März 2025

ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

Aktualisierte RZ-Standort-kriterien vom BSI

von Dr. Philipp Rüßmann
Rechenzentren (RZ) bilden das Rückgrat der digitalen Welt. Die Wahl eines geeigneten Standorts für RZ ist eine der wichtigs-ten Entscheidungen zur IT-Infrastruktur. Seit 2018 gibt das Bun-desamt für Sicherheit in der Informationstechnik (BSI) die RZ-Standortkriterien [1] heraus, die RZ-Betreibern Leitlinien bei der Auswahl eines geeigneten Standortes an die Hand geben. Im De-zember 2024 erschien eine Neuauflage, die wir hier unter die Lupe nehmen.

Seite 8

Der DeepSeek-Schock und die Folgen

von Dr. Behrooz Moayeri
Im Januar 2025 wurde das Open-Source-Modell DeepSeek-R1 veröffentlicht. Unabhängige Experten für Künstliche Intelligenz (KI) urteilen so, dass DeepSeek-R1 allen bisherigen KI-Systemen wie ChatGPT von OpenAI und Gemini von Google überlegen ist. An den US-amerikanischen Börsen löste DeepSeek-R1 eine Schock-welle aus.

Seite 2

Zwischen Vergangenheit und Gegenwart: Wie Apple die Ge-rätesicherheit stetig erhöht

von Mark Zimmermann
In den Anfangszeiten des iPhones konnten Nutzer durch soge-nannte Jailbreaks tief ins Betriebssystem eindringen. Öffentlich bekannte Schwachstellen ermöglichten es, Sys-tembeschrän-kungen zu umgehen, alternative Software zu installieren oder Systempro-zesse zu manipulieren.

Seite 14

Webinar der Woche

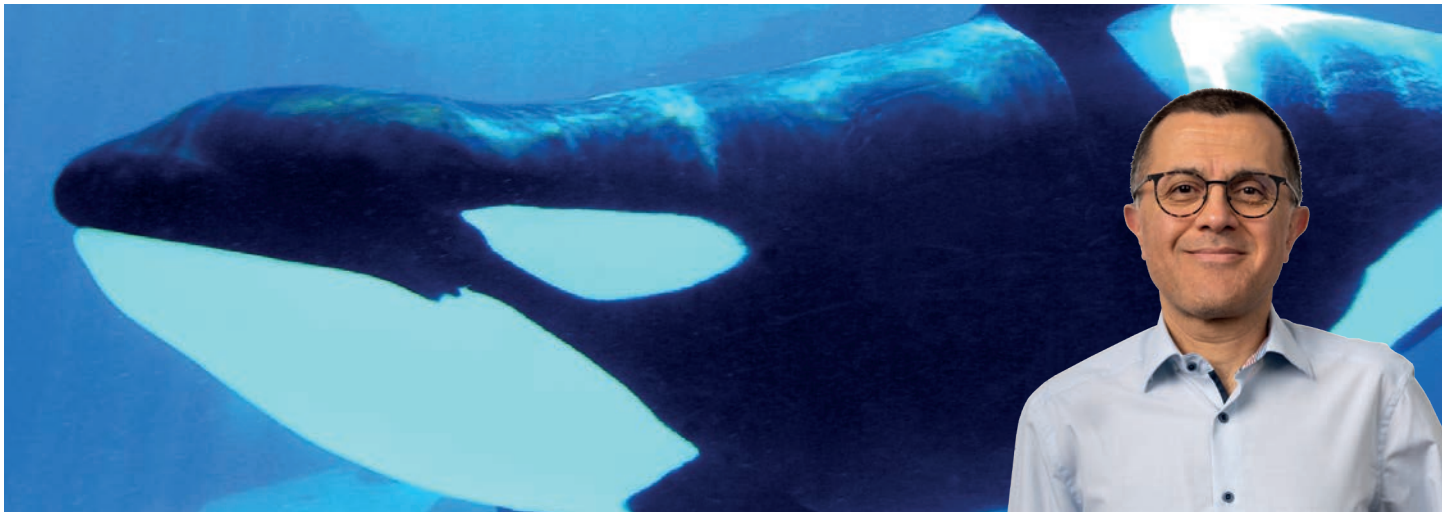
Design Patterns in Python

Seite 22

Und das nächste Datenleck: Business as usual?

von Dr. Markus Ermes
Und wieder gibt es ein neues Datenleck. Welches diesmal? Diese Frage allein zeigt schon das Problem: Datenlecks kom-men mittlerweile so oft vor, dass man kaum noch mitbekommt, welche Firmen es schon „erwischt hat“.

Seite 23



Der DeepSeek-Schock und die Folgen

von Dr. Behrooz Moayeri

Im Januar 2025 wurde das Open-Source-Modell DeepSeek-R1 veröffentlicht. Unabhängige Experten für Künstliche Intelligenz (KI) urteilen so, dass DeepSeek-R1 allen bisherigen KI-Systemen wie ChatGPT von OpenAI und Gemini von Google überlegen ist. An den US-amerikanischen Börsen löste DeepSeek-R1 eine Schockwelle aus.

Wer sind die Verlierer?

Am 27.01.2025 machte sich der DeepSeek-R1-Schock wie folgt bemerkbar:

- Der Technologie-Index Nasdaq 100 verlor im vorbörslichen Handel über vier Prozent.
- Zahlreiche Tech-Aktien verloren im vorbörslichen Handel teilweise über zehn Prozent.
- Die Aktien von Siemens Energy, Lieferant von Hardware für KI-Infrastrukturen, brach um mehr als 20 Prozent ein.
- Die Aktie von Nvidia, dem Hersteller von GPU-Chips, die in KI-RZs massiv eingesetzt werden, ging um 14 Prozent zurück.
- ASML, Hersteller von Maschinen für Chip-Hersteller, verlor 10 Prozent des eigenen Marktwertes.
- Microsoft verlor 6 Prozent.
- Arista Networks, dessen Netzkomponenten vor allem in Rechenzentren zum Einsatz kommen, gab um 9,5 Prozent nach.
- Aktien von Pure Storage, Hersteller von Speichersystemen für Rechenzentren, sanken um 9,5 Prozent.

Die obige Liste ist nicht annähernd vollständig.

Worin ist der Schock begründet?

Vor der Veröffentlichung von DeepSeek-R1 gingen sogenannte Analysten davon aus, dass das KI-Rennen schon gelaufen sei. Es galt als ausgemacht, dass die großen US-amerikanischen Firmen, die im KI-Bereich aktiv sind, eine Art Oligopol bilden werden, die auf Jahre den KI-Markt beherrschen würde, ein Oligopol vor allem aus folgenden Unternehmen:

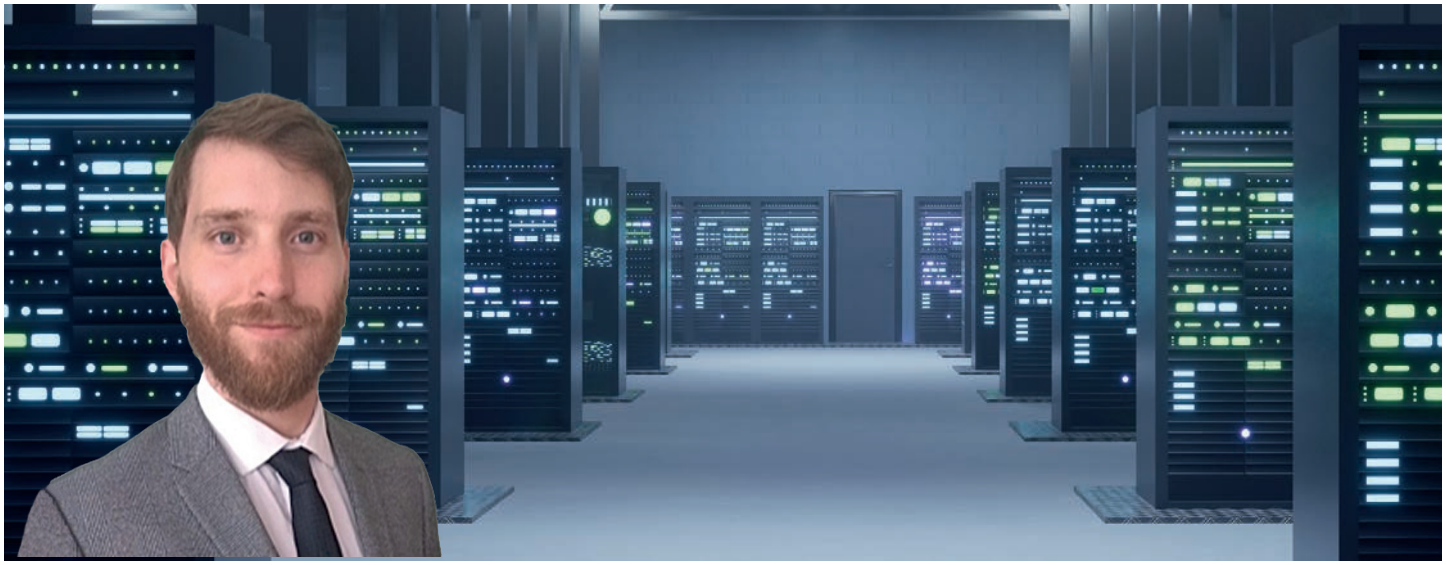
- Open AI (bekannt durch ChatGPT) und mit ihr Microsoft als Hauptaktionär von Open AI
- Nvidia mit ihren Chips für KI
- Alphabet, der Mutterkonzern von Google

Gleich in der ersten Woche seiner zweiten Amtszeit erschien der US-Präsident Donald Trump zusammen mit den Chefs von Open AI, Oracle und dem japanischen Unternehmen SoftBank vor der Presse und kündigte eine Investition der drei Firmen in Höhe von 500 Milliarden an, vor allem in den Bau von großen KI-Rechenzentren. (Sehr zum Missfallen Trumps stänkerte sein eigener Mitarbeiter Elon Musk, der mit X.AI eine eigene KI-Firma besitzt, das mit Trump aufgetretene Dreigespann habe gar nicht das nötige Kleingeld in Höhe von einer halben Billion US-Dollar.)

Nunmehr muss man davon ausgehen, dass viele KI-Aktivitäten rund um die Welt nicht auf KI-Berechnungen in den großen US-Rechenzentren angewiesen sein werden. Daher der Schock.

Open Source ist die Zukunft von KI

Open Source wird seit Jahrzehnten belächelt. In Deutschland wird Open Source fälschlicherweise immer nur mit missglückten Versuchen assoziiert, Alternativen zu Microsoft-Produkten, vor allem Windows und Office, zu nutzen. Man vergisst dabei, dass Open Source die Grundlage von vielem ist, was wir in der IT nutzen:



Aktualisierte RZ-Standortkriterien vom BSI

von Dr. Philipp Rüßmann

Rechenzentren (RZ) bilden das Rückgrat der digitalen Welt. Die Wahl eines geeigneten Standorts für RZ ist eine der wichtigsten Entscheidungen zur IT-Infrastruktur. Seit 2018 gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) die RZ-Standortkriterien [1] heraus, die RZ-Betreibern Leitlinien bei der Auswahl eines geeigneten Standortes an die Hand geben. Im Dezember 2024 erschien eine Neuauflage, die wir hier unter die Lupe nehmen.

Die RZ-Standortkriterien in Kürze

Die RZ-Standortkriterien beleuchten unterschiedliche Gefahrenquellen, die bei der Standort-wahl für RZ berücksichtigt werden müssen. Daraus abgeleitet ergeben sich Anforderungen wie Mindestabstände oder bauliche Vorgaben, die von RZ-Betreibern beachten werden sollten. Dies ist insbesondere für hoch- und höchstverfügbare RZ von Bedeutung, die eine Verfügbarkeit von 99,99% oder gar 99,999% sicherstellen müssen, was einer maximal tolerierbaren Ausfallzeit von etwa einer Stunde bzw. etwas mehr als 5 Minuten pro Jahr entspricht.

Ein wichtiger Aspekt, der bei der Standortwahl berücksichtigt werden muss, ist der Abstand zu möglichen Gefahrenquellen. Auf der einen Seite gibt es hier menschengemachte Anlagen, zu denen je nach möglichem Gefährdungspotenzial unterschiedliche Mindestabstände eingehalten werden müssen:

- **Kerntechnische Anlagen**: mindestens 40 km bei Anlagen, in denen es zu Ereignissen der Stufe 5 auf der internationalen Bewertungsskala für nukleare Ereignisse (INES) kommen kann. Zu kleineren Anlagen mit INES 2 bis 4 muss ein Abstand von 5 km eingehalten werden.
- **Chemische Produktion und Raffinerien**: 10 km
- **Gefährliche Stoffe** (Sondermüllverbrennungsanlagen, Lager von brennbaren, giftigen oder ätzenden Stoffen, Chemikalien, Feuerwerk, Munition, Explosivstoffe): 5 km
- **Andere gefährliche Stoffe** (Tankstellen, Propangashändler): 1 km
- **Verkehrswege** (öffentliche Straßen, die für Gefahrgut freigegeben sind, oberirdische Bahntrassen, Schifffahrtswege, An- und Abflugschneisen von Flughäfen): 1 km
- Zu **Bergbau, Sand- und Kiesgruben** muss ein Abstand eingehalten werden, der mindestens der zweifachen Grubentiefe entspricht, mindestens aber 200 m.

Für den dicht besiedelten Industriestandort Deutschland mit weit über 14.000 Tankstellen [2] und 13.000 km Autobahnen [3], auf denen auch Gefahrgut transportiert werden kann, ergeben sich deutliche Einschränkungen für mögliche RZ Standorte.

Daneben gibt es natürliche Gegebenheiten wie Erdbebengebiete [4], Windzonen [5] oder Gebiete, die von Hochwasser bedroht sind. Das führt zu weiteren Einschränkungen und baulichen Einschränkungen, die bei der RZ-Standortwahl eine Rolle spielen. Übrigens: Das ComConsult-Gebäude, aber auch die geplanten Hyperscaler-Standorte knapp 50 km nordöstlich von Aachen [6] befinden sich in der Erdbebenzone 2 (für Orte in Deutschland abfragbar auf der Website des Helmholtz-Zentrums für Geoforschung [7]). Hier müssen nach BSI-Vorgaben beim Bau eines RZ entsprechende bauliche Schutzmaßnahmen vor Erdbeben getroffen werden. Nur die Erdbebenzone 3 schließt die Ansiedlung eines hochverfügbaren RZ komplett aus, weswegen es z.B. in Tübingen kein im offenen Markt angebotenes Data Center gibt [8]. Darüber hinaus gibt es folgende Vorgaben:

Zwischen Vergangenheit und Gegenwart: Wie Apple die Gerätesicherheit stetig erhöht

von Mark Zimmermann

In den Anfangszeiten des iPhones konnten Nutzer durch sogenannte Jailbreaks tief ins Betriebssystem eindringen. Öffentlich bekannte Schwachstellen ermöglichten es, Systembeschränkungen zu umgehen, alternative Software zu installieren oder Systemprozesse zu manipulieren. Mit der Zeit hat Apple jedoch die Sicherheitsstandards konsequent erhöht: Der Bootloader wurde besser geschützt, Kernel-Exploits geschlossen, Verschlüsselungsmechanismen verbessert und Hardware-Sicherheitskomponenten wie die Secure Enclave eingeführt. Heute ist es deutlich schwieriger, auf geschützte Systembereiche zuzugreifen. Dauerhafte Jailbreaks sind selten geworden, und selbst spezialisierte Forensik-Tools stoßen zunehmend an ihre Grenzen.

Apple möchte seine Geräte so absichern, dass unautorisierte Zugriffe – sei es von Kriminellen, Ermittlern oder neugierigen Tüftlern – weitgehend ausgeschlossen sind. Mit iOS 18 führte Apple den Inactivity Reboot ein, der dieses Konzept weiter verstärkt. Nach 72 Stunden Inaktivität startet das Gerät automatisch neu, um alle temporären Daten wie Schlüssel, Session-Tokens oder im Arbeitsspeicher gehaltene Inhalte zu löschen. Wer ein iPhone nach längerer Untätigkeit vorfindet, trifft somit auf ein System, das sicherheitstechnisch in den Zustand unmittelbar nach dem Hochfahren zurückgekehrt ist.

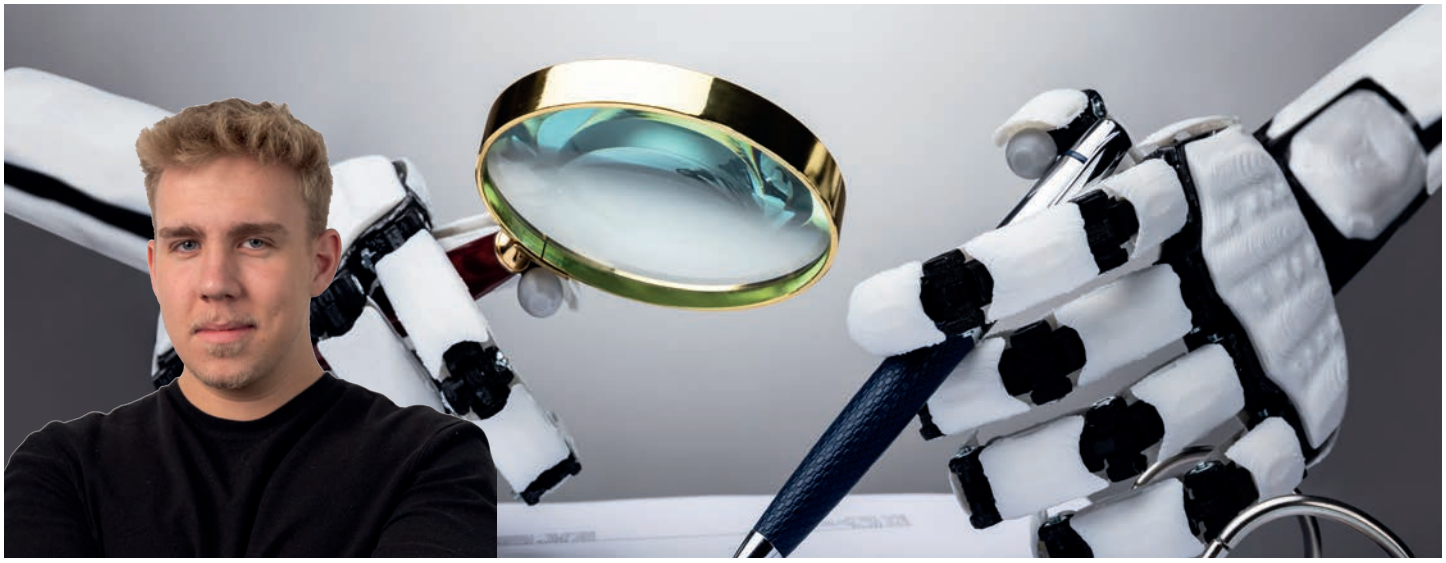
Wie Apple Sicherheit neu interpretiert

Früher konnten gesperrte, aber nicht neu gestartete Geräte für Forensiker oder Angreifer wertvolle Informationen liefern. Entschlüsselte Speicherbereiche, im RAM befindliche Schlüssel oder aktive Sessions ermöglichten tieferes Eindringen ins System. Der Inactivity Reboot unterbindet diese Möglichkeit: Wird das Gerät nicht genutzt, setzt der automatische Neustart einen Schlussstrich unter den vorherigen Betriebszustand. Erst nach erneuter Authentifizierung durch den Besitzer – meist durch Eingabe des Passcodes – werden verschlüsselte Daten wieder zugänglich. Biometrische Verfahren wie Face ID oder Touch ID stehen nach einem Neustart nicht zur Verfügung, um sicherzustellen, dass mindestens einmal bewusst der Passcode eingegeben wird (siehe Abbildung 1).

Verschlüsselung einfach erklärt

Auf einem iPhone sind Daten nicht einfach so gespeichert, sondern sie werden in verschiedene Sicherheitsstufen eingeteilt, je nachdem, wie sensibel sie sind und wann sie entschlüsselt werden dürfen. Man kann sich das vorstellen wie ein Safe mit mehreren Fächern, die unter unterschiedlichen Bedingungen geöffnet werden können.

Die höchste Schutzstufe sorgt dafür, dass Daten nur dann zugänglich sind, wenn das iPhone entsperrt ist. Sobald das Gerät gesperrt oder neu gestartet wird, werden diese Daten sofort wieder verschlüsselt und damit unlesbar. Zu diesen besonders sensiblen Daten gehören unter anderem private Schlüssel, Gesundheitsinformationen oder E-Mail-Anhänge. Eine Stufe darunter gibt es Daten, die nach einem Neustart erst wieder entschlüsselt werden, wenn der Nutzer das iPhone einmal entsperrt hat – hierzu zählen



Nutzung von KI im Arbeitsleben der Auszubildenden bei ComConsult

Mit Ben Grünbauer sprach Christiane Zweipfennig

In einer immer stärker digitalisierten Arbeitswelt sind Unternehmen zunehmend auf innovative Lösungen angewiesen, um ihre Prozesse effizienter zu gestalten. Eine dieser Lösungen ist der Einsatz von Open-Source-KI, die nicht nur die Arbeit im Hintergrund erleichtert, sondern auch die tägliche Arbeit von Teams direkt unterstützt. Besonders im IT-Support-Bereich, wo schnelle Problemlösungen und präzise Informationsverarbeitung gefragt sind, können solche Technologien einen erheblichen Mehrwert bieten.

Ben Grünbauer absolviert seit eineinhalb Jahren seine Ausbildung zum Fachinformatiker für Systemintegration bei ComConsult. Vorrangig arbeitet er im IT-Support, unterstützt jedoch auch zunehmend seine Kollegen in den verschiedenen Competence Centern bei der Projektarbeit. In diesem Interview spricht er darüber, wie Künstliche Intelligenz (KI) in seinem Arbeitsumfeld genutzt wird, welche Herausforderungen dabei auftreten und welche Vorteile die Technologie für den Arbeitsalltag bietet.

Wie hat der Einsatz von Künstlicher Intelligenz im Vergleich zu früher deine Arbeitsweise geändert?

In unserem Team sind wir aktuell insgesamt acht Personen: sechs Azubis und zwei Betreuer. Wir nutzen hauptsächlich ChatGPT und DeepL für Übersetzungen, Grammatiküberprüfungen und die Optimierung von Texten. Generell sparen wir durch die Nutzung von KI viel Zeit, besonders bei Aufgaben wie der Textüberarbeitung und dem Erstellen von längeren Texten. Ich lasse die Texte oft von der KI zusammenfassen oder nutze sie als Inspirationsquelle, um meine eigenen Texte zu verbessern. Dadurch kann ich effizienter arbeiten. Im Vergleich zu früher, als KI noch nicht so weit entwickelt war, kann ich heute viel mehr Aufgaben in kürzerer Zeit erledigen.

> Enorme Zeitersparnis durch den Einsatz von KI

Bei welchen Aufgaben ist der Einsatz von KI besonders hilfreich?

> KI für Übersetzungen und zur Textoptimierung

Ein gutes Beispiel sind Grammatiküberprüfungen. Wir nutzen DeepL, wenn wir mit englischsprachigen Kunden kommunizieren und stellen damit sicher, dass unsere Texte keine Rechtschreib- oder Grammatikfehler enthalten. Natürlich kommt die KI nicht zum Einsatz, wenn Projekt-, Kunden- oder ComConsult-interne Daten verwendet werden. In einem Projekt, in dem ComConsult die IT-Infrastruktur und Smart-Building-Komponenten eines historischen städtischen Gebäudes plant, tauschen wir uns momentan recht viel über die ge-

Und das nächste Datenleck: Business as usual?

von Dr. Markus Ermes

Und wieder gibt es ein neues Datenleck. Welches diesmal? Diese Frage allein zeigt schon das Problem: Datenlecks kommen mittlerweile so oft vor, dass man kaum noch mitbekommt, welche Firmen es schon „erwischt hat“.

Daher möchte ich in diesem Standpunkt auch nicht auf die Problematik der Datenlecks an sich eingehen, sondern ein wenig weiter ausholen. Es lassen sich nämlich drei zentrale Gemeinsamkeiten erkennen – einerseits zwischen verschiedenen Datenlecks, andererseits zwischen den Datenlecks und anderen erfolgreichen Angriffen:

- Die eigenen Daten sind zunehmend verstreut. Wo man früher mit wenigen Benutzeraccounts ausgekommen ist, benötigt mittlerweile jeder noch so kleine Dienst einen eigenen Account.
- Der oben genannte Gewöhnungseffekt und die Abstumpfung gegenüber Meldungen, die früher für Aufregung sorgten. Heute entlocken diese Meldungen den meisten interessierten Lesern nur noch ein resigniertes „Schon wieder?“
- Die Tatsache, dass die Schwachstellen, über die Daten abgegriffen werden, nicht lange bekannt oder auch nur vorhanden sein müssen. Manchmal reicht eine temporäre Schwachstelle, die nur wenige Tage ausnutzbar war.

Was hat es also mit diesen drei Aspekten auf sich?

Die vielen Benutzeraccounts

Ein Punkt, der einerseits zu Resignation führt, andererseits aber dafür sorgt, dass mittlerweile sehr viele Menschen von irgendeinem Datenleck betroffen sind, liegt in der Anzahl der Dienste, die man nutzt und für die man individuelle Accounts braucht.

Sei es das Social Network der Wahl, der Staubsaugroboter, das Smartphone, das Lieblings-Onlinespiel, ein Internet-Forum oder die Cloud des Spülmaschinenherstellers: Jede noch so geringe Interaktion mit einem smarten Device, einer Webseite oder irgendeinem sonstigen Dienst nötigt oder zwingt zum Erstellen eines Accounts, um den Komfort zu erhöhen. Was zunächst in vielen Fällen plausibel erscheint, kann auf den zweiten Blick durchaus stutzig machen. Ich persönlich kenne Online-Angebote, die noch vor kurzer Zeit viel Komfort auch ohne einen Account geboten haben, und die dann aktiv den Komfort für nicht angemeldete Nutzer reduziert haben, um mehr Nutzer dazu zu bringen, sich einen Account anzulegen. Hier sieht man dann relativ deutlich, dass der Dienst finanziell am meisten von den Daten der Nutzer profitiert.

Natürlich gibt es Dienste, bei denen eine Identifizierung des Nutzers elementar wichtig ist. Die oben genannten Social Networks und Online-Spiele sind hier ein gutes Beispiel. Wie sonst soll man wissen, mit wem man redet und was man in einem Spiel schon alles erreicht hat?

Mit der Idee der „Datensparsamkeit“ ist das jedoch in vielen Fällen nicht vereinbar. Warum muss ich einen Staubsaugroboter über die Cloud aus dem Urlaub fernsteuern können?!

Doch was kann man tun? Es gibt einige spannende Ansätze. Im