Digitale Forensik

Dipl.-Ing. Thomas Käfer, M.Sc.

6. Ausgabe



Digitalisierung
Made in Germany

www.KaeferLive.de

DigiFor Inside 6. Ausgabe

Digitalisierung
Made in Germany

Impressum

Herausgeber: KäferLive - Käfer IT Systeme e.K.
Elchenrather Weide 20
52146 Würselen
Tel. 02405/47949-0

Autor: Dipl.-Ing. Thomas Käfer, M.Sc.
Von der IHK Aachen Öffentlich bestellter und vereidigter Sachverständiger
für Systeme und Anwendungen der Informationsverarbeitung
Master of Science Digitale Forensik

Website: https://www.KaeferLive.de
E-Mail: service@KaeferLive.de

© 2025 – Das Werk ist urheberrechtlich geschützt. Die Vervielfältigung und Weitergabe (auch auszugsweise) ohne ausdrückliche Genehmigung des Autors ist untersagt. KaeferLive® ist eine eingetragene Marke von Dipl.-Ing. Thomas Käfer, M.Sc..

Bildnachweis: Quelle Fotolia.com bzw. eigene Aufnahmen/Grafiken (mit KI generiert)

Bezug und weitere Informationen und Artikel siehe:
https://www.kaeferlive.de

Erscheinungsdatum: Februar 2025

Danksagung

Besonderer Dank geht an meine Frau Michaela Käfer, die wieder die Qualitätskontrolle übernommen hat. Bei der akribischen Jagd auf Tippfehler ist sie natürlich wieder fündig geworden.

Inhalt

Impressum....2
Danksagung....2
Inhalt....3
About DigiFor Inside....4
About me....4
Motivation und Begriffsbestimmung....5
- Never touch a running system!....5
- Update vs. Upgrade....6
- Updates first!....7
- Backup first!....8
- Update-Frequenz und Zeitpunkt....9
- EOL-Systeme....10
- Daten und Fakten....10
- Wartungsfenster....11
- Ab in die Hölle....11

Beispiel Windows Upgrades 11 und Server 2025....13
- Motivation und Ausgangslage....13
- Windows 11 Upgrade....14
- Windows Server 2025....15
- Vorarbeiten....15
- Probleme....16
- Lösungen....17
- Ergebnis....17

Fazit....17

About DigiFor Inside

Was ist DigiFor Inside? DigiFor ist die Kurzform für den Begriff „Digitale Forensik“, einem Spezialgebiet der IT, welches sich mit der Analyse und Aufdeckung von Sicherheitsvorfällen (sogenannten Incidents) und missbräuchlicher Nutzung von Computern im Rahmen von Straftaten und zivilrechtlichen Auseinandersetzungen beschäftigt. DigiFor Inside ist eine Reihe von Fachaufsätzen und Veröffentlichungen, publiziert auf dem Portal KäferLive (https://www.KaeferLive.de), bei denen der Autor Thomas Käfer aus dem IT-Nähkästchen plaudert und Angriffskonzepte und Maßnahmen zu deren Erkennung bzw. Abwehr offenlegt.

Mit diesem Artikel „Digitalisierung – Made in Germany“ muss ich mir mal so richtig Luft machen, sonst platze ich. Als Anwender begegnen mir regelmäßig IT-Systeme und Lösungen, die mir abwechselnd die Tränen vor Lachen und vor Verzweiflung in die Augen treiben. Manches ist so dilettantisch gemacht, dass man es als amüsante Story zum Zeitvertreib erzählen kann, oft sind die gemachten Fehler aber von solcher „Güte“, dass es nicht mehr lustig ist. Dann geht es mir wie beim Zuschauen und Zuhören so mancher Satire-Sendung, bei der die Politik aufs Korn genommen wird und mir das Lachen im Hals stecken bleibt. Digitalisierung ist auch so ein Thema (neben KI). Uns wird hier in Deutschland seit Jahren das Thema Digitalisierung um die Ohren gehauen, mal als der neue heiße Scheiß, mals Enabler für neuer Geschäftsmodelle, mal als Lösung für bestehende Probleme (wie Bürokratie) und vielfach als Begründung, warum etwas nicht funktioniert. Man könnte sich also voller Frust in den Schlaf weinen oder wir machen es konstruktiv: Keiner ist unnütz. Er kann immer noch als schlechtes Beispiel dienen. Daher versuche ich einmal, anhand der schlechten Beispiele, die mir in den vergangenen zwei Jahren begegnet sind, zu erklären, wie man Digitalisierung, IT-Sicherheit und Kundendienst mittels EDV nicht macht. Vielleicht ergibt sich daraus dann etwas Positives, nämlich Ideen, wie man es besser / richtig macht. Bei aller Bissigkeit bleibt die Sachlichkeit und der fachliche Hintergrund definitiv nicht auf der Strecke – Versprochen!

Also viel Spaß (oder auch nicht) bei der Lektüre. Ihr Thomas Käfer

About me

Ich bin mit meinem IT-Systemhaus seit 1990 selbstständig in der IT tätig. Das Tätigkeitsfeld der Firma Käfer umfasst Consulting-Leistungen im Bereich der IT-Sicherheit incl. Penetration-Testing u.a. im Automotive-Umfeld sowie die Entwicklung und der Vertrieb von Full-Motion-Simulatoren für Racing und Flight. Seit 2002 arbeite ich als Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung (seit 2006 öffentlich bestellt), als IT-Consultant, Fachautor und beschäftigte mich vor allem mit Fragen der IT-Sicherheit, dem Datenschutz und dem Gebiet der Digitalen Forensik. Ehrenämter als Handelsrichter am Landgericht Aachen sowie als Mitglied der Vollversammlung der IHK Aachen (Ausschüsse Industrie und Technologie, Außenhandel sowie Berufsbildung) komplettierten in der Vergangenheit meine Tätigkeiten. 2015 habe ich aus lauter Langeweile erfolgreich den berufsbegleitenden Masterstudiengang „Digitale Forensik“ an der Hochschule Albstadt-Sigmaringen in Kooperation mit der LMU München und der FAU Erlangen abgeschlossen und in diesem Rahmen eine umfangreiche Forschungsarbeit zum Thema Digitale Kfz-Forensik (Car-Forensics) erstellt. Ich bin Speaker auf Veranstaltungen zum Thema IT-Sicherheit und Daten-schutz und halte Schulungen und Workshops zu diesem Thema für Automobilindustrie, Industrie, Zulieferern, Behörden und Verbände. Privat bin ich glücklich verheiratet, begeisteter Motorradfahrer und seit 2024 auch Inhaber einer Pilotenlizenz PPL(A) für einmotorige Motorflugzeuge. Die Begeisterung für Literatur und die Freude am Spiel mit dem gesprochenen und geschriebenen Wort spiegelt sich in vielen eher technisch und sachlich



orientierten Publikationen und Schriftsätzen aber auch in den Kriminalromanen „Praha“ und „Falk Zwo“ wieder.

Motivation

Durch Deutschland muss endlich wieder ein Ruck gehen!

„Durch Deutschland muss endlich ein Ruck gehen“. Der frühere Bundespräsident Herzog bezog das auf gesellschaftliche Themen (und die damalige Rede ist übrigens heute so aktuell wie damals), aber ich beziehe den Satz jetzt auf die Digitalisierung.
Das, was deutsche Behörden und Institutionen, aber auch namhafte Firmen im Bereich IT hier in Deutschland abliefern, ist oft beschämend.
Aber niemand ist unnütz. Er kann immer noch als schlechtes Beispiel dienen. Ein paar Beispiele werden hier gesammelt.
Hoffen wir, dass die Anzahl überschaubar bleibt, aber mir schwant nichts Gutes.

Made in Germany
Wir erinnern uns: Am 23.08.1887 beschloss das Parlament des Vereinigten Königreichs den Merchandise-Markts-Act, der vorschrieb, dass auf Waren unmissverständlich das Herkunftsland anzugeben sei. Auslöser war, dass in der zweiten Hälfte des 19. Jahrhunderts Warenexporte aus europäischen Ländern (allen voran Deutschland) von minderer Qualität auf die Insel kamen. Die Briten wollten daher die Verbraucher im eigenen Land vor Schund aus dem Ausland warnen und so war das Siegel "Made in Germany" alles andere als ein Gütesiegel. Bekanntlich hat sich das nach dem Zweiten Weltkrieg verändert und Produkte "Made in Germany" galten über Jahrzehnte weltweit als das Non-Plus-Ultra. Aus dem Malus hatte sich ein Qualitätsmerkmal entwickelt.
Bei digitalen Produkten (und Dienstleistungen) haben wir in Deutschland jedoch längst den Anschluss verloren und bewegen uns vielfach auf dem Niveau eines Entwicklungslandes. Im Jahr 2025 kommt kein Smartphone oder Computer mehr aus deutscher Entwicklung oder Produktion. Die Big Five aus den USA diktieren, was wir im Bereich Betriebssystemen, Suchmaschinen, Online-Shops und Social Networks gefälligst zu konsumieren haben, und wir können dem nichts Adäquates entgegensetzen. Bei KI sieht es ähnlich düster aus. Hier wird es schon als Erfolg gefeiert, wenn wir in Unternehmen KI (aus Übersee) wenigstens produktiv einsetzen. Schaut man sich dagegen an, was deutsche Unternehmen, Behörden und Dienstleister an digitalen Produkten und Services anbieten und welche Güte und welchen Funktionsumfang (Nutzen) diese Dinge dann am Ende haben, treibt es einem die Schamesröte ins Gesicht. Hier sollten wir fairerweise wieder das Siegel "Made in Germany" als Warnung anbringen.
Sie denken, ich übertreibe? Oder Sie sind der Auffassung, dass das Schwarzseherei und Nestbeschmutzung ist? Dann schauen Sie sich mal die Beispiele an, die ich in meiner täglichen Arbeit mal als IT-Fachmann und mal als stinknormaler Anwender so finde. Alle paar Wochen mache ich eine Kiste auf und packe voll in die Sch....
Was ist die Konsequenz? Niemand ist unnütz. Er kann immer noch als schlechtes Beispiel dienen, wie man es besser nicht macht. Aber auch das reicht nicht. Wir müssen auch im Bereich "Digitalisierung" mit allen Nebenkriegsschauplätzen wie "IT-Sicherheit" und "Datenschutz" an die Weltspitze kommen, um dauerhaft überlebensfähig zu sein (und das nicht nur in wirtschaftlicher Hinsicht). Wer nicht in der Lage ist, Software wenigstens einigermaßen fehlerfrei zu programmieren und sie mit etablierten Standard-Verfahren Security-technich gegen Missbrauch und Kompromittierung abzusichern, der soll sich bitte schulen lassen und schlaumachen, wie es geht. Aber bitte nicht: Weiter so und "die Ware reift beim Kunden". Computer sind keine Bananen und wir sind keine Bananenrepublik. Auf geht's!

Ich habe ja immer gesagt: So ein Thermomix ist Teufelswerk.

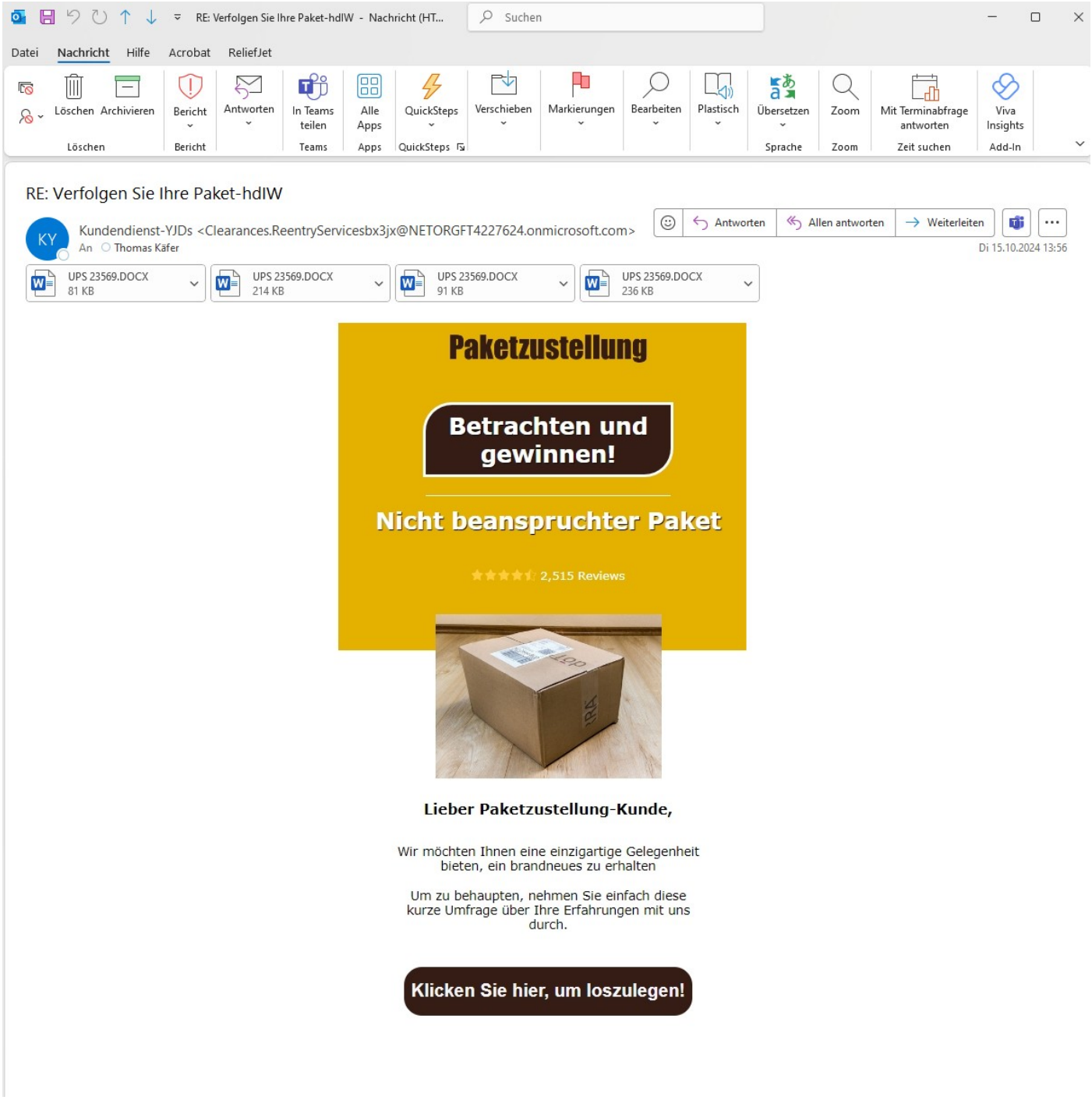
Aber was daran überhaupt nicht lustig ist, dass nun eine Million Nutzerdaten im Darknet verhökert werden. Auch das ist "Digitale Inkompetenz".

https://www.heise.de/news/Datenleck-bei-Thermomix-Daten-von-1-Million-deutscher-Nutzer-im-Darknet-10273696.html

Digitale Inkompetenz jetzt auch in Österreich:
https://on.orf.at/.../fax-verbot-bringt-chaos-ins...
Quelle: ORF
Seit Anfang 2025 gilt im österreichischen Gesundheitswesen aus Datenschutzgründen ein Faxverbot. Und das sorgt derzeit für ein Chaos, obwohl das Ende des Faxsystems bereits 2012 beschlossen worden ist, habe man verabsäumt, ein funktionierendes Ersatzsystem zu entwickeln, kritisiert die Ärztekammer.
13 Jahre Digitalisierung verpennt? Das könnte uns in Deutschland nicht passieren. So schnell sind wir nicht.

MADE IN GERMAYN MALLUS

Digitale Inkompetenz: hier Sonos
31. Dezember 2024 von Thomas Käfer
Digitale Inkompetenz Folge 543 – Heute Sonos
Wie könnte es anders sein? Wir schließen das Jahr 2024 mit einer neuen Folge „Digitale Inkompetenz“.
Ich habe den Fehler gemacht und mir für die heutige Silvesterparty noch ein drittes Sonos Roam zuzulegen. Was eigentlich eine Sache von fünf Minuten sein sollte, stellte sich als eine Operation von 5 Stunden, davon 3 Stunden mit dem Support von Sonos heraus. Das neue Gerät ließ sich nicht nur in das vorhandene System integrieren, sondern der Support hat es dann noch geschafft, mir auch das funktionierende Gerät Nr. 2 zu zerschießen. Nach drei Stunden gemeinsamer Fehleranalyse hat der freundliche Mensch sich dann entschuldigt und aufgegeben. Man würde sich in den kommenden Tagen bei mir melden und sicher eine Lösung finden.
Am Ende hatte ich dann nach dem Ausschlussverfahren die entscheidende Idee: Ich habe den Sonos Boxen eine feste IP-Adresse aus dem Class-C-Subnetz gegeben, in dem sich auch der Router befindet: Also anstatt 192.168.1.x mit einer Subnet Mask von 255.255.240.0 liegen die Sonos Boxen jetzt auf festen IPs im 192.168.0.0 Netz mit 255.255.255.0. Sonos kommt offenbar nicht damit klar, dass es außer dem Deppen-Subnetz 255.255.255.0 auch „kompliziertere“ Netzwerke geben könnte. Damit sind bei uns schon reihenweise Azubis auf die Fresse geflogen. Wie ich es hasse, wenn IT-Leute ihr Handwerk nicht beherrschen. Damit ist nur das Symptom behoben, nicht, dass die Boxen intelligent und formal nach Standard sauber programmiert wären.
Bei Sonos ist bescheidene Software (um es diplomatisch auszudrücken) Tradition. Wenn die Boxen einmal funktionieren, sind die prima, aber die Apps dazu kann man in der Pfeife rauchen. Bloß nichts mehr verändern!
Setzen: Sechs.
Wenigstens kann jetzt die Party steigen. Guten Rutsch! Und möge 2025 wenigstens IT-technisch besser werden als das 2024.



Alles umsonst!
15. Oktober 2024 von Thomas Käfer
Oh geil. Es gibt etwas umsonst. Da schalte ich mein Gehirn aus und überlese auch die Tippfehler und das schlechte Deutsch. Und vier Word-Dokumente als Anhang sind doch auch keine Gefahr, oder? Hey, und immerhin 2.500 Rezensionen mit fast fünf Sternen. Also los! Ab ins Verderben.


Marco Saile
Präsident TSV Ehningen 1914 e.V.
Link zur Besprechung:
https://teams.microsoft.com/dl/launcher/launcher.
html?url=%2F_%23%2Fl%2Fmessage
%2F19%3Ad11231ef4a504d27a5535da
5024979ad%40thread.tacv2%2F1614670582832
%3FtenantId%3D1344368c-4b25-41e2-
b80c-c7775488879e0%26groupId
%3D33142804-7882-458d-9a37-7de1f
94906be%26parentMessageId%3D
1614670582832%26teamName%3
DPr%25C3%25A4sident%26channelName
%3DAllgemein%26createdTime%3
D1614670582832&type=message&
deeplinkId=f62b559c-1990-4733-87a2-aa1563
ab321b&directDl=true&msLaunch=true&enable

Entwarnung: Digitalisierung der Bahn
6. September 2024 von Thomas Käfer
Am heutigen Morgen (06.09.2024) kam die Nachricht in den Medien, dass die Deutsche Bahn die Digitalisierung der Stellwerke stoppt. Stattdessen baut man zunächst mal Technik aus den 90er Jahren ein.
Man könnte sich an den Kopf fassen oder diesen schütteln.
Aber Entwarnung: Es handelt sich laut Bahn um „etablierte Technik“. Ja dann!
Das (!) meine Damen und Herren ist der Stand der Digitalisierung in Deutschland.
Ich hätte noch ein paar Computer beizusteuern. Auch Stand der Technik der 90er Jahre.
Kostenlos abzugeben.





Deutschlandtakt braucht noch gut 40 Jahre, bis er vollständig umgesetzt wird.

3. März 2023 von Thomas Käfer

Heutige Schlagzeile: Deutschlandtakt braucht noch gut 40 Jahre, bis er vollständig umgesetzt wird.

Darüber machen wir jetzt bitte keine Witze!

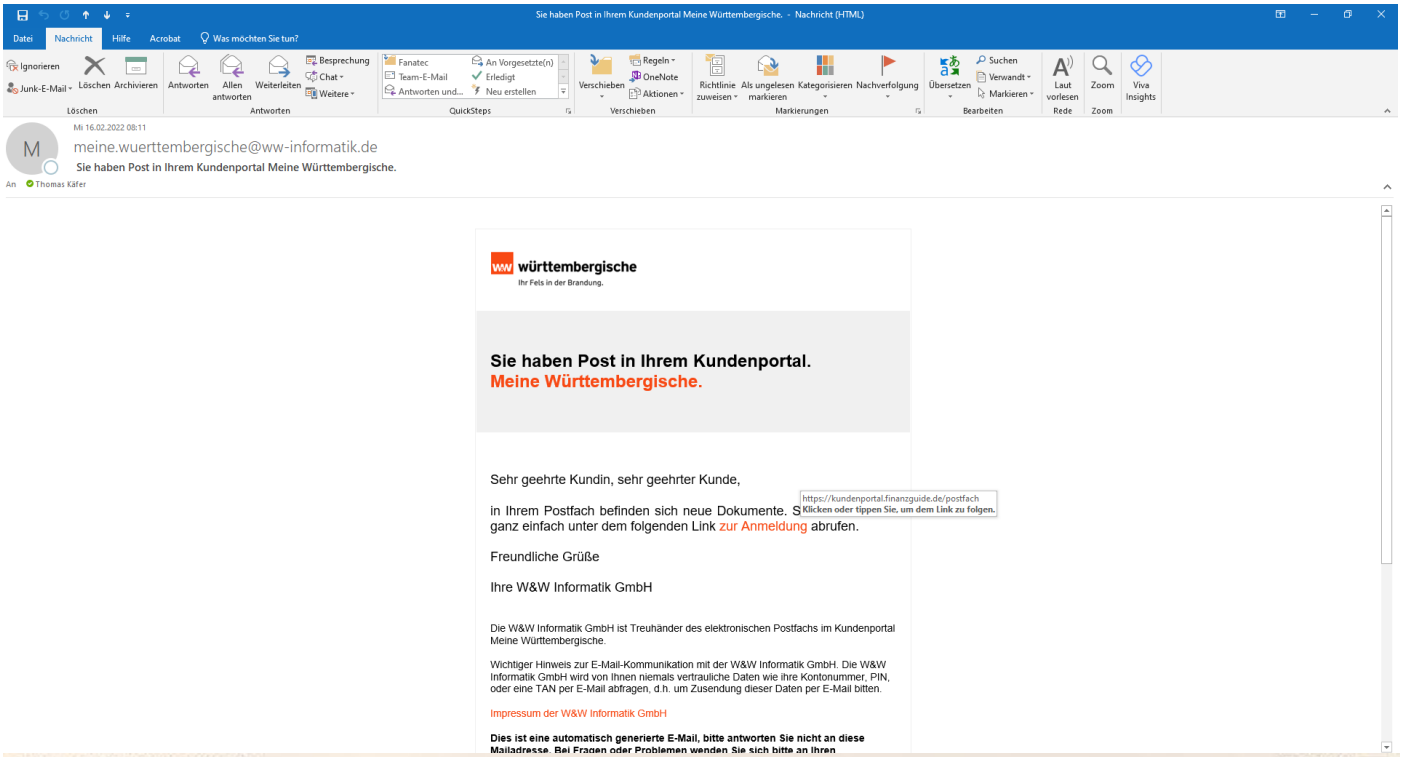
Die Erklärung, warum das jetzt doch so lange dauert (also etwa bis 2070), alle Fernzüge in einen 30-Minutentakt zu synchronisieren, ist ganz einfach.

40 Jahre dauert es, bis zunächst die Generation Menschen geboren und aufgewachsen ist, die dann später die Ausbildung und die Detailplanung der Menschen durchführt, die in 20 Jahren geboren werden und dann eben weiter 20 Jahre später Lokführer, Verkehrspolitiker, Weichenwärter oder Programmierer für automatisiert fahrende Züge werden.

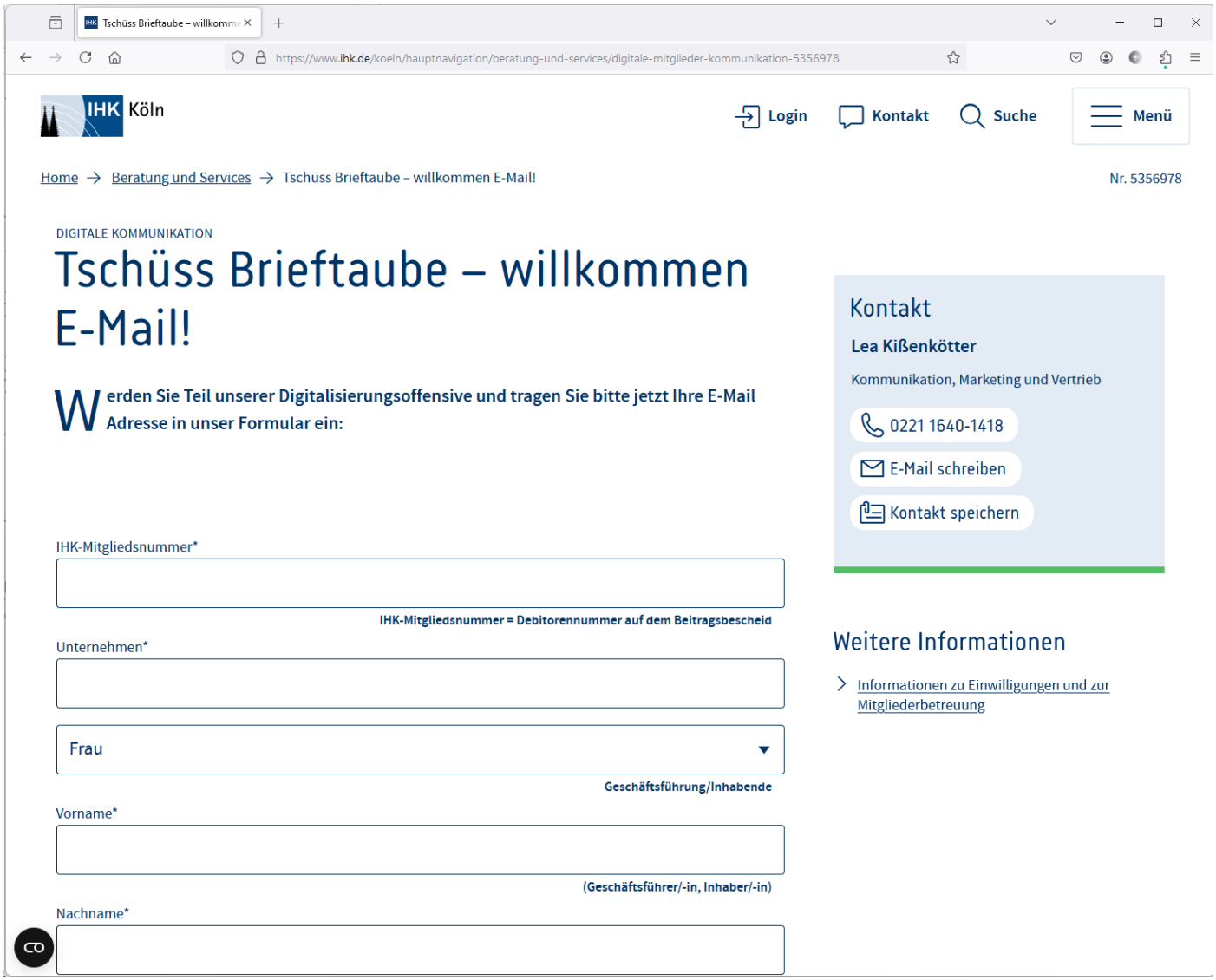
Das ist nicht lustig. Können wir das wirklich nicht besser?

Vorschlag an die Klimakleber, die gerade auf der Straße sitzen: Macht Ihr doch mal was Konstruktives und baut den Deutschlandtakt in den nächsten 5 Jahren! Aber dafür müsst Ihr jetzt ganz schnell wieder in die Schule und die Uni zurück. Husch!

P.S. Teaserbild mit KI generiert – Auftrag für die KI „Mann mit Kind an der Hand steht auf dem Bahnsteig und wartet auf den Zug“. Vielleicht sollten wir mal die KI fragen, wie das mit dem Deutschlandtakt schneller gehen könnte. Wir sind ja offenbar zu doof dafür.


Sie haben Post in Ihrem Kundenportal Meine Württembergische. - Nachricht (HTML)
Datei
Nachricht
Hilfe
Acrobat
Was möchten Sie tun?
Ignorieren
Junk-E-Mail
Löschen
Archivieren
Antworten
Allen antworten
Weiterleiten
Besprechung
Chat
Weitere
Fanatec
Team-E-Mail
Antworten und...
An Vorgesetzte(n)
Erledigt
Neu erstellen
Verschieben
Regeln
OneNote
Aktionen
Richtlinie zuweisen
Als ungelesen markieren
Kategorisieren
Nachverfolgung
Übersetzen
Suchen
Verwandt
Markieren
Laut vorlesen
Zoom
Viva Insights
Mi 16.02.2022 08:11
meine.wuerttembergische@ww-informatik.de
Sie haben Post in Ihrem Kundenportal Meine Württembergische.
An Thomas Käfer
württembergische
Ihr Fels in der Brandung.
Sie haben Post in Ihrem Kundenportal.
Meine Württembergische.
Sehr geehrte Kundin, sehr geehrter Kunde,
in Ihrem Postfach befinden sich neue Dokumente. S
ganz einfach unter dem folgenden Link zur Anmeldung abrufen.
https://kundenportal.finanzguide.de/postfach
Klicken oder tippen Sie, um dem Link zu folgen.
Freundliche Grüße
Ihre W&W Informatik GmbH
Die W&W Informatik GmbH ist Treuhänder des elektronischen Postfachs im Kundenportal Meine Württembergische.
Wichtiger Hinweis zur E-Mail-Kommunikation mit der W&W Informatik GmbH. Die W&W Informatik GmbH wird von Ihnen niemals vertrauliche Daten wie Ihre Kontonummer, PIN, oder eine TAN per E-Mail abfragen, d.h. um Zusendung dieser Daten per E-Mail bitten.
Impressum der W&W Informatik GmbH
Dies ist eine automatisch generierte E-Mail, bitte antworten Sie nicht an diese Mailadresse. Bei Fragen oder Problemen wenden Sie sich bitte an Ihren


Mail 15:25 Samstag 2. Okt.
100 %
9. September
19:29
LIVE
00:50
No connection!
05214572



Digitalisierungsoffensive der IHK Köln

6. August 2024 von Thomas Käfer

1. **Absolut vorbildlich: IHK Köln stellt von Brieftaube auf E-Mail um.**
2. **Ich habe zwei Fragen:**
3. **Gibt es dieses „Fax“ nicht mehr und überspringen wir hier nicht einen Schritt?**
4. **Ist das alles? Also in Richtung Digitalisierung? E-Mails schicken ist noch keine Digitalisierung.**
5. **Aber ich soll ja nicht immer nur meckern und einer meiner Professoren im Erststudium sagte immer: Man kann seine Erwartungen so niedrig ansetzen, dass man irgendwann positiv überrascht wird.**

6. **Weiter so!**

7. **Wer jetzt sagt: Die sind aber spät dran, hat recht. Die erste E-Mail in Deutschland wurde vor ziemlich genau 40 Jahren verschickt (am 03.08.1984). Vielleicht wollte man der IHK Köln warten, bis das System einigermaßen ausgereift ist. Oder zum Geburtstag gratulieren…**

Zu diesem Fall passt eine Entscheidung von mir von 2021:

Jetzt haben wir das Faxen dicke…
6. Februar 2021 von Thomas Käfer
Das Fax hat ausgedient und gehört abgeschafft. Man muss sich auch einmal von Errungenschaften des vergangenen Jahrhunderts verabschieden. Und es kann vor allem nicht angehen, dass wichtige und dringende Nachrichten noch per Fax übertragen werden – so geschehen während der Pandemie bei der Übermittlung von Fallzahlen und Infektionsmeldungen. So fordern viele gerade angesichts der Herausforderungen von Corona zur Digitalisierung eine schnelle Abschaltung der Faxgeräte in Behörden und Ämtern. Ein Fax ist nicht digital – auch wenn es Pieptöne von sich gibt und bei Empfang einer Nachricht blinkt.
Doch halt. Einfach nur den Stecker ziehen, ist jetzt auch keine Lösung und wieder mal zu kurz gesprungen. Denn warum sind die ollen Fax-Geräte noch so „beliebt“ und im Einsatz? Es gibt zwei gute Gründe: Rechtssicherheit und Vertraulichkeit. Zum einen wird eine Unterschrift auf einem Fax-Dokument als rechtssicher angesehen, was bei einer einfachen nicht qualifiziert digital signierten E-Mail nicht der Fall ist. Lösung hier: Qualifizierte Digitale Signaturen verwenden und auch auf allen Seiten die notwendigen Voraussetzungen zum Versand und zur Annahme schaffen. Die Gesetze, die das ermöglichen, gibt es schon seit zwei Jahrzehnten! Nur mit der Infrastruktur (Endgeräte, Software) dafür haperts es seit langem.
Zum anderen kann i.d.R. bei einem Fax-Versand von personenbezogenen Daten davon ausgegangen werden, dass die Daten nur an den gewünschten Empfänger übermittelt werden und nicht von Dritten mitgelesen werden können (Punkt zu Punkt Verbindung). Das ist zwar technisch möglich, aber weit aufwändiger als eine unverschlüsselt übertragene E-Mail mitzulesen oder aus versehen an eine Vielzahl von Empfängern weiterzuleiten. Daher raten Datenschützer zum Griff zum Fax-Gerät, wenn es um den Transport von personenbezogene Daten geht und es keine verschlüsselte digitale Übertragung gibt (auch wenn das durch ein Urteil des OVG Lüneburg Beschluss vom 22.07.2020 11 LA 104/19 mittlerweile auch anders gesehen wird). Denn das unverschlüsselte Senden ist genau das Problem. Einfach eine Liste mit Adressen oder gar Patientendaten mit Befunden per E-Mail zu verschicken, ist unzulässig. Zu groß ist die Gefahr, dass diese Daten in fremde Hände geraten. Also verschlüsseln! Richtig blöd ist es dann aber, das Passwort für die verschlüsselten Daten (Anhänge) mit in die Mail zu packen. Sehr clevere Zeitgenossen greifen daher zu diesem überwältigend logischen Trick und schicken das Passwort in einer separaten Mail. Darauf muss man erst einmal kommen. Nun, der Datendieb, der Zugriff auf die Mail mit den verschlüsselten Anhängen hat, wird mutmaßlich dann über denselben Weg auch die zweite Mail mit dem Passwort abfangen. Also nicht wirklich clever. Umso erstaunlicher, dass Gesundheitsämter und andere Behörden mit Segen der dortigen Datenschutzbeauftragten genau diesen Weg gehen bzw. fordern. Entweder wird einfach nur platt die Zusendung von personenbezogenen Daten per E-Mail gefordert (ohne ein Wort über den Schutz der Daten zu verlieren) oder es wird (bei Intervention des betrieblichen Datenschutzbeauftragten der Gegenseite) dann von der Behörde bzw. deren Datenschutzbeauftragten die zweite Version dem Passwort in der separaten Mail vorgeschlagen. Der betriebliche Datenschutzbeauftragte bleibt da nur noch kopfschüttelnd zurück. Das kann es nicht sein, denn auch eine Pandemie bricht nicht die DS-GVO. Lösung: Entweder man verständigt sich auf separatem und sicherem Weg (Telefon) auf ein Passwort für die Verschlüsselung oder die Behörden schaffen endlich Portale und Upload-

Möglichkeiten, mit denen die vertraulichen Daten zeitgemäß verschlüsselt und zielgerichtet übertragen und gesichert werden. So ein Portal einzurichten, schafft ein IT-Azubi in einem Tag, oder wenn es richtig gut werden soll, in einer Woche. Also los! Und dann können wir auch den Stecker vom Fax-Gerät ziehen.
Übrigens: Die neue „Lösung“, anstelle von echten Fax-Geräten nun digitale Schnittstellen mit einer automatischen Konvertierung von Faxen von bzw. in E-Mails (Fax-to-E-Mail oder E-Mail-to-Fax) ist keine Lösung im Sinne des Datenschutzes. Hierbei wird das an sich sichere Verfahren einer früher leitungsgebundenen Kommunikation zwischen zwei Endpunkten, die extrem schwer abhörbar war, dadurch ausgehebelt, dass heutzutage die Fax-Daten über VoIP-Netze geroutet und dann mittels klassischer (unverschlüsselter) E-Mail weitertransportiert werden. Da kann man die Nachricht auch direkt wieder als Klartext-E-Mail schicken.

P.S: Ich habe immer noch eine Fax-Nummer, die auf meiner Fritz-Box aufgeschaltet ist (kostet ja nix), aber dort kommt alle Paar Monate nur SPAM und Betrugszeugs an siehe FAX vom 31.01.2025

Fall 1: DWD

Stand der Digitalisierung in Deutschland

Hier: Sicherheitslücke beim pc_met Metrologie-Dienst www.flugwetter.de des Deutschen Wetterdienstes (DWD)

Autor: Dipl.-Ing. Thomas Käfer, M.Sc. – 05.08.2024

Als Pilot der allgemeinen Luftfahrt ist man verpflichtet, vor jedem Flug eine sorgfältige Flugplanung durchzuführen. Zur Flugvorbereitung gehört insbesondere, dass man sich über die Wetterbedingungen auf der geplanten Flugstrecke informiert.

Nun ist der Autor nicht nur Privat-Pilot (mittlerweile mit einer gültigen PPL(A) Lizenz mit Musterberechtigung für einmotorige Flugzeuge mit einer MTOW von max. 2 to) sondern auch Fachmann für IT-Security und Datenschutzthemen.

So kam es, dass er sich im Rahmen der seinerzeit noch laufenden Pilotenausbildung am 04.04.2024 ein Benutzerkonto beim Deutschen Wetterdienst zulegte und den kostenpflichtigen Wetterdienst „pc_met“ buchte. Der Deutsche Wetterdienst (Bundesoberbehörde im Geschäftsbereich des Bundesministeriums für Digitales und Verkehr) stellt im Rahmen seiner gesetzlichen Aufgaben meteorologische Informationen im Selfbriefing-System „pc_met Internet Service“ (www.flugwetter.de) zur Verfügung.

Mit großer Verwunderung hat der Autor dann den Registrierungsvorgang für ein Jahresabo Flugwetter.de (pc_met) abgeschlossen. Das erste Wunder: Bei der Bestellung sollte ein achtstelliges Passwort ohne Umlaute und Sonderzeichen angegeben werden.

In der Maske wurde es als „Wunschpasswort“ tituliert, was den Eindruck erwecken könnte, dass man es später ändern könnte. Weit gefehlt.

Die Eingabe einer reinen Zahl, wie hier exemplarisch „12345678“, wurde problemlos akzeptiert.

Das entspricht alles nicht gängigen Sicherheitsstandards. Nach heutigem Stand beträgt die Mindestlänge eines Passwortes 8 Zeichen (eher mehr) und sollte nicht auf diese Anzahl maximal beschränkt sein. Gerade durch das Einbauen von Sonderzeichen wird die Kennwortsicherheit erheblich gestärkt. Zudem sind Buchstaben in Groß- und Kleinschreibung und Zahlen gemischt zu verwenden und moderne Portale prüfen so etwas vorab, bevor sie die Verwendung eines schwachen Passwortes überhaupt zulassen. Anschließend wird jedoch nicht das Passwort im

Klartext, sondern immer nur ein sogenannter HASH-Wert davon im System gespeichert, gegen den das nachher vom Nutzer eingegebene Passwort abgeglichen wird. Der HASH verhindert (richtig implementiert), dass das gespeicherte Kennwort in Klartext zurückgewandelt werden kann. Grundsätzlich gilt: Je länger das Passwort, umso sicherer. Und die Kontosicherheit steht und fällt mit der Absicherung der Website gegen Brute-Force-Attacken. Wird das systematische Durchprobieren des 8-stelligen Zeichenvorrats konsequent eingedämmt, dann ist die Gefahr gering. Aber ob dem so ist, könnte nur ein Penetration-Test zeigen, für den der Autor weder die Legitimierung noch die Lust hat, auch das noch unentgeltlich zu prüfen.

Zurück zum Registrierungsprozess: Des Weiteren war eine Mobilfunknummer für die Übermittlung des Passwortes anzugeben. Das macht wiederum stutzig. Eine Mobilfunknummer als zweiter Faktor bei einem Multi-Faktor-Authentifizierungsprozess ist üblich und eine gute Idee, aber warum wird hier ein Passwort im Klartext übermittelt? Vor allem, wo man es doch selbst als Wunschpasswort angeben muss? Das Mitlesen von SMS ist zwar deutlich schwieriger als bei E-Mais, aber man versendet hierüber höchstens Einmal-Passwörter oder temporäre Codes als zweiten Faktor bei einem Login.
Anmeldemaske DWD pc_met

Aber es kommt noch „besser“. Zunächst wurde vor Absenden des Warenkorbes noch die Mobilrufnummer für die Kennwortübermittlung wiederholt dargestellt. So weit – so gut.
Bestellbestätigung pc_met

Dann der Hammer. Das zuvor gewählte Passwort wurde nun im Klartext zusammen mit der Bestellbestätigung an die im Bestellprozess angegebene E-Mail Adresse verschickt.
Bestellbestätigung pc_met

Anmerkung: Das hier gezeigte Passwort 12345678 wurde natürlich nicht vom Autor verwendet und ist hier nur zu Illustrationszwecken eingefügt. Aber es wäre ein mögliches Passwort gewesen. An dieser Stelle stand jedoch das echte vom Autor gewählte Passwort.

Das macht man schon mal überhaupt nicht (Wunder 2), denn jeder sollte mittlerweile wissen, dass eine E-Mail grundsätzlich unverschlüsselt übertragen wird und der Weg, den die Nachricht vom Absender zum Empfänger nimmt, nicht vorherzusagen ist. Auch wenn heutzutage Teile der Kommunikation verschlüsselt übertragen werden, darf man sich darauf bei einer E-Mail nicht verlassen.

Und dann wird dem Nutzer dieses Passwort per SMS zugeschickt, was aus zweierlei Gründen unsinnig ist, da er es ja selbst gewählt hat und es zweitens in der E-Mail Bestätigung enthalten war.

Jetzt kommt Wunder 3: Unter Flugwetter.de findet man keinen Punkt, wo man das nun als kompromittiert geltende Passwort in ein geheimes, nur dem Nutzer bekanntes ändern könnte (ebenfalls gültiger Sicherheitsstandard).

Besonders schlimm: Würde man dieses Passwort auch an anderer Stelle benutzen (was bei vielen Usern nicht unüblich ist), gelten auch diese Accounts ab sofort als gefährdet. Und das ist hier die eigentliche Gefahr: Mit dem bei DWD erbeuteten Passwort kann ein fremder Dritter nicht viel anfangen, denn er kommt damit nicht in ein Portal beim DWD, um z.B. Bezahlinformationen wie z.B. Kontonummern auszulesen. Diese Funktionen gibt es gar nicht. Er könnte nur ein Jahr lang den Flugwetterdienst nutzen. Also ist zu hoffen, dass kein Nutzer dasselbe Passwort an anderer Stelle nutzt, wo es mehr Schaden anrichten kann.

Nur noch als Sahnehäubchen zu so viel Security-Inkompetenz: Es gibt offenbar keinen Link, über den man das Passwort anfordern könnte, wenn man es denn einmal vergessen hat (wobei es auch dann nicht im Klartext übermittelt werden, sondern nur ein Reset-Link verschickt werden dürfte).

Das ganze ist umso überraschender, als das der Deutsche Wetterdienst (DWD) eine dem Bundesministeriums für Digitales und Verkehr unterstellte Institution ist und er für die Erfüllung der meteorologischen Erfordernisse aller Wirtschafts- und Gesellschaftsbereiche in Deutschland zuständig ist (Die Aufgaben basieren auf einem gesetzlichen Informations- und Forschungsauftrag, dem Gesetz über den Deutschen Wetterdienst.). Da gilt wieder einmal der Spruch „Der Schuster hat die schlechtesten Schuhe“ und mit solch mangelhafter Umsetzung sind wir weit von einer Digitalisierung in Deutschland entfernt.

Responsible Disclosure:

Nun ist der Vorfall gut vier Monate her und der Autor hat selbstverständlich den DWD um eine Stellungnahme zu diesen Unzulänglichkeiten und insbesondere, ob die Passwörter im Klartext in den Systemen gespeichert werden, aufgefordert. Schade, dass es vorher niemand anderem aufgefallen war.

Nun kommen die guten Nachrichten.

Der DWD hat sich innerhalb weniger Tage beim Autor gemeldet und den Vorwurf bestätigt. Aber mehr noch. Man hat nach eigenen Angaben umgehend das Versenden der Kennwörter im Klartext in der E-Mail-Benachrichtigung deaktiviert und Maßnahmen projektiert, um das System auf einen adäquaten und modernen Sicherheitsstandard umzubauen. In den folgenden Wochen gab es daher einen intensiven Austausch über die Planung und den Umsetzungsstand und man geht seitens des DWD davon aus, dass ein neues System in Q4/2024 bzw. Anfang 2025 in Betrieb gehen wird. Das ist nicht besonders schnell, aber Sorgfalt geht im Zweifelsfall vor Schnelligkeit. Das ist schon einmal als professionelle Reaktion zu begrüßen.

Einem wesentlichen Kritikpunkt des Autors ist der DWD nun am 31.07.2024 nachgekommen, nämlich der Benachrichtigung aller pc_met-Benutzer, dass diese prüfen, ob sie dasselbe Passwort auch auf anderen Plattformen oder Diensten verwenden. Dann wird dringend empfohlen, dieses dort zu ändern.

Im Rahmen des Responsible Disclosures erfolgt daher erst jetzt die Veröffentlichung der Sicherheitslücke, damit der Betreiber ausreichend Zeit für das Schließen der Angriffsfläche hat. Eine Veröffentlichung ist jedoch allein deshalb nötig, um den Druck auf den Betreiber aufrecht zu erhalten, alle in diesem Zusammenhang stehenden Lücken zu schließen. Die Erfahrung an anderer Stelle zeigt, dass, ohne Veröffentlichung nach üblicherweise 90 Tagen, gefundene Lücken nie oder nicht zeitnah geschlossen werden.

Der DWD geht in seiner Benachrichtigung nicht davon aus, dass es sich um eine Datenpanne handelt und er keine Anhaltspunkte dazu hat, dass Dritte auf Ihre Daten zugegriffen haben.

Eine Datenpanne ist es nach Auffassung des Autors sicherlich, aber es ist zu hoffen, dass tatsächlich kein Hacker auf die Datenbank des DWD bzw. das E-Mail-Postfach des Sendmail-Prozesses zugreifen konnte, denn die ganzen User-Passwörter müssen dort im Klartext herumliegen bzw. vorhanden gewesen sein. Ansonsten wäre ein Versand im Klartext nicht möglich gewesen.

Schlecht ist, dass das als kompromittiert geltende Passwort im DWD-System nun weiterhin erst einmal nicht geändert werden kann und unklar ist, ob die Passörter nun tatsächlich nur noch als HASH gespeichert abgelegt sind. Auch wenn das bei einem nur 8-stelligen Passwort heutzutage auch kein ausreichender Schutz gegen das Entschlüsseln ist, wäre das zumindest ein erster Schritt in Richtung mehr IT-Security. Gefährlich wird es aber hier, wenn ein Angreifer die gesamte Datenbank der schwachen Passwörter bzw. deren HASH-Werte erbeuten kann. Für 8-stellige Passwörter gibt es im Darknet Rainbow-Tabellen mit zugehörigem Klartext zu kaufen.

Man sieht: IT-Security ist komplex und gehört in professionelle Hände.

Fazit: Nach der haarsträubend schlechten Umsetzung von IT-Security und Datenschutz im System pc_met hat der DWD in der Folge sehr professionell reagiert. Dem Autor liegen Details zur geplanten Umsetzung vor, die aus Sicherheitsgründen nicht veröffentlicht werden, aber das Vertrauen erhöhen, dass zukünftig ein heutigen Standards der IT-Sicherheit und Datenschutz entsprechendes System aufgebaut wird.

Dem Dienstherrn „Bundesministeriums für Digitales und Verkehr“ incl. dem zuständigen Bundesdatenschutzbeauftragten muss man vorhalten, dass beide ihrer Aufsichtsplicht offenbar nicht nachgekommen sind. Ob sie es nun tun, bleibt abzuwarten, denn auch das neue System bedarf spätestens nach Inbetriebnahme (besser schon vorher) einer externen fachlichen Überprüfung.

Positiv an der ganzen Sache ist, dass sie als Anschauungs-Beispiel für andere dienen kann, wie man es definitiv nicht machen darf.

So, und nun loggen wir uns mal wieder ins pc_met ein und schauen, ob das Wetter mitspielt und wir fliegen können. Denn das war die eigentliche Aufgabenstellung.
Fall 2: IHK Business Network

Versand von Gerichtsakten per USB-Sticks
2. August 2024 von Thomas Käfer
Stand der Digitalisierung in Deutschland
Hier: Versand von Gerichtsakten per (unverschlüsselten) USB-Sticks
Autor: Dipl.-Ing. Thomas Käfer, M.Sc. – 02.08.2024
Wie sieht es bezüglich des Standes der Digitalisierung in Deutschland aus? Schlecht!
Ein besonders krasser Fall von Digitalinkompetenz fiel dem Autor Thomas Käfer im Rahmen seiner Sachverständigentätigkeit als gerichtlich bestellter Gutachter im März 2024 auf.
Um den Beteiligten genügend Zeit zu geben, auf die seinerzeit geäußerte Kritik angemessen und vor allem mit Abhilfemaßnahmen zu reagieren, erfolgt erst jetzt im August 2024 eine Veröffentlichung – leider ohne, dass sich irgendetwas nachhaltig getan hätte.
Die Protagonisten:
Ein Amtsgericht
Das Bundesjustizministerium
Die IHK Aachen
Im Rahmen seiner Tätigkeit als öffentlich bestellter und vereidigter Sachverständiger erhielt der Autor im März 2024 den Auftrag zur Untersuchung eines Computers im Rahmen eines Zivilprozesses. Zum zweiten Mal kam die Gerichtsakte nicht, wie bisher üblich, als Original in Papierversion, sondern digitalisiert (eingescannt) auf einem USB-Stick. Das Passwort zu dem angeblich verschlüsselten USB-Stick kam einen Tag später ebenfalls per Post in einem separaten Schreiben.
Die Überraschung war groß, als der Autor feststellte, dass sich die auf dem Stick vorhandene PDF ohne jegliche Passworteingabe öffnen ließ. So viel zur Verschlüsselung.
Aber auch das Passwort konnte nicht wirklich überzeugen. Es war so trivial aufgebaut, dass man davon ausgehen muss, dass andere USB-Sticks mit anderen Gerichtsakten mit logischem Abändern des verwendeten Passwort-Schemas leicht zu erraten sind. Wenn denn die Sticks diesmal verschlüsselt sind.
Alles halb so wild? Auf den ersten Blick vielleicht. Fehler passieren. Aber: Es geht um einen Zivilprozess (es könnte auch ein Strafprozess sein), dessen Details erst einmal nicht der breiten Öffentlichkeit zugänglich gemacht werden sollen (auch wenn Gerichtsprozesse selbst i.d.R. öffentlich sind, aber das ist wohl nicht damit gemeint).
Dem gerichtlichen Sachverständigenauftrag lag ein Schreiben bei, das Anweisungen an den Sachverständigen zum Umgang mit dem USB-Stick enthielt und ihm datenschutzrechtliche Verpflichtungen auferlegte, die nach seiner Meinung so rechtlich nicht haltbar sind.

Zitat: *Bitte beachten Sie die damit verbundenen datenschutzrechtlichen Folgen:*
Bei der elektronischen Überlassung einer Verfahrensakte zum Zwecke der elektronischen Akteneinsicht handelt es sich um eine Verarbeitung personenbezogener Daten.
Hierbei sind die Grundsätze aus Art. 5 Datenschutz-Grundverordnung (DS-GVO) einzuhalten. Die Verarbeitung in Form der Gewährung von elektronischer Akteneinsicht findet ihre Rechtsgrundlage in der anwendbaren Verfahrensordnung i.V.m. Art. 6 Abs. 1 Buchst. e DS-GVO i.V.m. §.3 BDSG, § 3 DSG NRW.
Betroffene, deren personenbezogene Rechte durch die Akteneinsicht betroffen sind, wurden gemäß den Artikeln 12 ff. DS-GVO, 32 ff. BDSG, § 11 ff. DSG NRW durch ein Informationsschreiben informiert. Dieses Schreiben unterrichtet den Betroffenen insbesondere über die mögliche Weitergabe der Akte an Akteneinsichtsberechtigte und belehrt ihn über seine weiteren Rechte.
Mit dem Übergang des USB-Sticks in Ihre Verfügungsgewalt gehen sämtliche Pflichten als datenschutzrechtlicher Verantwortlicher auf Sie über.
Nach Art 24 DS-GVO setzt der Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der Datenschutz-Grundverordnung erfolgt.
Dies schließt die Informationspflicht mit dem Inhalt der Art. 13, 14 DSGVO, §§ 32 und 33 BDSG, § 11 DSG NRW ein.
Um zu vermeiden, dass die datenschutzrechtlichen Pflichten andauern und Sie für deren Einhaltung die Verantwortung tragen, wird ausdrücklich angeregt, die personenbezogenen Daten auf dem USB Stick nach Erhalt und Einsichtnahme umgehend (revisionssicher) zu löschen.
Zitat Ende
Das ist der eigentliche Hammer. Es ist nach Ansicht des Sachverständigen mitnichten so, dass die Verantwortliche (hier das Gericht) die Verantwortlichkeit im Sinn der DS-GVO auf den Sachverständigen (also einen Dritten) übertragen kann. Das Gericht bleibt Verantwortliche.
Jetzt kann man trefflich darüber diskutieren, ob der Sachverständige Auftragsdatenverarbeiter im Sinn der DS-GVO wird. Dann müsste das Gericht einen AVV mit ihm schließen. Auch diese Rolle ist eher zu verneinen.
Also bleibt noch die Rolle als Dritter oder Empfänger personenbezogener Daten in der Lesart der DS-GVO. Selbstverständlich ist ein ö.b.u.v. Sachverständiger allein schon aufgrund seiner Bestellung zur Verschwiegenheit und zum sorgsamen Umgang mit allen Daten rund um einen Gutachtenauftrag verpflichtet, aber er wird nicht zum (alleinigen oder gemeinsamen) Verantwortlichen nach DS-GVO.
Und auch die Hinweise auf das Auskunftsrecht des Betroffenen sind überraschend und stehen im direkten Widerspruch zur Rollenverteilung vor Gericht. Der Sachverständige ist sachkundiger Gehilfe des Gerichts und weder Partei noch Herr des Verfahrens. Somit liegt das alleinige Auskunftsrecht beim Gericht.
Sehr schön, aber leider praxisfremd ist die Aufforderung, den Stick alsbald revisionssicher zu löschen, damit die (angeblich übertragenen) datenschutzrechtlichen Pflichten nicht andauern. Bei einer Papierakte wird diese nach Abschluss des Gutachtens wieder an das Gericht zurückgegeben. Nur wichtige Auszüge bleiben als Kopie i.d.R. beim Gutachter für den Fall, dass es später Rückfragen gibt bzw. diese zum Verständnis des Gutachtens notwendig sind. So etwas speichert man als Sachverständiger üblicherweise nach Stand der Technik gesichert auf eigenen Systemen mit entsprechender Zugangssicherung. Das würde sich auch für die PDF anbieten, aber wird ja nicht empfohlen. Also weg damit! Und zwar schnell!
Sollten später tatsächlich Rückfragen gestellt werden, müsste dem Sachverständigen erneut die Gerichtsakte (digital) zugestellt werden.
Warum so kompliziert? Dafür gibt es doch ein elektronisches Akteneinsichtsportal und/oder ein elektronisches Justizpostfach. Über beide Systeme könnten Daten gesichert übertragen werden.
Bei letzterem kommt jetzt die IHK ins Spiel. Wenige Tage vor Weihnachten 2023 informierte die IHK Aachen, dass ö.b.u.v. Sachverständige ab dem 01.01.2024 „technisch für den sicheren elektronischen Übertragungsweg aufgestellt sein müssen“.
Zitat:

Seit Januar 2018 dürfen Sachverständige ihre Gutachten bei Gericht elektronisch einreichen. Zusätzlich verlangt § 173 Abs. 2 der Zivilprozessordnung, dass ab dem 1. Januar 2024 professionell am Prozess Beteiligte, einen sicheren elektronischen Übermittlungsweg für die Zustellung zu eröffnen haben. Auch öffentlich bestellte Sachverständige werden dadurch verpflichtet sein. Dies bedeutet, dass regelmäßig für Gericht tätige Sachverständige zum 1. Januar 2024 entsprechend technisch aufgestellt sein müssen.

Zitat Ende

Der Autor hat sich dann noch vor dem Jahreswechsel in das Abenteuer „Mein-Justizpostfach“ gestürzt. Die Einrichtung und die Nutzung ist an nicht unerhebliche Hürden gebunden. Gut, wenn man schon einmal einen elektronisch auslesbaren Personalausweis hat und sich dann ein passendes Lesegerät dafür besorgt. Dann durch die typisch deutsche umständliche Oberfläche mit allerlei Widersprüchen und Unzulänglichkeiten kämpfen, um dann prinzipiell elektronische Nachrichten auf gesichertem Weg an Gerichte und Rechtsanwälte schicken zu können. Leider nur in der Theorie. Und dass das Ganze eine Insellösung ist, die fern von einem Standardverfahren liegt, ist fast überflüssig zu erwähnen.

Empfangen könnte man Nachrichten auf diesem Weg auch, nur kann man sich leider vom Portal nicht per E-Mail o.ä. über den Eingang einer Nachricht benachrichtigen lassen. Daher muss man schon regelmäßig selbst nachschauen (incl. Authentifizierung über den umständlichen Weg mit App, Personalausweis und Lesegerät), ob es vielleicht eine neue Nachricht oder gar einen Gutachtenauftrag gibt. IT-Azubis würden so etwas als Abschlussprojekt in 35 oder 70 Stunden umsetzen.

Das (!) ist der Stand der Digitalisierung in Deutschland und eine Frechheit. Denn das zuständige Bundesjustizministerium bedauert nur lapidar, dass eine Benachrichtigung über eingehende Nachrichten „derzeit“ noch nicht möglich ist. An diesem Stand hat sich auch im August 2024 nichts geändert. Das Portal ist zudem vollkommen unbrauchbar, da eine Kommunikation zwischen Sachverständigen und Prozessanwälten (bisher) auch nicht möglich ist. Man findet die Kommunikationspartner nämlich nicht (oder wieder nur mit Expertenwissen und Tricks). Daher schreibt man sich schön weiterhin per Brief, per Fax (wenn es denn so etwas noch gibt) oder ersatzweise per unverschlüsselter E-Mail an.

Und damit kommen wir zum nächsten Punkt. Wenn dann anschließend Schriftsätze (ggf. auch wieder mit personenbezogenen Daten) per unverschlüsselter E-Mail z.B. von den Prozessanwälten an den Sachverständigen geschickt werden, wird die ganze Sache mit dem verschlüsselten Versenden ausgehebelt.

Und jetzt soll der Sachverständige datenschutzrechtlich für diese ganzen Vorgänge den Kopf hinhalten? Sicherlich nicht. Und überhaupt stellt sich die Frage, was für personenbezogene Daten der Gutachter bei einer sachverständigen Untersuchung denn erfassen und speichern soll. Handelt es sich z.B. um die Untersuchung eines streitgegenständlichen Computers, dann kommt beim Asservat eine erhebliche Menge teils hochbrisanter Daten in Frage (man denke an Fotos und private Korrespondenz). Dagegen ist die auf dem Stick überlassenen Akte datenschutzrechtlich ein Witz.

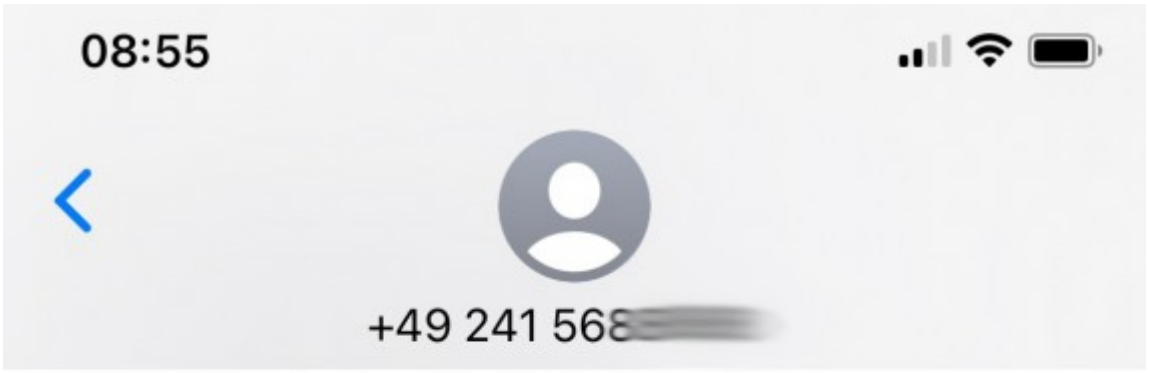
Zwischenfazit: Der verantwortungsvolle Umgang mit privaten (personenbezogenen) Daten, die im Rahmen von sachverständigen Untersuchungen gesammelt werden, ist dem Gutachter spätestens mit der öffentlichen Bestellung als ein über allem stehendes Credo mitgegeben. Ihm jetzt aber eine datenschutzrechtliche Verantwortung incl. einer zur ZPO widersprüchlichen Auskunftspflicht nach DS-GVO für die Verfahrensakte aufzuerlegen, ist mehr als überraschend.

Der Autor hat die IHK Aachen als bestellende Behörde um Stellungnahme und Unterstützung gebeten. Zuerst war man auf Seiten des Gerichts. Mit ein bisschen Nachbohren schwenkte die Stellungnahme schon etwas um und nach noch beharrlicherem Nachhaken wurde ein datenschutzrechtlicher Sprecher der IHK NRW eingeschaltet, der die Linie des Autors vollständig stützt. Auch er berichtet davon, dass Gerichte nach wie vor regelmäßig USB-Sticks durch die Gegend schicken, dass die datenschutzrechtlichen Vorgaben und Aussagen in dem Formschreiben unzutreffend sind und dass das elektronische Justizpostfach ein Scherz sei.

Das Gericht selbst hat übrigens auf die Beschwerde des Sachverständigen nicht reagiert. Eine weitere Nachfrage beim Direktor des Amtsgerichtes ergab – kurz zusammengefasst -„Eigentlich haben wir (außer bei diesem Einzelfall) nichts falsch gemacht und man gehe davon aus, dass das

Formblatt rechtlich geprüft sei, da es im gesamten OLG Bezirk verwendet würde.“ Ja dann. „Eigentlich“ ist ein Füllwort und wenn alle es so machen, muss es ja richtig sein.
Wenn wir jetzt wirklich Datenschutz und IT-Sicherheit ernst nehmen wollen, dann muss man als Sachverständiger die Annahme fremder USB-Sticks grundsätzlich ablehnen, denn wir predigen ja den zu schulenden Usern: „Finger weg von USB Sticks aus fremder Hand“. Und meistens unterbindet eine Security-Policy der Company ohnehin technisch, fremde USB-Sticks in den PC einzustecken. Das wird nun beim Autor auch bei Gerichts-Sticks so umgesetzt.
Dabei könnte es so einfach sein: Tatsächlich gibt es das elektronische Akteneinsichtsportal, zu dem man dem Sachverständigen fallweise und für die Zeit der Bearbeitung des Gutachtens einen gesicherten Zugriff geben könnte. Damit wären alle IT-Security- und Datenschutz-Fragen erledigt.
Aber wann können wir das elektronische Justizpostfach für den sicheren Austausch von Daten und Nachrichten bi-direktional nutzen? Wie viele Jahre soll das noch dauern? Das ist doch beileibe kein digitales Hexenwerk.
Und warum kümmern sich nicht Bundesjustizministerium, die IHK und die Gerichte darum, die Voraussetzungen für eine digitale Kommunikation und Aktenführung zeitnah und handwerklich sauber umzusetzen und bleiben am Ball? Warum muss da wieder ein einzelner Sachverständiger aktiv werden?
Schön wäre, wenn es zu Weihnachten 2024 ein Schreiben der IHK geben würde, dass nun alles geklärt wäre. Schön wäre auch, wenn dem Autor nicht immer wieder solche handwerklichen Fehler im Bereich Digitalisierung, IT-Sicherheit und Datenschutz begegnen würden. Leider ist auch dieser Bericht nur ein Beispiel in einer langen Reihe von Digital-Unfällen.
Und mal ganz persönlich: Jeder macht Fehler (auch der Autor). Das ist menschlich. Und wenn der Sachbearbeiterin der Fehler passiert ist, dass sie den Stick nicht verschlüsselt hat, dann ist das kein Beinbruch. Aber wenn Politik, Behörden und Institutionen immer weiter und immer mehr Vorgaben und Auflagen rund um IT-Sicherheit, Digitalisierung und Datenschutz machen, dann müssen sie selbst mit gutem Beispiel vorangehen und sich nicht ständig selbst vorführen lassen.

BMW und Digitalisierung – Teil 264
5. August 2024 von Thomas Käfer
Ich weiß nicht, ob ich nur noch lachen soll oder jetzt anfangen werde, bitterlich zu weinen. Warum immer ich? Oder ist es doch nur die Spitze des Eisbergs?
Die Stammleser meines Blogs kennen die Stories rund um digitalisierte und automatisiert fahrende Fahrzeuge aus meinem Testfuhrpark.
Heute Morgen erreichte mich überraschend eine SMS mit folgendem Text:



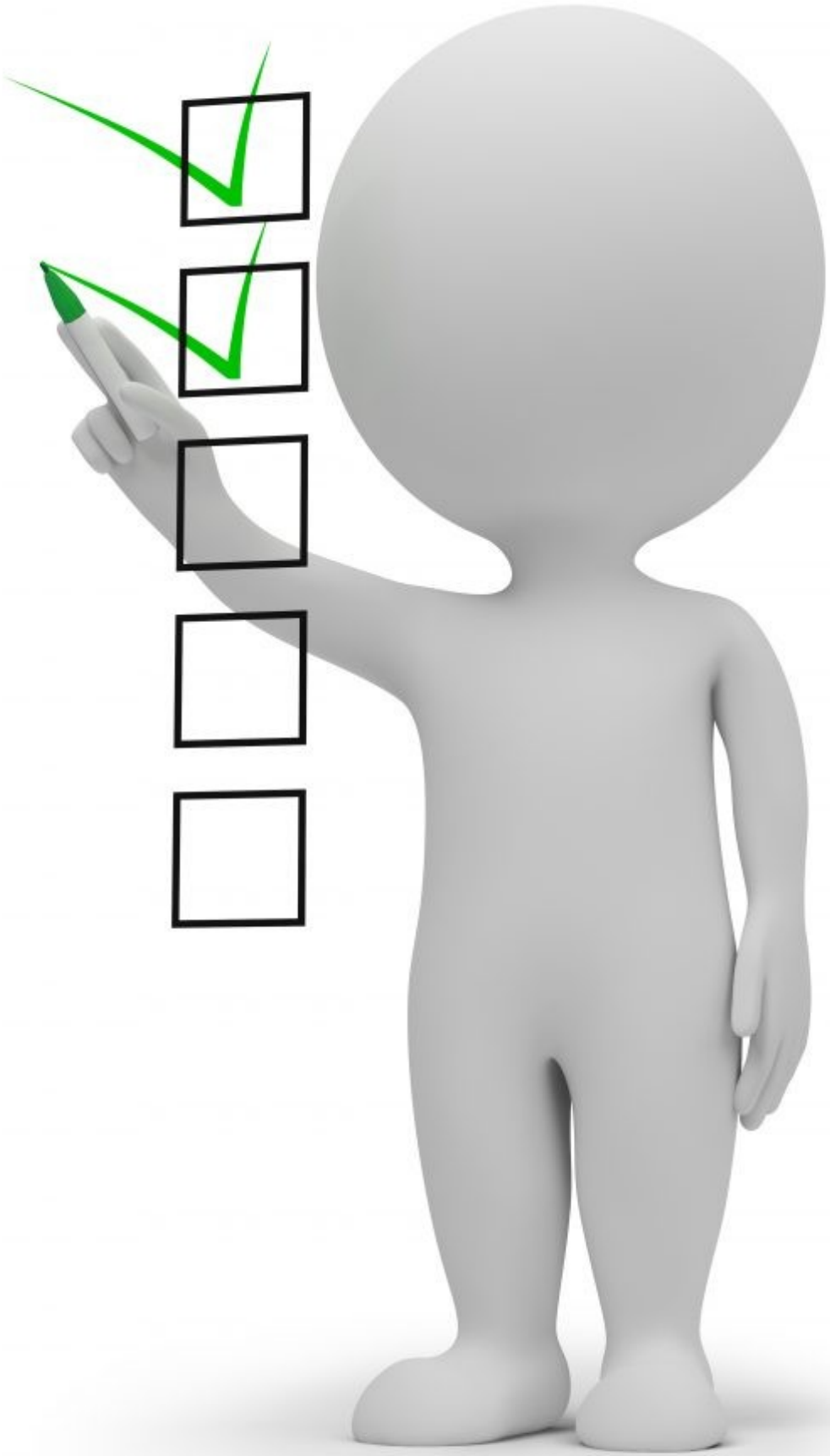
Heute, 08:35

Sehr geehrte Damen und Herren, vielen Dank für Ihre Terminbuchung. Bitte schicken Sie uns vorab Ihren Fahrzeugschein mit Telefonnummer an se[redacted]@kohl.de. Bitte antworten Sie nicht auf diese SMS. Ihr Service Team Kohl Bergheim Kohl automobile GmbH Aachen

Absender ist nicht in deiner Kontaktliste.

Spam melden

SMS-Nachricht



Zum Verständnis: Ich bekomme von meinem BMW Händler eine SMS an meine Mobilrufnummer, mit der Bitte, meine Telefonnummer mitzuteilen. Ja, so habe ich auch geschaut.
Und ich soll meinen Fahrzeugschein an diese Service-Adresse (per E-Mail – unverschlüsselt) schicken. Mein Fahrzeug wurde bei Kohl gekauft und angemeldet. Und es war natürlich auch schon dort zum Service. Sollte man daher nicht die Fahrzeugdaten dort vorliegen haben?
Oder liegt es daran, dass diese Daten an die Filiale nach Bergheim statt nach Eilendorf geschickt werden sollen? Das würde natürlich Sinn machen. Die kennen ja mein Auto noch gar nicht. Nur was soll ich mit meinem BMW in Bergheim?
Sind dort vielleicht die Digitalisierungsspezialisten ansässig, die jetzt das eigentliche Problem an meinem BMW (fehlende eSIM, defekte Tempolimiterkennung, defektes Remote-Update etc.) in Ordnung bringen sollen/können (siehe LINK)? Dafür fahre ich natürlich gerne 100 km weiter (wahrscheinlich 200 km, denn einen Drive-In haben die sicher nicht und ich darf nach ein paar Tagen mein Auto unrepariert wieder abholen).
Ich könnte ja einfach mal nachfragen, aber nein: Antworten soll man auf die SMS nicht (wie ich diese NoReply-SPAMMER hasse…)
Und jetzt die alles entscheidende Frage: Wann ist eigentlich mein Termin? Ich habe ja noch gar keinen vereinbart und warte eigentlich darauf, dass sich von Kohl nun jemand bei mir meldet und einen Termin mit mir abspricht.
Oder ist das nur einer dieser nervigen SPAM und Phishing-Attacken, die wir jeden Tag bekommen? Die ist dann tatsächlich gut gemacht, weil die Story und die Absendertelefonnummer stimmen könnten.
Aber nein, es ist SPAM und kann weg. Ich bin gehackt worden. HILFE!
Ist das ein typisches BMW-Problem? Nein. Die Erfahrungen aus meinem Testfuhrpark mit folgenden Marken (alphabetische Auflistung, Mehrfachnennungen möglich) und zugehörigen Autohäusern zeigen: Es ist kein Einzelfall und es muss an mir liegen.
Alfa Romeo
Audi
BMW
Hyundai
Opel
Von Beileidsbekundungen ist bitte abzusehen.
Aktualisierung: Ok, jetzt wird es lustig. Das System entwickelt ein Eigenleben. Ich schwöre, ich habe nichts gemacht.

Über Fälschungen von Corona-Test-Ergebnissen, Kunden-Desorientierung und digitalen Rohrkrepierer
27. Mai 2021 von Thomas Käfer

Ich weiß gerade nicht, ob ich lachen oder nur noch heulen soll.

Digitalisierung und Kundenorientierung sind in Deutschland offenbar weiterhin Neuland. In den letzten Tagen erlebe ich am eigenen Leib, wie desolat die tatsächliche Situation in diesen Bereich wirklich ist. Und nach dem Eisbergprinzip kann meine subjektive Momentaufnahme der letzten fünf Tage nur bedeuten, dass unter der Oberfläche noch mehr ist. Das muss sich ändern, wenn wir uns nicht vollkommen lächerlich machen oder wegen Herzinfarkt reihenweise vom Bürostuhl kippen wollen. Das oft dümmliche Gelaber von Politikern und Nichtwissenden zu diesem Thema ist da weder hilfreich noch fachlich untermauert. Ach so: Breitbandausbau ist nicht Digitalisierung (sondern nur die notwendige Voraussetzung) und iPads für Schüler sind es auch nicht, wenn es keine wirklich digitalen Lerninhalte und interaktive Lernmedien darin gibt. Aber zurück zu meinen konkreten und aktuellen Erfahrungen…

Kostprobe gefällig?

Fall 1:

Die Sparkasse Aachen stellt zum Juli das HBCI-Verfahren ein. Das erfolgt ohne große Not, denn andere Banken wie VR-Bank oder Aachener Bank kündigen das Verfahren nicht ab. Blöd, dass man deshalb einen neuen Kartenleser kaufen und sich erst einmal schlau machen muss, welches Ersatzverfahren denn adäquat wäre. Für die Umstellung von HBCI auf Chip/TAN-USB hat mir die Sparkasse dann heute über ihr „Secure-Mail"-Portal 7 (in Worten sieben) E-Mails mit 10 Anhängen und insgesamt rund 80 Seiten DIN-A4 Formulare und Vertragstext geschickt. Schon blöd, dass meine Frau und ich mehrere Konten mit unterschiedlichen „Firmierungen" dort betreiben. Die Benachrichtig über die Secure-Mail kommt dann via „noreply-Adresse" und es hat keine 10 Minuten gedauert, bis ich den richtigen meiner drei Secure-Mail-Zugänge identifiziert und das Passwort zurückgesetzt hatte. Dann ist das Tageslimit leider zum wiederholten Mal falsch und nach einem Dutzend Unterschriften scheitert der Versuch, die eingescannten (!) Dokumente (22 Seiten), die ich ja wegen Unterschrift ausdrucken musste, wieder über Secure-Mail hochzuladen an der dortigen Begrenzung von 5 MB. Puls 180. Aber ich habe dann einfach den ganzen Mist als normale Mail an meinen Bankberater geschickt, der mir einen Teil der obigen Mails neben dem Weg über Secure Mail auch über die normale unverschlüsselte Mail geschickt hat. Er ist aber nach eigenem Bekunden unschuldig. Er ist nicht Mister Sparkasse. Das merke ich mir mal, wenn sich einer meiner Kunden beschwert. Ich bin dann auch unschuldig. Jetzt bin ich mal gespannt, ob die tatsächliche Umstellung des Verfahrens wenigsten reibungslos klappt. Das wäre das erste Mal.

Fall 2:

Die IHK Aachen verschickt PDFs zur Online Abstimmung an uns Vollversammlungsmitglieder. Darin sollen wir „online" ankreuzen, ob wir bestimmte Beschlüsse unterstützen oder nicht. So weit so gut. Blöd, dass sich die PDF nicht bearbeiten lässt und so eine Abstimmung gar nicht möglich ist. Kein Problem. Einfach kurze Email zurück an „noreply…". Ach nee, kurz „richtige" E-Mail-Adresse raussuchen und Hinweis verschicken. Prompte Reaktion: „Danke für den Hinweis – haben wir sofort geändert". Gerne. Jetzt kann ich wenigstens die Klicks „online" machen und das Ergebnis direkt als PDF per Mail verschicken. Zum Glück ist das kein echtes Wahlverfahren, bei dem es auf etwas ankommen würde (Stichwort: Vertraulichkeit, Sicherheit, Zuordnungsfähigkeit zu einer bestimmten Person etc.).

Fall 3:

Die Städteregion Aachen verschickt offenbar grundsätzlich alle möglichen E-Mails mit einer „noreply"-Adresse, damit man bloß nicht direkt darauf antworten kann, wenn etwas nicht stimmt. Harmlos bei einer Online Terminanmeldung beim Straßenverkehrsamt. Richtig blöd, wenn eine (offenbar fehlerhafte) Terminstornierung für den zweiten Corona-Impftermin am Pfingstsonntag eintrudelt. Meine Frau hat sich dann die Mühe gemacht, „echte" Emailadressen herauszusuchen, nachdem ihre Beschwerde wegen der unverständlichen Terminstornierung an die „noreply"-Adresse des Impfzentrums als unzustellbar zurückkam. Das hat dann ausgelöst, dass sehr schnell die Terminstornierung storniert wurde (unerklärlicher Systemfehler) und ein neuer Termin bestätigt wurde (zunächst als „echte" Mail von Menschenhand und dann nochmal per Noreply-Mail). Gestern rief dann eine weitere Mitarbeiterin an und wollte das Thema nochmal klären. Zum Glück hatte sie den gleichen bestätigten zweiten Impftermin auch in ihrem System. Sie erklärte mir auch, dass die mehrfachen Nachfragen jetzt daran liegen, dass meine Frau ihre Beschwerde an mehrere Adressen geschickt hatte. Auf meinen Einwand, dass das daher kommen würde, wenn man u.a. die Stornomail mit einer „noreply" Adresse verschickt, meinte sie nur: „Dafür kann ich nichts. Das macht die Städteregion bzw. Regio-IT immer so". Genau das ist das Problem. Also auch „unschuldig".

Fall 4: Tja und dann habe ich bei meiner Versicherung (Gothaer) letztes Wochenende per Mail angefragt, wie denn die Konditionen für die Versicherung eines Zweitfahrzeugs wären. Darauf erreicht mich sehr schnell am nächsten Werktag ein Anruf – dummerweise gerade nur unterwegs mit keiner Möglichkeit zum Mitschreiben (ich brauche einen Chauffeur). Auf meine Bitte, die Konditionen

doch einfach kurz per E-Mail zu schicken, meinte die Dame nur: „Das geht leider nicht. Wir können das nur telefonisch oder per Post“. Ich habe dann nochmal entsetzt nachgefragt, ob das ihr Ernst sei, war dann aber zu perplex, um schlagfertig darum zu bitten, eine Eule oder eine Kutsche zu schicken. Wir einigten uns daher auf einen erneuten Anruf heute Vormittag. Den muss ich gerade verpasst haben, als ich die 10 Unterschriften für die Sparkasse nebenan von meiner Frau eingesammelt habe, denn gerade kamen zwei E-Mails der Gothaer-Versicherung. Überraschung: Die Gothaer kann doch E-Mail. In der 1. Mail steht:

Sehr geehrte Damen und Herren,
Sie haben eine neue Nachricht von Ihrer Gothaer erhalten.
Der Schutz Ihrer Daten ist uns sehr wichtig. Deshalb haben wir die Nachricht für Sie in einem sicheren elektronischen Postfach (Gothaer Webmailer) hinterlegt.
Sie können die Nachricht nach dem Login in den Gothaer Webmailer aufrufen und auch abspeichern.
Der Login zum Gothaer Webmailer ist erreichbar unter der Adresse: https://www.gothaer.de/app/webmailer/webmail_users/login…
Wenn Sie den Webmailer bislang noch nicht benutzt haben, erhalten Sie in einer weiteren E-Mail das Kennwort für den ersten Login.

In der zweiten Mail (direkt dahinter) kommt dann:

Wir haben Ihnen für die Erstanmeldung im Gothaer Webmailer ein Initialkennwort erstellt.
Den Link zum Gothaer Webmailer erhalten Sie in einer separaten E-Mail. Bitte prüfen Sie auch Ihren SPAM-Ordner auf Erhalt der Nachricht.
Das Initialkennwort für Ihren Gothaer Webmailer-Zugang lautet: …

Als Addendum dann noch ein Link zum BSI zur Vergabe sicherer Passwörter (das ist der Treppenwitz schlechthin).

Ich musste lachen. Nun, tatsächlich muss man nach dem ersten Login eine eigenes (sicheres) Passwort vergeben. Aber das Versenden eines Initialpasswortes in einer separaten Mail suggeriert eine Sicherheit, die es nicht gibt. Das ist fast so dumm, wie echte Passwörter in einer separaten Mail zu verschicken, um den Anhang in einem passwortverschlüsselten Anhang der vorherigen Mail „abzusichern“ (unter anderem vom Gesundheitsamt der Stadt Aachen so als Verfahren zur Übermittlung personenbezogener Daten mir gegenüber vorgeschlagen – aber das ist Fall 5).

Zurück zur Gothaer:
(Die Gothaer hat übrigens nicht angerufen. Sie hat es nur behauptet, aber das kommt gleich).
Nachdem ich nun also ein eigenes Passwort eingegeben hatte und die Gothaer somit immer noch nicht weiß, ob ich tatsächlich der Thomas Käfer bin, konnte ich die so wichtige Mail nun endlich lesen. Da war nicht etwa ein Angebot enthalten, sondern dass hier:

Und jetzt – die Spannung steigt: Was verbirgt sich hinter der HTML-Datei, die man eigentlich aus Sicherheitsründen eher nicht öffnen sollte?

Das hier: Leider konnten wir Sie telefonisch nicht erreichen. Gerne klären wir Ihr Anliegen in einem persönlichen Gespräch.

Nachdem ich mich wieder vom Boden aufgerappelt, den umgestürzten Stuhl aufgerichtet und meine Tränen getrocknet hatte, dachte ich mir: Jetzt reicht es …

Aber es reicht noch nicht (Übrgens habe ich die Sache dann mit ein „paar“ Telefonaten, darunter mit einer unfassbaren dummen Mitarbeiterin (diesmal bei Check24) regeln können – aber das ist kein digitales Thema).

Kommen wir zum Schluss noch zum Thema „Fälschen von Covid-Testergebnissen“ unserem heutigen Fall 6:

Den nachfolgenden Text habe ich am 14.05.2021 an die Kaiser-Apotheke Würselen, den Betreiber der Software-Lösung des dort verwendeten Covid-Tests (no-q.info) und den Sprecher des Gesundheitsamtes der Städteregion Herrn Ziemons mit der Bitte um Stellungnahme vor Veröffentlichung meiner Befunde geschickt.

Ich lasse mich seit einigen Wochen brav jede Woche im Testzentrum in der Kaiser-Apotheke in Würselen testen. Da ich mich hauptberuflich mit Datenschutz und IT-Sicherheit befasse, wurde meine Neugier geweckt, wie gut denn die Testbescheinigungen vor Manipulationen geschützt sind. Das neuerdings das Geburtsdatum als Passwort genutzt wird, ist nett, aber – wenn wir mal ehrlich sind – kein wirksamer Schutz. Am Anfang gab es nicht mal diesen trivialen Passwortschutz.

Schlimmer noch ist, dass die PDF nach Eingabe des Passwortes dann vollkommen ungeschützt ist und problemlos in gängigen Programmen wie Adobe Acrobat o.ä. komplett editiert und verfälscht werden kann.

Ich habe mal als Fingerübung mein letztes Testergebnis in 10 Minuten beliebig modifiziert und könnte mir damit nun täglich neue negative Testbescheinigungen auszustellen. Das Ergebnis dieser – hier bewusst plumpen – Urkundenfälschung habe ich Ihnen mal beigefügt. Wenn dann ein Kontrolleur (wie mutmaßlich praktisch jeder Laden- oder Restaurantbesitzer) so ein Blatt Papier vorgelegt bekommt (ohne die hier offensichtlichen plumpen Modifikationen), wird er in der Mehrzahl der Fälle den QR-Code gar nicht prüfen und die Urkunde als echt hinnehmen.

Aber auch das wäre kein wirkliches Problem , wenn dies Anbieter mit krimineller Energie als Dienstleistung im Netz anbieten würden. Denn den QR-Code könnte ich als Kür auf einer von mir als Hacker bereitgestellten Website, die an https://verify.no-q.info/ angelehnt ist (um nicht zu sagen kopiert) und die z.B. https://verify.noq.info heißen könnte, ebenfalls beliebig als valide bestätigen lassen. Dazu übergibt man im QR-Code einfach in der gewünschten URL den Namen und das Testdatum als get-parameter. Den Übergabeparamater kann man dann genauso kodieren wie die offensichtlich simpel mit Base64 codierten Übergabeparameter der originalen QR-Codes. Die Webseite braucht dann nur die wahlfrei übergebenen Parameter wieder zu dekodieren und genauso wie auf der Original-Website formatiert auszugeben. Wetten, dass kaum ein Kontrolleur diesen Betrug erkennt? Denn wer weiß schon, dass das Testergebnis auf verifiy.no-q.info (mit Bindestrich) verifiziert werden muss und nur das dann als valide Echtheitsprüfung gilt? Und dafür ist auch im Alltag keine Zeit!

Die Website https://verify.no-q.info/ enthält keinerlei Anbieterkennung oder Impressum und damit ist für den Prüfenden ohnehin nicht zu erkennen, ob das Ergebnis der QR-Code-Prüfung vertrauenswürdig bzw. echt ist.

Warum wird keine wirklich offizielle und eindeutig zuzuordnende Adresse (wie z.B. www.rki.de) benutzt? Und warum wird überhaupt ein so unsicheres Verfahren wie eine einfach zu fälschende oder selbst zu erstellende PDF als Testnachweis benutzt? Warum wird so etwas nicht mit der offiziellen Corona-App gekoppelt, sodass eine Manipulation nahezu ausgeschlossen werden kann? Die Corona-App gibt es nun seit über einem Jahr und der Nutzen ist mehr als fraglich. Das ärgert mich umso mehr, als dass wir im April 2020 mit der Cyber-Security Fokusgruppe des digihub Aachens auf Basis meiner Initiative ein Konzept für eine Corona-App vorgestellt haben, die wohl nur

einen Bruchteil der jetzigen Kosten verursacht hätte, aber dennoch hinsichtlich Datenschutz und IT-Sicherheit wohl deutlich besser gewesen wäre, als das, was wir jetzt vorfinden. Im Konzept wurden damals schon genau die jetzt hochkommenden Probleme thematisiert, aber das ist wieder ein anderes Thema. Nur kann man jetzt nicht sagen, „das war ja alles überraschend und wir mussten schnell eine Lösung haben“. Die Probleme und Herausforderungen sind seit Monaten, wenn nicht seit gar seit Anfang der Pandemie bekannt.

Dennoch müsste die Corona-App längst flächendeckend zum Verarbeiten und Nachweis von Testergebnissen eingesetzt werden können, aber das ist wohl immer noch Utopie. Denn auch die QR-Codes, die ich auf meinen Testergebnissen erhalte, werden nach wie vor von der aktuellen Corona-Warn-App nicht erkannt. Das ist umso unverständlicher, als das auf der Website von https://www.no-q.info/ genau mit der Kompatibilität zur Corona-Warn-App geworben wird. Warum funktioniert mein Test-Ergebnis damit nicht?

Und beim Blick auf die Nachlässigkeit, wie die Testergebnisse verwaltet und wenig fälschungssicher verteilt werden, brauchen wir nicht ernsthaft über fälschungssichere Impfnachweise nachzudenken.

In Anbetracht der massiven Einschränkungen mit der wir Bürger seit über einem Jahr konfrontiert werden, würde ich mir endlich mal mehr Professionalität beim Einsatz der IT-Werkzeuge zur Bekämpfung der Pandemie wünschen.

Und jetzt das Positive an dem negativen Test:

Sowohl die Kaiser-Apotheke als Betreiber des Testzentrums als auch der Software-Anbieter Vertical Life aus Südtirol haben sich sehr schnell und konstruktiv zurückgemeldet. So wurde umgehend ein Impressum auf die Verifikationsseite hinzugefügt (wenn auch nicht auf allen Seiten) und die PDF ist seither schreibgeschützt und kann nicht mehr auf einfachster Weise direkt manipuliert werden. Zudem verwies der Software-Hersteller darauf, dass das Formular den Vorgaben der Corona-Schutzverordnung des Landes NRW entspricht. Dort wird eine gewisse Formfreiheit bejaht und auch die Möglichkeit zum Bestätigen per Online-Formular erlaubt. Der Vordruck sieht jedoch trotzdem anders aus und beinhaltet vor allem einen Hinweis auf die Strafbarkeit der Fälschung einer solchen Bestätigung, die übrigens gerade vom Bundestag nochmals mit schärferen Strafen auch im Fall eines gefälschten Impfausweises unterstrichen wurde. Das ist gut und wichtig, damit jedem klar wird, dass das einfache Manipulieren kein Kavaliersdelikt ist. Dieser Hinweis fehlt leider nach wie vor auf dem Corona-Testergebnis von Vertical (wie vermutlich in vielen anderen selbst entworfenen Formularen). Vor Gericht wäre wahrscheinlich aber spannend, wie scharf das Gesetzesschwert dann wäre, wenn es dem Urkundenfälscher zu leicht gemacht wird…

Und Vertical-Life gab mir gleich noch eine Anleitung mit, wie denn das Testergebnis auch mit der Corona-Warn-App verknüpft werden kann: https://www.coronawarn.app/de/blog/2021-05-11-how-to-rapid-test-integration/

Das ist leider etwas schwerfällig beschrieben bzw. aus der Benutzerführung der Warn App nicht sofort klar ersichtlich. Man muss die Warn App dazu entweder autorisieren und das Testprofil dann vor dem Test beim Testzentrum vorzeigen oder die Mitarbeiter im Testzentrum müssen den Zugriff auf die Warn-App explizit freischalten, wenn man das bei der Testbuchung nicht bereits selber gemacht hat. Für mich als Informatiker war das offenbar schon zu kompliziert, denn es hat dann nur einmal geklappt, als der Mitarbeiter dies vor Ort explizit freigeschaltet hat. Mit der Testregistrierung aus der Corona-Warn-App konnte man dort nichts abfangen. Und tatsächlich haben wir in der Registrierungsmaske bei der Terminbuchung auch nichts gefunden. Da sollte man also noch nachbessern…

Fazit: Die Reaktion des Betreibers der Tests war vorbildlich und lösungsorientiert. Das habe ich auch schon anders erlebt. Die Städteregion Aachen hat sich zu dem Thema bisher nicht geäußert. Tja… vielleicht schicke ich ihr den Text hier nochmal an eine noreply-Adresse…

Die Lösung mit den Testergebnissen per PDF ist aber nach wie vor nicht optimal und krankt daran, dass es keine offizielle und einheitliche Form und Verifikationsmöglichkeit zur Echtheitsprüfung gibt. Denn letztlich kann ich mir so eine PDF ja auch komplett selber bauen. Das ist zwar strafbar, schützt aber nicht vor Missbrauch und von der Unsicherheit beim Test des Tests. Schließlich gestaltet ja auch nicht jeder von uns seine eigenen Banknoten und behauptet dann, die wären echt…

So, ich rufe jetzt mal bei der Gothaer an und versuche mein Glück erneut. Bin gespannt, auf welchem Weg ich die EVB Nummer bekomme…

Aber wenn gleich der nächste mit so einem Digitalisierungs-Rohrkrepierer um die Ecke kommt, platzt hier eine Bombe oder ich.

Durch Deutschland muss endlich ein Digitalisierungs-Ruck gehen.

Fazit
Und die Moral von der Geschichte? Upgrades kosten Zeit, Geld und manchmal Nerven. Sie nicht durchzuführen und zu verschleppen, kostet noch mehr Zeit, Geld und sicher Nerven.

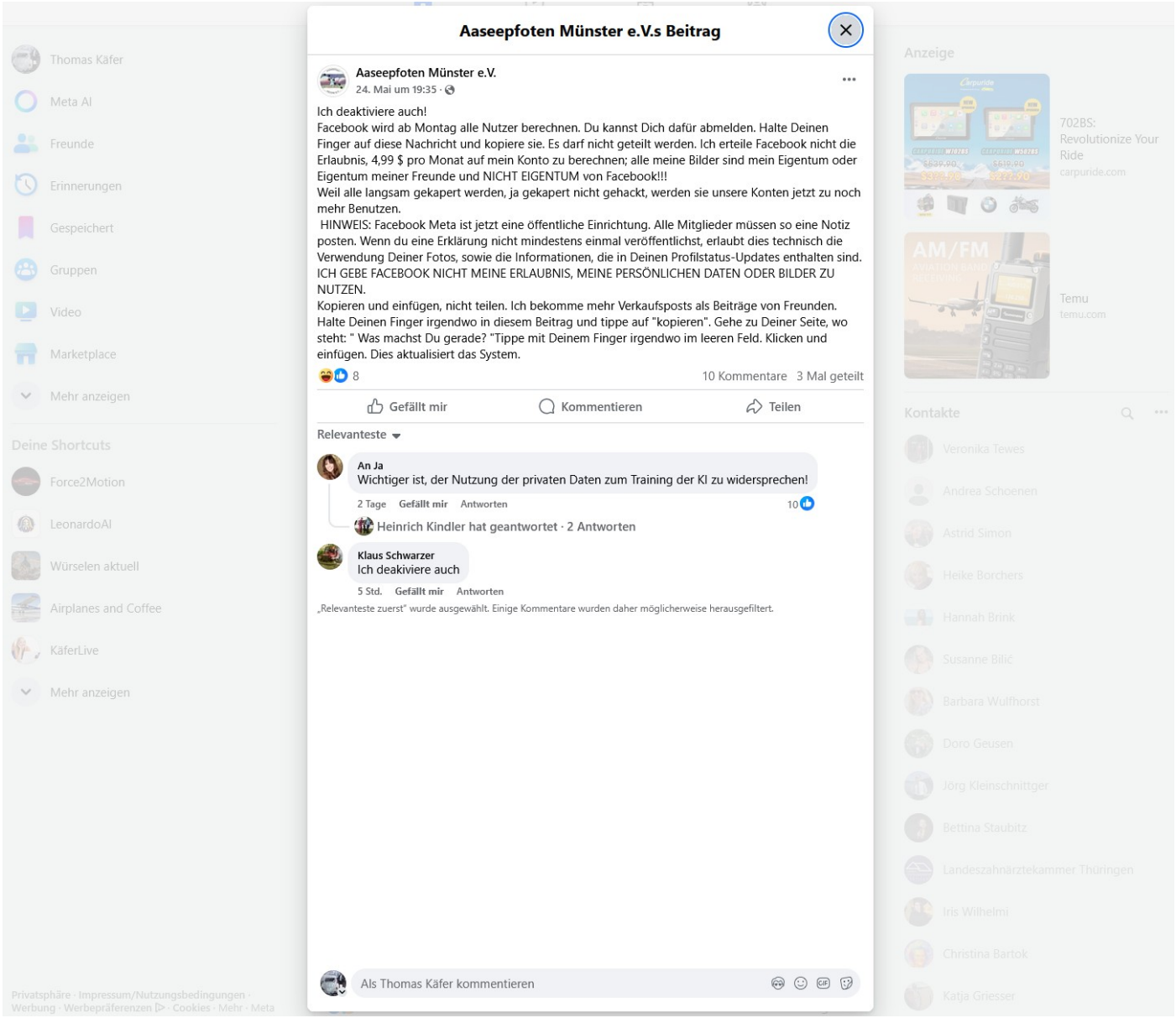
Jetzt haben Sie die Wahl: Lieber Updates machen oder sich hacken lassen?

Übrigens: Wenn Sie sich für die zweite Option entscheiden und in Kürze Opfer einer Cyber-Attacke geworden sind, rufen Sie gerne an. Mein Geld verdiene ich primär damit, Incident-Response und Forensik zu machen und weniger, kostenlose Warnungen wie diesen Aufsatz zu publizieren. Vielleicht war er aber ja tatsächlich nur kostenlos aber nicht umsonst.

Aber jetzt ernsthaft: Vielleicht kontaktieren Sie mich tatsächlich, bevor etwas schlimmes passiert, für eine Systemberatung. Das ist viel entspannter als mich nachher bei einem Incident Response dazuzuholen.

Facebook HOAX

https://www.mimikama.org/facebook-ki-widerspruch-per-status-reicht-nicht/



Ich deaktiviere auch!
Facebook wird ab Montag alle Nutzer berechnen. Du kannst Dich dafür abmelden. Halte Deinen Finger auf diese Nachricht und kopiere sie. Es darf nicht geteilt werden. Ich erteile Facebook nicht die Erlaubnis, 4,99 $ pro Monat auf mein Konto zu berechnen; alle meine Bilder sind mein Eigentum oder Eigentum meiner Freunde und NICHT EIGENTUM von Facebook!!!
Weil alle langsam gekapert werden, ja gekapert nicht gehackt, werden sie unsere Konten jetzt zu noch mehr Benutzen.
HINWEIS: Facebook Meta ist jetzt eine öffentliche Einrichtung. Alle Mitglieder müssen so eine Notiz posten. Wenn du eine Erklärung nicht mindestens einmal veröffentlichst, erlaubt dies technisch die Verwendung Deiner Fotos, sowie die Informationen, die in Deinen Profilstatus-Updates enthalten sind.
ICH GEBE FACEBOOK NICHT MEINE ERLAUBNIS, MEINE PERSÖNLICHEN DATEN ODER BILDER ZU NUTZEN.
Kopieren und einfügen, nicht teilen. Ich bekomme mehr Verkaufsposts als Beiträge von Freunden. Halte Deinen Finger irgendwo in diesem Beitrag und tippe auf "kopieren". Gehe zu Deiner Seite, wo steht: " Was machst Du gerade? "Tippe mit Deinem Finger irgendwo im leeren Feld. Klicken und einfügen. Dies aktualisiert das System.

Positiv Beispiel: Telekom esim Negativ BMW

Positiv Dreame Mova
Positiv: Benachrichtigung egp; negativ Nicht konsistente Nutzung