

Hast du schon einmal einen Anruf von einer bekannten Nummer erhalten, nur um festzustellen, dass es sich um einen Fremden handelt?

Klarer Fall von Opfer von Call ID Spoofing geworden.

In Zeiten zunehmender Telefonbetrugsversuche ist es wichtiger denn je, über die Methoden der Betrüger Bescheid zu wissen. Eine davon ist das sogenannte **Call ID Spoofing**, das dem Angerufenen vorgaukelt, der Anruf käme von einer

vertrauenswürdigen Quelle.

Betrüger nutzen Caller ID Spoofing, im Missbrauch zu betreiben

Was ist Call ID Spoofing?

Call ID Spoofing bezeichnet die Manipulation der Anruferkennung, um die wahre Identität des Anrufers zu verschleiern. Dabei wird eine gefälschte Telefonnummer übermittelt, die oft von bekannten Unternehmen, Behörden oder sogar von Ihren eigenen Kontakten stammt. Das Ziel ist es, Vertrauen zu erwecken und Sie dazu zu bringen, den Anruf anzunehmen

Betrüger nutzen spezielle Software oder Dienste, um die Anruferkennung zu manipulieren. Sie können nahezu jede beliebige Nummer einsetzen, sogar

solche, die gar nicht vergeben sind. Die Technik dahinter ist relativ einfach, was es umso wichtiger macht, wachsam zu sei

Wer ist von Call ID Spoofing betroffen?

Potenziell kann jeder Telefonbesitzer Opfer von Call ID Spoofing werden. Betrüger gehen oft wahllos vor und rufen massenhaft Nummern an, in der Hoffnung, dass einige Personen darauf hereinfallen. Besonders gefährdet sind ältere Menschen oder solche, die wenig Erfahrung mit Telefonbetrug haben.

Wie erkenne ich Call ID Spoofing?

Es gibt einige Anzeichen, die auf einen gefälschten Anruf hindeuten können:

- Die angezeigte Nummer passt nicht zum angeblichen Anrufer (z.B. Behörde mit Mobilfunknummer)
- Sie werden von einer bekannten Nummer angerufen, aber die Stimme ist fremd
- Der Anrufer verlangt persönliche Daten oder Geld

- Sie werden unter Druck gesetzt, schnell zu handeln

Was kann ich gegen Call ID Spoofing tun?

- Seien Sie misstrauisch bei unerwarteten Anrufen, auch von bekannten Nummern

- Geben Sie niemals persönliche Daten oder Geld am Telefon heraus

- Fragen Sie im Zweifelsfall zurück und lassen Sie sich die Identität bestätigen

- Legen Sie einfach auf, wenn Ihnen etwas verdächtig vorkommt

- Melden Sie Betrugsversuche der Bundesnetzagentur oder der Polizei

Technische Maßnahmen gegen Call ID Spoofing

Leider gibt es keine hundertprozentige technische Lösung gegen Call ID Spoofing. Einige Anbieter von Telefonanlagen bieten jedoch Funktionen wie eine Anrufvalidierung an, die zumindest einige gefälschte Anrufe herausfiltern können. Auch die Bundesnetzagentur arbeitet an Lösungen, um das Problem einzudämmen.

Call ID Spoofing ist eine weit verbreitete Methode von Telefonbetrügern, um arglose Bürger zu täuschen. Doch mit der richtigen Portion Misstrauen und Vorsicht können Sie sich effektiv davor schützen. Lassen Sie sich nicht unter Druck setzen und hinterfragen Sie verdächtige Anrufe. So können Sie sich vor den finanziellen und emotionalen Folgen von Telefonbetrug bewahren.

Bitcoin, Ethereum, NFTs und Co: Wie klimaschädlich sind Kryptowährungen?

Bitcoin, Ethereum, Dogecoin: Es wird viel über solche Kryptowährungen gesprochen, vor allem auf Social Media. Doch vo einigen ist bekannt, dass sie sehr viel Energie verbrauchen.

Gerade erst war der Bitcoin wieder in den Schlagzeilen, weil die „Belohnung“ für das Schürfen neuer Bitcoin halbiert wurde (Bitcoin Halving genannt).

Viele schwärmen im Netz von Bitcoin, NFTs und Co. Viele fragen sich, soll ich da mit einsteigen? Wie sind die Risiken – und was ist eigentlich mit den Folgen für die Umwelt?

Beim Bitcoin bleibt alles beim Alten

Kryptowährungen: Keine Geldscheine und Geldstücke

Kryptowährungen: Da müssen keine Geldscheine gedruckt, auch keine Geldstücke geprägt und im Umlauf gebracht werden. Alles rein digital. Trotzdem haftet insbesondere dem Bitcoin das Stigma an, eine Klimakiller zu sein Stimmt das noch?

„Killer“ ist ein großes Wort. Aber der Energiebedarf für den Bitcoin ist schon groß, und es wird eher mehr als weniger.

Im Bitcoin-Netzwerk muss viel gerechnet werden, um das Blockchain-Netzwerk am Laufen zu halten, um es abzusichern und neue Bitcoins zu „schürfen“, sozusagen zu erschaffen.

Bitcoin verantwortlich für 0,6 des Stromverbrauchs

Das kostet alles unvorstellbar viel Energie. Schätzungen zufolge verbraucht das Bitcoin-Netzwerk allein jährlich etwa 130 Terawattstunden (TWh) Strom (Stand 2022).

Das entspricht etwa 0,6% des weltweiten Stromverbrauchs. Dazu kommen aber noch andere Umweltkosten, da geh ich gleich noch mal drauf ein.

Und der Rechenaufwand und Ressourcenverbraucht steigt, je beliebter solche dgitalen Währungen wie Bitcoins, Etherium, Dogcoins werden, oder auch sogenannte NFTs, digitale Kunstwerke, die technisch ganz ähnlich funktionieren.

Bitcoin hat immer mehr Nutzer

Allein für den Bitcoin gab es zuletzt rund 90 Mio. Wallets, also digitale Brieftaschen. Ein Jahr davor 76 Millionen- Im Jahr 2014 waren es nur drei Mio. Man kann wohl von einem Anstieg sprechen.

Alle, die mit Kryptowährungen Geld verdienen, zum Beispiel Tauschbörsen, die EU in Bitcoin umwandeln oder die Bitcoin auch hinterlegen, machen viel Werbung auf Social Media – direkt und indirekt. Das Thema ist sehr präsent auch, weil sich viele für diese vergleichsweise neue Anlageform interessieren.

Der Bitcoin lebt davon, dass er durch seine technischen Details als sehr sicher gilt. Jede Transaktion wird in der sogenannten digital erechneten Blockchain

gespeichert. Es kann nicht manipuliert und gefälscht werden. Allerdings kann ich fast nirgendwo direkt mit Bitcoin bezahlen, eigentlich ist er eher ein bisschen wie Gold.

Bitcoin und Gold

Gold selbst hat auch keinen direkten Geldwert. Ich kann damit nicht in den Laden gehen und einkaufen. Aber es hat trotzdem weltweit einen Wert.

Kryptowährungen: Keine Geldscheine und Geldstücke. Richtig, ist beim Bitcoin auch so. Gold steigt im Wert, wenn mehr Leute dort ihr Geld investieren, häufig in globalen Krisen.

Beim Bitcoin ist es schon seit einer ganzen Weile ähnlich. Der Bitcoin ist eine künstlich beschränkte Ressource. Es wird nie mehr als 21 Mio. Bitcoin geben. Klassisches Geld kann immer mehr gedruckt werden, stichwort **Inflation**, vor der viele im Moment Sorge haben an. Bitcoin kennt das so nicht. Das macht ihn begehrt. Als Anlage.

Die Kurse steigen manchmal enorm, ähnlich wie beim Gold, fallen aber auch manchmal enorm. Es gibt eine hohe „Volatilität“, wie die Fachleute sagen. Die Kurse schwanken stark.

Heisst unterm Strich: Als ich im Januar 1011 mal 1000 Bitcoin gekauft habe, waren die für knapp 5 EUR pro Bitcoin zu haben. Als sie sich im Wert verdoppelt haben, habe ich sie verkauft.

Riesen Fehler, muss ich heute sagen. Heute ist ein Bitcoin 60.000 EUR wert. Das wären dann also 60 Mio. EUR. Hätte ich die mal noch...

Klar, Man kann viel gewinnen, aber auch viel verlieren.

Und noch etwas ist mit Gold identisch: Die meisten Aktien werfen regelmäßig Dividenden ab. Ausgezahlte Gewinne der Unternehmen. Bei Gold ist das nicht so. Bei Bitcoin ebenso.

Bitcoin und der Stromverbrauch

Bitcoin-Netzwerk und andere digitale Währungen verbrauchen enorm viel Strom. Allein der Bitcoin ist für 0,6 % des weltweiten Stromverbrauchs verantwortlich.

Das entspricht in etwa dem Stromverbrauch von Ländern wie Argentinien oder Schweden. Der Bitcoin-Stroimverbraucht übersteigt bereits den Stromverbrauch von Ländern wie den Niederlanden.

In einer Studie wurde mal berechnet, wieviel Energie statistisch gesehen für eine einzige Bitcoin-Transaktion verbraucht wird: Es sind ca. 1.700 kWh.

Damit könnte ein durchschnittlicher deutscher Vier-Personen-Haushalt fast vier Monate lang mit Energie versorgt werden. Wenn ich einen Bitcoin kaufe oder verkaufe oder jemandem einen sende, ist energietechnisch also dasselbe, als würde ein Haushalt vier Monate lang Strom verbrauchen.

Und Elektroschrott fällt auch noch an.

Krypto Farming gefährdet

Bitcoin und grüner Strom

Setzt man denn wenigsten mehr auf grünen Strom um den CO2-Ausstoss zu verringern?

Ja, bei der Kryptowährung Ethereum war das schon vor längerer Zeit ein gestecktes Ziel, das nach und nach auch umgesetzt wird. Aber auch beim Bitcoin bemüht man sich zunehmend, grüne Energie zu verwenden.

Der hohe Stromverbrauch von Bitcoin führt aber derzeit noch zu einem erheblichen CO2-Ausstoß, da ein großer Teil der verwendeten Energie bisher aus fossilen Brennstoffen stammt.

Seriöse Schätzungen gehen davon aus, dass der jährliche CO2-Fußabdruck von Bitcoin bei etwa 65 Megatonnen liegt (das wurde in 2022 ermittelt). Das entspricht in etwa den jährlichen CO2-Emissionen von Griechenland. Eine andere Studie der TU München kommt „nur“ auf 22 Mio. Tonnen CO2 jährlich, so viel wie Hamnurg oder Las Vegas.

Dazu muss man wissen: Es werden komplette Rechenzentren betrieben, um den Bitcoin zu verwalten und neue Bitcoin zu schürfen. Einige hingen zeitweise an ausschließlich dafür bereitgestellte Kohlekraftwerden in den USA. Ein komplettes Kraftwerk, nur um ein Bitcoin-Rechenzentrum zu betreiben.

Und das hat Folgen: Der CO2-Ausstoß einer einzelnen Bitcoin-Transaktion wird auf etwa 700 kg geschätzt, was den Emissionen eines Fluges von London nach New York entspricht.

Bitcoin und Elektroschrott

Ich hatte bereits erwähnt, dass jede Bitcoin-Transaktion auch Elektroschrott verursachst – auch nicht gerade umweltfreundlich. Was steckt dahinter?

Es ist nicht so, dass bei jeder Transaktion, also wenn ich Dir einen Bitcoin überweise, zum Beispiel, irgendwo auf der Welt ganz konkret Elektroschrott anfällt.

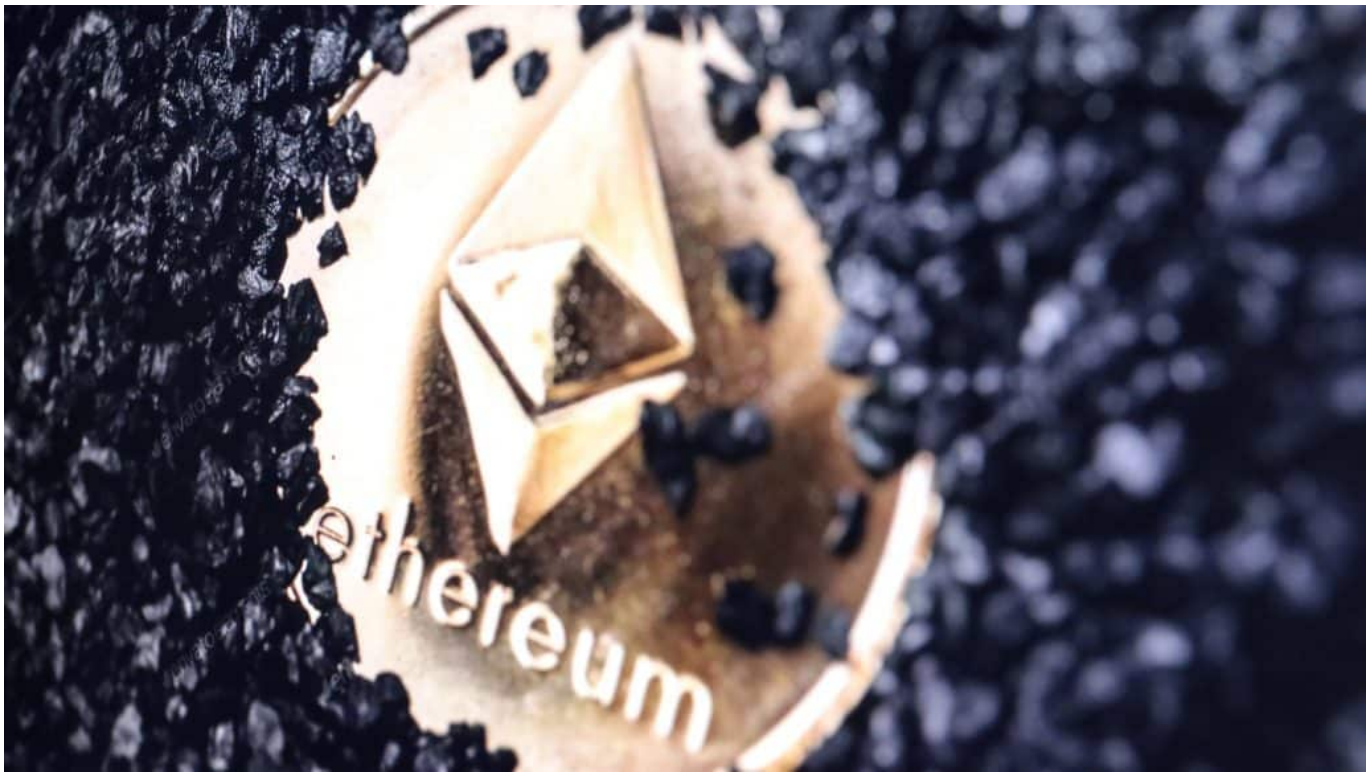
Es ist eine statistische Größe und hat damit zu tun, wie der Bitcoin funktioniert. Wir haben schon über das Mining gesprochen, das beim Bitcoin so typisch ist.

Es ist enormer Rechenaufwand nötig, um die Bitcoin-Blockchain abzusichern, um jede Transaktion zu bestätigen – und am Ende auch, um neue Bitcoin zu „schürfen“, zu erschaffen. Der Rechenaufwand wird von Tag zu Tag größer.

Deshalb setzen Bitcoin Miner immer spezialisiertere Hardware ein, die nichts anderes macht, als für den Bitcoin zu rechnen, zu rechnen, zu rechnen. Nach durchschnittlich 18 Monaten sind die Geräte durch – und dann durch zu langsam, um mit anderen Rechnern mithalten zu können. Sie werden dann ersetzt.

Da fragt man sich unweigerlich: Und diese Computer-Hardware könnte man dann nicht für was anderes nutzen, zum beispiel an schulen spenden

In der regel nicht, weil sie so spezialisiert ist Die Folge: Sie werden entsorgt. Auf die Müllkippe. So entstehen doch immense Berge an Elektroschrott. Die Angabe von 250 Gramm Elektroschrott pro Bitcoin-Transaktion stammt aus einer Studie aus dem Jahr 2021 mit dem Titel „Bitcoin´s growing e-waste problem“.



Auch klassisches Geldsystem verbraucht Energie

Aber zur Ehrlichkeit gehört dazu: Auch für normales Geld in scheinen und Münzen gibt es Prägewerkstätten, Druckereien, die Papier und Metalle brauchen, und auch viel Energie. Ist klassisches Geld also nicht auch ein Klimakiller? Vielleicht der Schlimmere?

Das Banksystem verbraucht viel Energie, keine Frage, vor allem kommt ja auch dazu, dass das Geld noch transportiert werden muss. Man kann den ganzen Aufwand wirklich nur grob schätzen; es ist unmöglich, das genau zu sagen.

Eine Studie mit dem Titel **On Bitcoin's Energy Consumption: A Quantitative Approach to a Subjective Question** (2021) vergleicht den Energieverbrauch von

Bitcoin mit dem des traditionellen Finanzsystems, einschließlich Banken, Geldautomaten und der Goldproduktion.

Allein das Bankensystem verbraucht laut dieser Studie jährlich etwa 238,92 TWh, während Geldautomaten und Zweigstellen weitere 26,48 TWh verbrauchen.

Das wäre ein doppelt so hoher Stromverbrauch wie beim Bitcoin. Allerdings wurde diese Studie von Finanzdienstleistungsunternehmen im Bereich Kryptowährungen in Auftrag gegeben. Man kann also davon ausgehen, dass diese Zahlen eher Bitcoin-freundlich ist.

Wir brauchen Geldsysteme

Der Unterschied ist: alle Menschen auf der Welt benutzen klassisches Geld, täglich, andauernd. Dadurch ist der Strombedarf auch höher. Wir brauchen das klassische Geldsystem.

Der Bitcoin ist aber ein exklusiver, vergleichsweise kleiner Verein. Niemand braucht den Bitcoin wirklich. Er wird zur Spekulation genutzt, so gut wie gar nicht als echtes Bezahlsystem.

Niemand hat ausgerechnet, wieviel Energie es kosten würde, wenn alle Menschen auf der Welt den Bitcoin nutzen würden anstelle von Bargeld. Die Blockchain und die dahinter liegende technische Infrastruktur würde am Rad drehen. Es würde deutlich mehr Energie verbrauchen – niemand kann berechnen, wieviel.

Man kann also den Energieverbrauch von Bitcoin und dem echten Geldsystem weltweit nicht wirklich miteinander vergleichen, weil sie nicht diesele Aufgabe erfüllen, nur ins Verhältnis setzen.

Ein Ende des Minungs für Ether

Ehtereum und Co.

Wir haben jetzt vor allem über den Energieverbrauch des Bitcoins gesprochen, weil der natürlich die bekannteste und führende Kryptowährung ist. Wie sieht es denn bei anderen Kryptowährungen aus, ist es da vergleichbar?

Bei Bitcoin ist der Energieverbrauch am höchsten, weil: am weitesten verbreitet und aufgrund der Art und Weise, wie der Bitcoin funktioniert. Nicht alle Kryptowährungen haben den gleichen Energieverbrauch und CO2-Ausstoß. Es gibt ja viele, sie heißen Ethereum, Ripple, Cardano, Dogecoin, Litecoin und viele andere.

Einige verwenden andere Methoden, um ihre Blockchain zu betreiben und abzusichern, die weniger energieintensiv sind. Ethereum zB. verwendet nicht mehr den gleichen energieintensiven Mechanismus wie Bitcoin, der „Proof of Work“ (PoW) genannt wird, Mechanismus wie Bitcoin, sondern „Proof of Stake“.

Der Umstieg hat den Energieverbrauch um 98% reduziert. Aber auch die Sicherheit reduziert. Unter Strich bedeutet das eine Cardano-Transaktion braucht nur noch eine halbe Kilowattstunde, statt die 707 kWh pro Bitcoin-Transaktion.

Der jährliche Stromverbrauch von Cardano wird auf 0,0066 TWh geschätzt, was nur einen Bruchteil des Verbrauchs von Bitcoin ausmacht.

Ich könnte die Liste endlos fortsetzen: Keine Kryptowährung ist derart energiehungrig wie der Bitcoin.

Grüne Anlage oder weniger?

Fassen wir mal zusammen: Wenn ich mich auf Bitcoin oder andere Kryptowährungen einlasse, ist das was für Menschen, denen es an einer ökologischen Anlage gelegen ist – und ist das dann sicher?

Diese Frage lässt sich unmöglich pauschal beantworten. Der Bitcoin ist in Sachen Umweltbilanz eindeutig kritisch. Hier anzulegen bedeutet, das in Kauf zu nehmen und auch mitzumachen, da jede Transaktion Energie kostet.

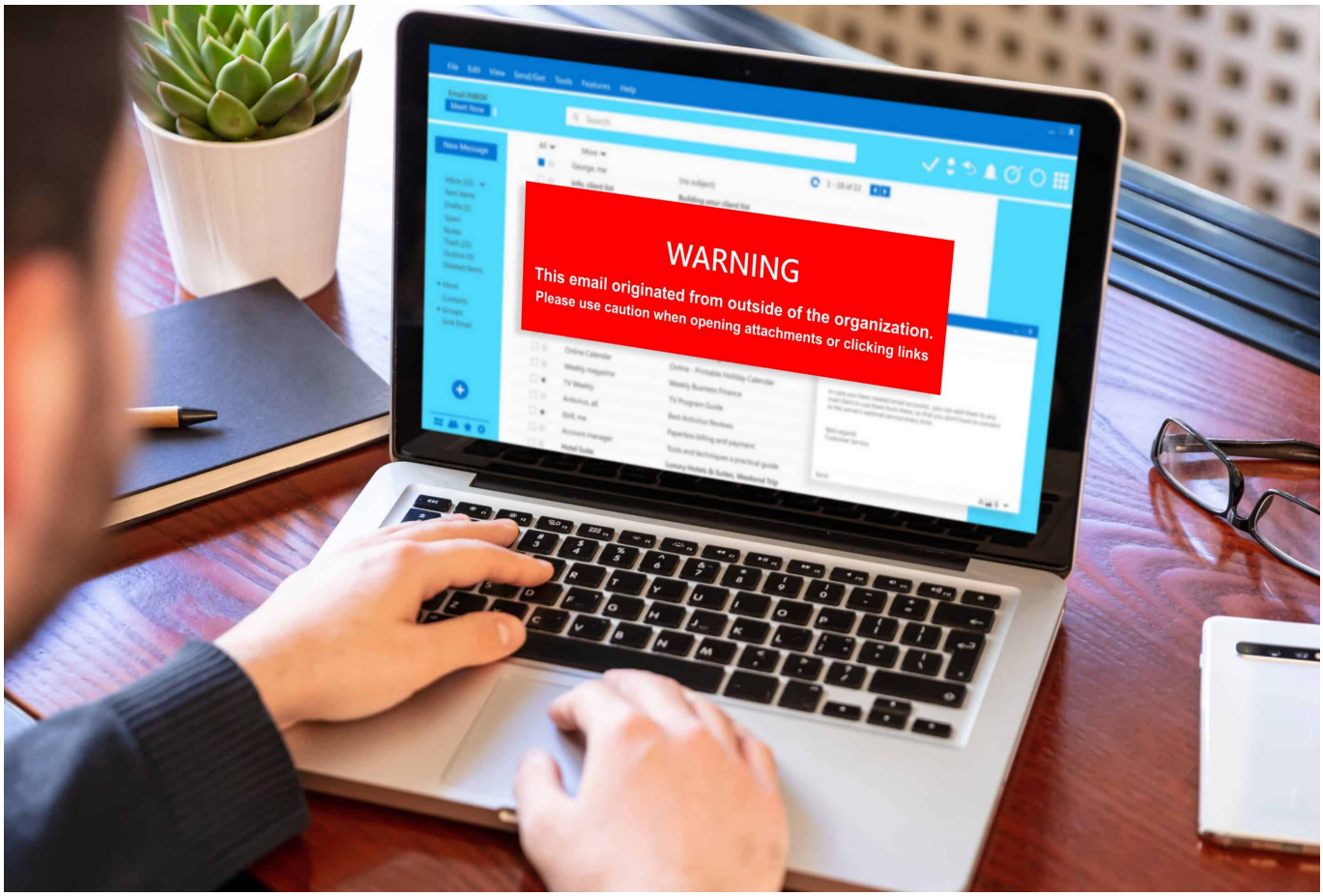
Wer Aktien oder Fonds kauft, die sich dem Umweltschutz oder klimafreundlichen Projekten verschreiben, ist da viel eher auf der „grünen“ Seite. Oder man nimmt andere Kryptowährungen als Bitcoin, da die Bilanz da besser ausfällt.

Was das Risiko anbelangt: Jede Anlageform hat Risiken. Sogar das Sparbuch. Da geht zwar die Einlage nicht flöten, aber wenn der Zins niedriger ist als die Inflation, wird das Geld auch weniger. Bei Aktien und Gold sind enorme Kursschwankungen möglich.

Das ist bei Bitcoin und anderen Kryptowährungen auch so. Wer schnell Blutdruck bekommt, wenn die Kurse um 20 oder 30% in wenigen Tagen schwanken, und das eben auch nach unten, für den sind Kryptowährungen und NFTs eher ungeeignet.

Wer das aber aushält und Chancen für große Gewinne nutzen möchte – und dem Klimaproblematik nicht so wichtig ist –, für den sind Bitcoin und Co. interessant.

Kryptowährungen: Wie Cyberkriminelle digitale Währungen zu ihrem Vorteil nutzen



Es geht mal wieder im Sicherheit im Netz. Die Ergebnisse einer Studie des Unternehmens SoSafe zu Beginn dieses Jahres haben für Aufsehen gesorgt. Cyberkriminelle führen zunehmend erfolgreiche Ransomware-Angriffe gegen deutsche Unternehmen durch.

Cyberkriminelle sind variantenreich, wenn es darum geht, ihre Ransomware zu verteilen. So verschicken die Kriminellen beispielsweise mit einer Malware infizierte E-Mails an Mitarbeiter.

Sobald der Mitarbeiter auf den Link klickt, wird das System über die

Schadprogramme komplett gesperrt, sodass das Unternehmen keinen Zugriff mehr hat. So funktioniert Ransomware in der Regel.

Cyberkriminelle wenden immer neue Tricks an, um ihre schädliche Malware zu verteilen

Zu viele Unternehmen zahlen Lösegeld

Bei 45 Prozent der auf diese Weise erfolgreich angegriffenen Unternehmen kommt es seitens der Cyberkriminellen zu einer Lösegeldforderung. Im Schnitt liegt diese mittlerweile pro Ransomware-Angriff bei durchschnittlich 4,54 Millionen US-Dollar!

Im europäischen Schnitt neigen deutsche und niederländische Unternehmen

vermehrt dazu, diesen Forderungen nachzugeben.

Zukünftig wird die Anzahl der Angriffe durch den Einsatz von künstlicher Intelligenz sogar noch ansteigen. Der Einsatz von ChatGPT und anderen KI-Bots verspricht den Cyberkriminellen eine Zeitersparnis bei Phishing-Angriff (Einfallstor) von mindestens 40 Prozent.

Unternehmen sind gezwungen, zu reagieren!

Unternehmen, egal ob klein, mittel oder groß, müssen die Mitarbeiter sensibilisieren, Software per Patch-Management auf dem aktuellen Stand halten und die Passwortsicherheit erhöhen.

Ransomware kommt meist per Malware

Kryptowährungen bevorzugt

Auffällig bei den Lösegeldforderungen ist die von Cyberkriminellen bevorzugte Zahlungsmethode: Kryptowährungen. Warum eigentlich?

Im Jahr 2023 spülten Lösegelder über eine Milliarde Euro in die Kassen der Cyberkriminellen, wie aus dem Cyber Crime Report der Analysefirma Chainalysis hervorgeht.

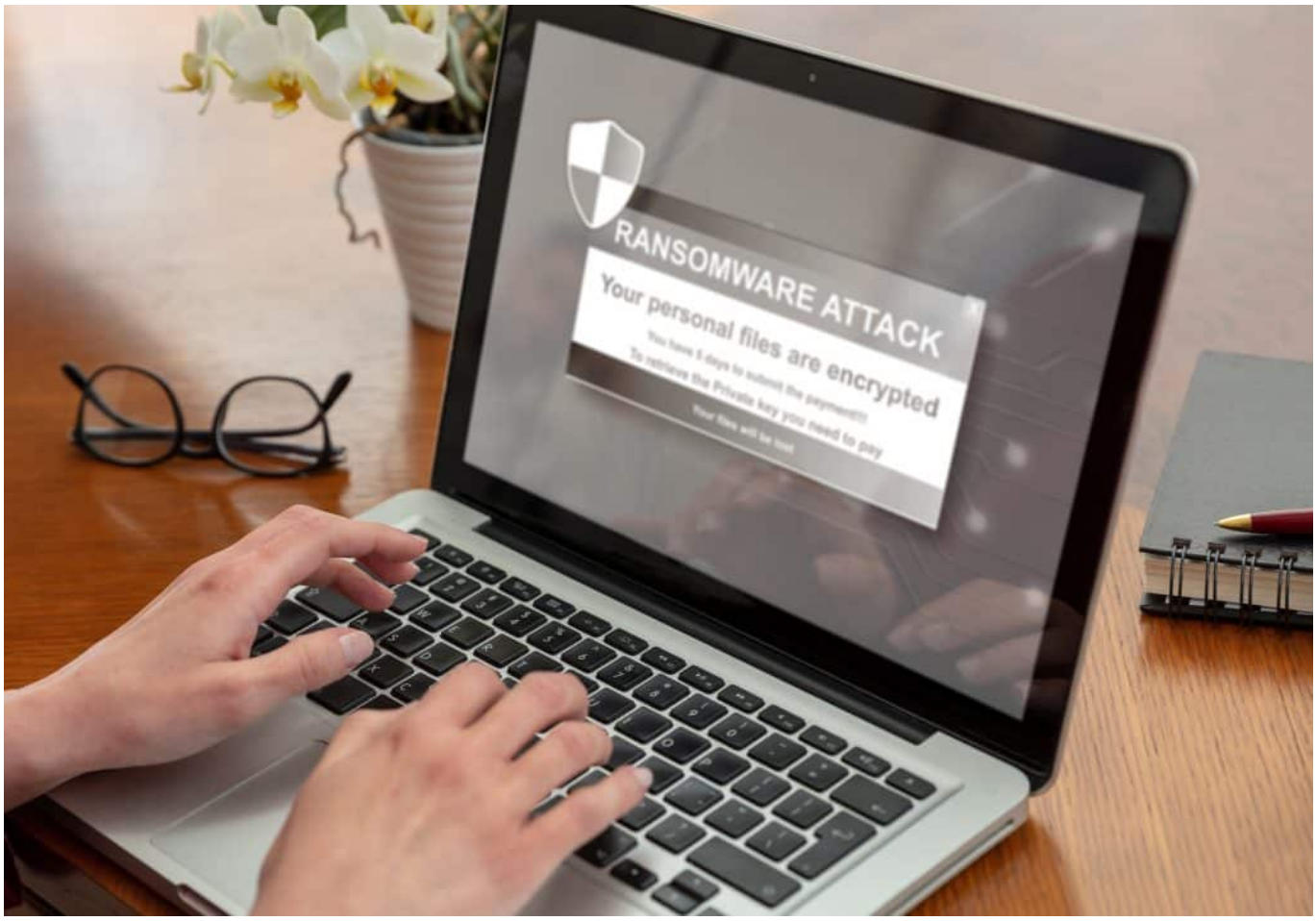
Betroffen sind sowohl Unternehmen als auch einzelne Privatpersonen. Der Hauptfokus liegt jedoch hauptsächlich im Unternehmenssektor, da hier höhere Lösegeldforderungen möglich sind.

Manche Aktionen gibt es nur im Kino

Jetzt stellt sich die Frage: Wie treiben die Cyberkriminellen eigentlich die Lösegelder ein? Wer jetzt an einen Hollywood-Blockbuster denkt, bei dem ein Mitarbeiter des Unternehmens eine Tüte voller Bargeld im Mülleimer deponiert, irrt gewaltig. So etwas gibt es im Kino oder in der Realität vielleicht vor 50 Jahren.

Eine Überweisung per Bankkonto, Paypal oder eine Einzahlung auf eine Prepaid-Kreditkarte wäre eine Option. Hierbei muss jedoch einer der Cyberkriminellen ein Konto eröffnen, seine persönlichen Daten preisgeben und seinen Personalausweis vorlegen. Es würde also nur eine Frage der Zeit sein, bis die Polizei an der Tür klopft.

Kriminelle tüftelten auch hierzu eine Strategie aus. Sie ließen Bankkonten auf fremden Namen eröffnen. Hierzu veröffentlichten sie Jobangebote im Homeoffice auf Plattformen wie Kleinanzeigen (ehemals Ebay-Kleinanzeigen). Sie lockten die Bewerber mit attraktiven Gehältern, die Aufgabe war einzig, Bankkonten im eigenen Namen zu eröffnen. Diese Masche funktionierte jedoch nur für eine gewisse Zeit.



Mitarbeiter und Privatleute müssen immer wachsam sein

Kryptowährungen versprechen maximale Anonymität

So hat es nicht lange gedauert, bis Kryptowährungen in den Fokus von Cyberkriminellen rutschten. Diese digitalen Währungen sind dezentralisiert und nicht abhängig von Bundesbanken oder dem Staat.

Die finanziellen Transaktionen (Wallet-to-Wallet) finden komplett anonym statt!

In der Lösegeldforderung nennen die Cyberkriminellen den aus 26 bis 35 alphanumerischen Zeichen bestehenden (Public Key) der Wallet – keine Namen, keine Bankdaten. Auf diese Wallet senden die Unternehmen Lösegeld, ohne zu wissen, wem diese Wallet gehört.

Für Strafverfolgungsbehörden stellt die Anonymität der Täter hinter den Cyberangriffen eine erhebliche Herausforderung dar.

Obwohl jede Transaktion in der Blockchain – einem öffentlichen Ledger, das alle Transaktionen aufzeichnet – vermerkt wird, ist die Rückverfolgung dieser Transaktionen zu realen Personen ohne zusätzliche Informationen schwierig.

Cyberkriminelle nutzen diese Anonymität aus, um Lösegeldforderungen zu stellen, wohl wissend, dass die digitale Spur, die sie hinterlassen, verwischt und schwer zu verfolgen ist