Mai 2026

ComConsult
BERATUNG • PLANUNG • SCHULUNG

Der Netzwerk Insider

Zutrittskontrolle

von Johannes Heinen
Die Zahl der Projekte im Bereich Gebäudesicherheit nimmt spürbar zu. Dabei spielen elektronische Zutrittskontrollsysteme eine zentrale Rolle. Sie regeln, wer wann welche Bereiche betreten darf und schaffen damit die Grundlage für ein sicheres und zugleich effizientes Gebäudemanagement. In diesem Beitrag gebe ich einen Überblick über die Grundlagen der Zutrittskontrolle, typische Einsatzszenarien, verfügbare Technologien sowie die planerischen Herausforderungen.

Seite 8

Mikroskopie am Glasfaserstecker – Theorie und Praxis

von Hartmut Kell
Über viele Jahrzehnte hinweg spielte die visuelle Prüfung von Glasfaseranschlüssen als Leistung des Installateurs oder Elements des Abnahmeprozederes keine oder nur eine sehr untergeordnete Rolle. Bei der Qualitätsprüfung einer installierten Glasfaserverkabelung stand neben der groben visuellen Kontrolle der handwerklichen Qualitäten vor allem die Messung der Strecken im Vordergrund.

Seite 16

Keine digitale Souveränität ohne Anpassung des Vergaberechts

von Dr. Behrooz Moayeri
Im Juni 2025 habe ich in einem Beitrag für den Netzwerk Insider behauptet, dass digitale Souveränität vor allem bedeutet, auf Open Source zu setzen. Im Folgemonat hat mein Kollege Dr. Ermes geschrieben, dass digitale Souveränität auch Hardware betrifft. Nun greife ich die sinnvolle Ergänzung von Dr. Ermes auf.

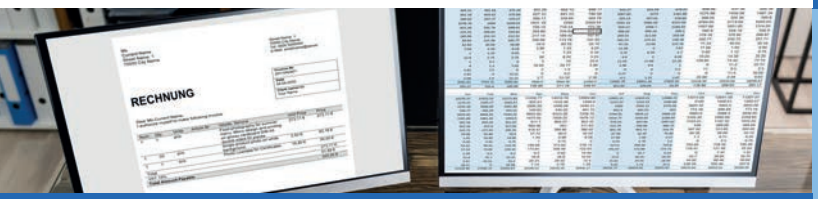
Seite 2

IT-Notfallvorbereitung für deutsche KMU

Warum digitale Resilienz kein Luxus, sondern betriebswirtschaftliche Pflicht ist

von Kevin Schneider
Die IT-Notfallvorbereitung hat direkte Auswirkungen auf die Betriebs- und damit Zukunftsfähigkeit eines jeden Unternehmens. Egal, ob kleiner Handwerker, produzierender Mittelständler oder globaler Dienstleister im B2B-Bereich.

Seite 28



Webinar der Woche

Lost in Transformation:

Warum E-Rechnung scheitert – und wie sie erfolgreich wird!

Seite 27

Ein lästiges Osterei: Zertifikatsaustausch durch D-Trust

von Dr. Markus Ermes
Viele Administratoren haben sich zu Ostern über ein tolles Geschenk freuen dürfen: D-Trust hat zahlreiche Zertifikate (wahrscheinlich mehrere Tausend) zurückrufen müssen. Die bishe-rigen Zertifikate behielten ihre Gültigkeit nur noch bis zum 6. April, also Ostermontag. Doch was genau ist passiert und welche Bedeutung hatte es?

Seite 33

Keine digitale Souveränität ohne Anpassung des Vergaberechts

von Dr. Behrooz Moayeri

Im Juni 2025 habe ich in einem Beitrag für den Netzwerk Insider behauptet, dass digitale Souveränität vor allem bedeutet, auf Open Source zu setzen. Im Folgemonat hat mein Kollege Dr. Ermes geschrieben, dass digitale Souveränität auch Hardware betrifft. Nun greife ich die sinnvolle Ergänzung von Dr. Ermes auf und versuche einen Weg aufzuzeigen, wie Deutschland und die EU digital souveräner werden können.

Der Staat ist gefordert

Die Mehrheit der Akteure in der hiesigen IT-Wirtschaft sieht ein, dass digitale Souveränität eine dringende Aufgabe ist. Diese Überzeugung sollte immer wieder artikuliert werden. Zum Beispiel finde ich es folgerichtig, dass ein Leser unserer Publikationen die Kritik an der von ComConsult genutzten Microsoft-Plattform für die Verbreitung unserer Inhalte vorgebracht hat. ComConsult nimmt diese Kritik auf. Wir hinterfragen bereits unsere gesamte IT-Ausstattung. Ich hoffe, dass wir bald zu Ergebnissen kommen, die ComConsult unabhängiger von nichteuropäischen kommerziellen Produkten machen.

Natürlich würde ich diesen Weg auch anderen Unternehmen empfehlen. Die Strategie kann man kurz zusammenfassen: Verlagerung der Hardware-Lieferketten nach Europa und Nutzung von Open-Source-Software. Die dritte IT-Säule, nämlich Dienstleistungen, ist zum Glück kein großes Problem. Europa und insbesondere Deutschland müssen sich im globalen Wettkampf um die besten Talente nicht verstecken. Es gibt Millionen, auch junger Menschen, die weiterhin hier leben und arbeiten wollen.

Damit jedoch der Aufruf zur Verlagerung der Lieferketten und zur Nutzung von Open Source keine hohle Sonntagsrede bleibt, ist der Staat gefordert. Kein privatwirtschaftliches Unternehmen priorisiert in seinen Entscheidungen volkswirtschaftliche Kriterien. Es muss sich lohnen, digitale Souveränität umzusetzen. Dazu kann der Staat die ihm zur Verfügung stehenden Instrumente nutzen.

Das Vergaberecht muss angepasst werden

Das wichtigste Instrument des Staates bei der Realisierung der digitalen Souveränität ist das Vergaberecht. Die Marktmacht der EU und der Bundesrepublik Deutschland darf nicht unterschätzt werden. Mit dieser Marktmacht kann der Staat der digitalen Souveränität dermaßen Vorschub leisten, wie kein Unternehmen es könnte. Der Staat ist der größte Auftraggeber. Er vergibt seine Aufträge gemäß dem Vergaberecht, das in der EU weitgehend der europäischen Zuständigkeit unterliegt.

Dieses Vergaberecht bindet momentan den öffentlichen Auftrag-

Zutrittskontrolle

von Johannes Heinen

Die Zahl der Projekte im Bereich Gebäudesicherheit nimmt spürbar zu. Dabei spielen elektronische Zutrittskontrollsysteme eine zentrale Rolle. Sie regeln, wer wann welche Bereiche betreten darf und schaffen damit die Grundlage für ein sicheres und zugleich effizientes Gebäudemanagement. In diesem Beitrag gebe ich einen Überblick über die Grundlagen der Zutrittskontrolle, typische Einsatzszenarien, verfügbare Technologien sowie die planerischen Herausforderungen und zeige anhand eines Beispiels, wie der Zugang durch eine gesicherte Tür in der Praxis funktioniert.

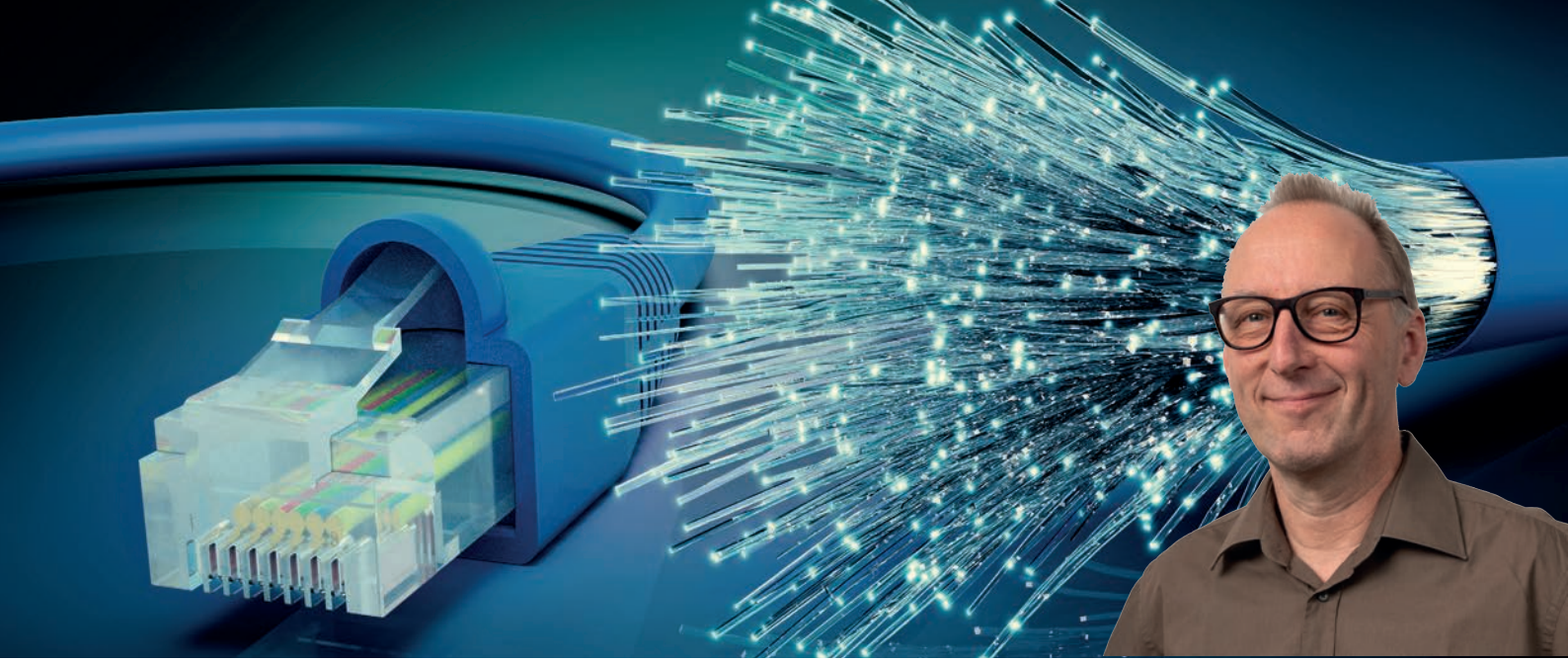
Was ist Zutrittskontrolle?

Zutrittskontrolle (ZuKo) bezeichnet Systeme und Maßnahmen, die den Zugang zu bestimmten Bereichen kontrollieren und nur berechtigten Personen den Zutritt erlauben. Moderne Zutrittskontrollsysteme sorgen elektronisch dafür, dass sich Türen nur für autorisierte Personen öffnen und halten Unbefugte zuverlässig fern. Um Personen, Sachwerte und sensible Daten zu schützen, geht es im Kern dabei immer um die Frage: Wer darf wann wohin? ZuKo kann sich sowohl auf physische Orte (Gebäude, Räume, Gelände) als auch auf digitale Ressourcen (z.B. Computernetzwerke) beziehen. In diesem Artikel wird ausschließlich auf die physische ZuKo eingegangen. Traditionell wurde der Zugang oft durch Pförtner oder Sicherheitspersonal überwacht, doch heute kommen überwiegend elektronische ZuKo-Systeme zum Einsatz, die diese Aufgabe effizienter, sicherer und nachvollziehbarer erfüllen.

Ein ZuKo-System prüft automatisch die Berechtigung einer Person, einen bestimmten Bereich zu betreten. Die Regeln dafür werden vom Betreiber festgelegt – typischerweise anhand von Kriterien wie Person, Ort und Zeit. So kann beispielsweise festgelegt sein, dass nur bestimmte Mitarbeiter (wer) während der Arbeitszeiten (wann) Zugang zu bestimmen Räumen (wohin) erhalten. Die Berechtigungen lassen sich flexibel einstellen, etwa zeitlich begrenzt (üblich ist die Gültigkeit einer Zutrittskarte bis zu einem Datum oder nur zu bestimmten Uhrzeiten, z.B. den Hauptgeschäftszeiten). Wird eine Person am Zugangspunkt erkannt, vergleicht das System ihre Identität mit diesen hinterlegten Regeln und entscheidet in Sekundenbruchteilen, ob der Zutritt gewährt oder verweigert wird. Dabei entstehen automatisch Protokolle über Zutrittsversuche, was für Nachvollziehbarkeit und ggf. Audits wichtig ist. Insgesamt bildet eine ZuKo oft das Rückgrat der Sicherheitsinfrastruktur eines Unternehmens oder einer Einrichtung, indem sie sicherstellt, dass nur autorisierte Personen bestimmte Räumlichkeiten betreten können.

Wird zusätzlich eine Einbruchmeldeanlage (EMA) eingesetzt, arbeitet diese eng mit der ZuKo zusammen. Dieses Zusammenspiel wird als Zwangsläufigkeit bezeichnet. Dabei sollte gelten: Ist ein durch die EMA gesicherter Bereich scharfgeschaltet, muss dieser zunächst unscharf geschaltet werden, bevor die ZuKo Zutrittsanfragen verarbeitet und einen Zutritt freigeben kann.

Abbildung 1: ZuKo - Schema (KI-generiert mit händischer Anpassung)



Mikroskopie am Glasfaserstecker – Theorie und Praxis

von Hartmut Kell

Über viele Jahrzehnte hinweg spielte die visuelle Prüfung von Glasfaseranschlüssen als Leistung des Installateurs oder Elements des Abnahmeprozederes keine oder nur eine sehr untergeordnete Rolle. Bei der Qualitätsprüfung einer installierten Glasfaserverkabelung stand neben der groben visuellen Kontrolle der handwerklichen Qualitäten vor allem die Messung der Strecken im Vordergrund. Fielen diese Messungen positiv aus, galt in der Regel als gesichert, dass die Strecken auch langfristig zuverlässig funktionieren. Zwar war bekannt, dass die Sauberkeit und Unversehrtheit der Glasfaseranschlüsse, insbesondere der Ferrulen, für die nachhaltige Nutzung der Anschlüsse wichtig sind, doch sollte diese Funktionalität durch die Messung automatisch mit abgedeckt und abgesichert werden. In den letzten 5-10 Jahren jedoch haben sich einige Standards diesem Thema zunehmend gewidmet – teils nur in empfehlender, teils auch in verbindlicher Form. Dies hat dazu geführt, dass man sich im Rahmen der Fachplanung und insbesondere bei der Erstellung von Leistungsverzeichnissen und Pflichtenheften mit der Frage auseinandersetzen muss, ob eine Mikroskopie als Prüfelement fest vorgeschrieben werden soll oder nicht. Auch in der Betriebsphase ist zu entscheiden, ob eine dauerhafte Mikroskopie der in den Rangierfeldern eingebauten Ferrulen oder der beigestellten Patchkabel ein fester Bestandteil des Betriebsprozesses sein soll, was letztlich auch die Anschaffung eines Mikroskops beeinflusst. Im nachfolgenden Artikel werden die Methoden beschrieben, die Empfehlungen der wichtigsten Standards wiedergegeben, Praxisbeispiele aufgeführt und Ansätze für den Umgang mit dieser Prüfart vorgestellt.

Sinn und Zweck

Eine optische Verbindung zweier über eine Kupplung oder ein Mittelstück verbundener Glasfaserstecker besteht darin, dass die Steckerstirnflächen einen sehr präzisen Glas-zu-Glas-Übergang ohne Luftspalt bilden (daher der Begriff „PC“ = physical contact). Der mit Abstand größte Teil der sich berührenden Fläche ist der Körper der Ferrule (z.B. Keramik). Bei einem SC-Stecker beträgt der Ferrulendurchmesser 2,5 mm und bei einem LC-Stecker 1,25 mm. Im Vergleich dazu ist der Manteldurchmesser der Glasfaser 125 µm und der Kerndurchmesser 9 µm oder 50 µm, also deutlich kleiner und besitzt damit eine wesentlich kleinere Fläche. Die gesamte Steckerstirnfläche kann beschädigt oder verschmutzt sein. Diese Beeinträchtigungen außerhalb des Kernbereiches wirken sich nicht auf die Glasfaserverbindung aus – zumindest geht man davon aus. Doch leider trifft das nicht in jedem Fall zu. Kratzer auf der Ferrule außerhalb des Glasfasermantelbereichs sollten sich tatsächlich nicht auf die Übertragung auswirken, aber bei Schmutz ist das anders. Schmutz in Form von Staub oder Schmiere kann sich z.B. bei Wechsel des Anschlusses von einer Verbindung auf die nächste übertragen (= kontaminieren) und damit das Risiko erhöhen, dass Verunreinigungen in den kritischen Bereich gelangen. Eine stärkere Verschmutzung oder eine dicke Schmutzschicht kann zudem verhindern, dass die beiden Ferrulen einen Kontakt ohne Luftübergang haben und somit äußerst schlecht für die Verbindung bzw. Übertragung sind.

Damit stellen sich die ersten grundlegenden Fragen: Hat das tatsächlich Auswirkungen und wenn ja, welche? Und rechtfertigt dieser mögliche Einfluss überhaupt den zusätzlichen Prüfaufwand (darauf wird später noch näher eingegangen)?

In jedem Fall erscheint es plausibel, dass eine direkte Beeinträchtigung des Kernbereiches zu einer Verschlechterung der Übertragungseigenschaften führt. Bei der Suche nach praktischen Erfah-

LPWAN-Technologien für das Smart Building: Evaluierung, Implementierung und Praxistest

Mit Leon Scheidgen sprach Christiane Zweipfennig

Low Power Wide Area Networks (LPWAN) gewinnen im Kontext von Smart Buildings zunehmend an Bedeutung. Sie ermöglichen die energieeffiziente Vernetzung von Sensoren über große Distanzen und bilden damit eine zentrale Grundlage für moderne Gebäudeanwendungen. Die verfügbaren LPWAN-Technologien unterscheiden sich jedoch deutlich in ihren Eigenschaften und eignen sich jeweils für unterschiedliche Anwendungsfälle und Anforderungen. Ob es um Reichweite, Energieverbrauch, Datenrate oder Infrastruktur geht – jede Technologie bringt spezifische Stärken und Einschränkungen mit sich. Vor diesem Hintergrund ist es entscheidend, die eigenen Anforderungen sorgfältig zu analysieren und die passende Technologie gezielt auszuwählen.

Leon Scheidgen absolvierte zunächst eine Ausbildung zum Fachinformatiker der Fachrichtung Systemintegration an der Zentralen Hochschulverwaltung der RWTH Aachen. Nach erfolgreichem Abschluss entschied er sich, seine Kenntnisse weiter zu vertiefen und begann ein Informatikstudium an der Fachhochschule Aachen. Gegen Ende des Studiums suchte er ein Thema für seine Bachelorarbeit und bewarb sich bei ComConsult. Dort erhielt er als Werkstudent die Möglichkeit, seine Bachelorarbeit im Bereich Funktechnologien mit dem Schwerpunkt LPWAN zu schreiben.

Was war die Motivation für deine Bachelorarbeit?

Im Rahmen meiner Bachelorarbeit habe ich mich intensiv mit LPWAN-Technologien im Kontext von Smart Buildings beschäftigt. Besonders motiviert hat mich dabei der Ansatz, energieeffiziente Gebäude durch den Einsatz stromsparender Sensorik zu ermöglichen.

> Energieeffiziente Gebäude durch LPWAN und stromsparende Sensorvernetzung

LPWAN bietet die technische Grundlage, um Sensoren über große Distanzen hinweg mit minimalem Energieverbrauch zu vernetzen. Die Fragestellung, wie sich ein Smart Building effizient überwachen und steuern lässt, insbesondere unter Berücksichtigung eines geringen Stromverbrauchs und drahtloser Kommunikation, fand ich dabei besonders spannend.

Wozu werden Sensoren im Smart Building genutzt?

Sensoren in Smart Buildings werden in zahlreichen Anwendungsbereichen eingesetzt und von vielen unterschiedlichen Anbietern bereitgestellt. Das Spektrum reicht von der Parkplatzüberwachung über die Erfassung von Luftfeuchtigkeit und Temperatur bis hin zur Anwesenheitserkennung in Büroräumen. Entsprechend vielfältig sind die Einsatzmöglichkeiten dieser Sensoren. Durch die Erfassung und Auswertung der Daten entsteht ein umfassen-

IT-Notfallvorbereitung für deutsche KMU

Warum digitale Resilienz kein Luxus, sondern betriebswirtschaftliche Pflicht ist

von Kevin Schneider

Die IT-Notfallvorbereitung hat direkte Auswirkungen auf die Betriebs- und damit Zukunftsfähigkeit eines jeden Unternehmens. Egal, ob kleiner Handwerker, produzierender Mittelständler oder globaler Dienstleister im B2B-Bereich.

Und dennoch wird sie oft wie das schwarze Schaf der Unternehmensbereiche behandelt: Budgets werden so knapp wie möglich gehalten, menschliche Ressourcen gibt es kaum, und niemand möchte sich wirklich damit auseinandersetzen.

Die IT muss einfach funktionieren – bis sie es irgendwann nicht mehr tut.

Die Konsequenzen reichen von nicht planbaren Verzögerungen in der Lieferkette über mittelfristige wirtschaftliche Einschnitte bis hin zu gescheiterten Existenzen. Betriebe geraten in die Insolvenz, Mitarbeiter in einen unfreiwilligen dauerhaften „Urlaub“. Dieser Missstand hat inzwischen auch die europäischen Behörden auf den Plan gerufen, sodass aktuelle regulatorische Anforderungen wie die europäische NIS-2-Richtlinie initiiert wurden. Diese macht deutlich: IT-Notfallvorsorge ist kein Nice-to-have für IT-Nerds, sondern unternehmerische Pflicht für alle Betriebe mit mehr als einer Handvoll Mitarbeitern.

Doch was bedeutet das konkret für deutsche Unternehmen? Und wie kann man wirklich sicherstellen, dass man für den Ernstfall vorbereitet ist, bevor dieser eintritt?

In diesem Beitrag führen wir Sie durch den kompletten Prozess der strukturierten IT-Notfallvorbereitung: Von der Risikoanalyse über die Notfallplanung bis zur operativen Umsetzung.

Warum IT-Notfallvorbereitung relevant ist

IT-Ausfälle wirken sich oft viel stärker aus, als man auf den ersten Blick vermutet. Und der häufig zitierte Umstand, dass „die letzten Jahre ja auch nichts passiert ist“ schützt leider nicht vor künftigen Katastrophen – das beweisen alle aktuellen Studien darüber, wie hoch die Risiko-Lage in deutschen Unternehmen tatsächlich ist. Dabei führt bereits ein kurzer Ausfall von E-Mail, ERP-System oder Projektplattformen nicht selten zu:

- verzögerten Lieferungen,
- unterbrochenen Produktionsabläufen,
- verpassten Rechnungsstellungen,
- Reputationsschäden bei Kunden und Geschäftspartnern sowie
- behördlichen oder vertraglichen Sanktionen.

Diese Risiken sind unabhängig von der Unternehmensgröße real:

Ein Dienstleister mit fünf Mitarbeitenden kann genauso betroffen sein wie ein mittelständischer Serienfertiger mit 200 Angestellten – je nachdem, welche Prozesse digital unterstützt sind.

Ein lästiges Osterei: Zertifikatsaustausch durch D-Trust

von Dr. Markus Ermes

Viele Administratoren haben sich zu Ostern über ein tolles Geschenk freuen dürfen: D-Trust hat zahlreiche Zertifikate (wahrscheinlich mehrere Tausend) zurückrufen müssen. Die bisherigen Zertifikate behielten ihre Gültigkeit nur noch bis zum 6. April, also Ostermontag. Doch was genau ist passiert und welche Bedeutung hatte es?

Die Ursache – ein grober Überblick

Der Rückruf hatte glücklicherweise rein technische Gründe und stand in keinem Zusammenhang mit einem Cyberangriff oder einer sonstigen Kompromittierung. Vielmehr lag die Ursache in einem Fehler bei der Überprüfung der Zertifikate vor deren Ausstellung. Denn an Zertifikate werden durch das CA/Browser Forum strenge Anforderungen gestellt.

Das CA/Browser Forum umfasst – der Name lässt es schon vermuten – auch die großen Browserhersteller. Werden die Vorgaben nicht eingehalten, kann der jeweiligen Zertifizierungsstelle, in diesem Fall D-Trust, schnell das Vertrauen entzogen werden. In der Folge stufen gängige Browser sämtliche Webseiten, die Zertifikate von dieser Stelle nutzen, als unsicher ein.

Und genau in diesen Anforderungen liegt sowohl der Grund für den Rückruf der Zertifikate als auch das unschöne Timing, welches das Osterwochenende für einige Administratoren deutlich verkürzt haben dürfte.

Die Ursache – Details

Was ist nun genau schiefgelaufen? Eine Zertifizierungsstelle überprüft normalerweise jedes auszustellende Zertifikat vor der Ausstellung auf alle relevanten Vorgaben. Um diesen Prozess zu vereinfachen, gibt es gängige Tools, doch einige Zertifizierungsstellen setzen auch auf eigene Lösungen. Und genau das war bei D-Trust der Fall. Das interne Prüftool hat ein Detail nicht korrekt überprüft: Laut CA/Browser Forum dürfen Zertifikate nur eine maximale Gültigkeitsdauer von 200 Tagen haben. Da aber Zertifikate mit einer längeren Gültigkeitsdauer ausgestellt wurden, mussten diese zurückgerufen werden.

Ich bin mir ziemlich sicher, dass D-Trust den Prüfprozess genauer analysieren und um weitere Werkzeuge ergänzen wird – quasi ein automatisiertes 4-Augen-Prinzip für die Zertifikatsprüfung.

Das schlechte Timing

Jetzt, wo die Ursachen erläutert sind, stellt sich natürlich die Frage: Hätte man die Gültigkeit nicht einfach bis Dienstag (7. April) verlängern können, um allen Beteiligten ein ruhigeres Osterwochenende zu ermöglichen?

Die Antwort ist ein ganz klares „Nein“. Denn auch hier greifen die Vorgaben des CA/Browser Forum: Diese verpflichteten D-