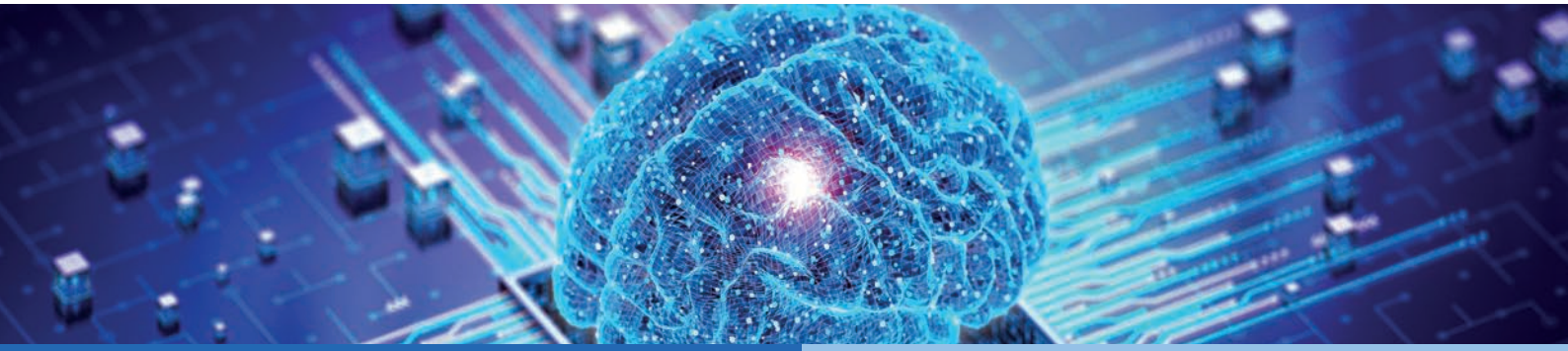
Februar 2026

ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider



Die hybride Zukunft der IT-Landschaft mit Quantencomputern

von Dr. Philipp Rüßmann
Quantencomputer bergen immenses Potenzial für neue Anwendungen und gefährden die heutige allgegenwärtige asymmetrische Verschlüsselung. Der Q-Day, an dem Quantencomputer unsere Verschlüsselung bedrohen, könnte bereits 2030 bevorstehen.

Seite 8

Das Management von Sicherheitsvorfällen

Ein Klassiker bekommt durch NIS-2 neue Brisanz

von Dr. Simon Hoff, Gaby van Laak, Dr. Kathrin Stollenwerk
Sicherheitsvorfälle, die eine Organisation unvorbereitet treffen, richten in der Regel bedeutenden Schaden an. Abhilfe schafft ein zuverlässiges Management von Sicherheitsvorfällen.

Seite 23

Netztrends 2026

von Dr. Behrooz Moayeri
Es ist über zwei Jahre her, seit ich an dieser Stelle die wichtigsten Netztrends zusammengefasst habe. Zwei Jahre sind in der IT-Entwicklung lang. Es wird Zeit, dass ich, gestützt auf Erkenntnisse aus ComConsult-Projekten, die wichtigsten aktuellen Netztrends zusammenfasse.

Seite 2

IT Service Desk auf Erfolgskurs: klug strukturiert, umsichtig gesteuert

von Petra Kallisch
Der IT Service Desk ist die zentrale Schnittstelle zwischen Anwendern und IT – und damit maßgeblich für die Wahrnehmung der gesamten IT Organisation. Klar strukturiert und professionell gesteuert, erreicht er eine hohe Servicequalität, sorgt für schnelle Störungsbehebung und trägt nachhaltig zur Zufriedenheit der Kunden bei.

Seite 15

Webinar der Woche

Netztrends 2026

Seite 22

Der Deutschland-Stack:

der nächste Schritt auf dem Weg zur digitalen Souveränität?

von Dr. Philipp Rüßmann
Die Aufregung um Grönland und die damit verbundenen Zollandrohungen gegen Dänemark und weitere Unterstützer haben es wieder einmal gezeigt: Eine zu starke Abhängigkeit von den USA macht angreifbar, wenn nicht sogar erpressbar.

Seite 29

Netztrends 2026

von Dr. Behrooz Moayeri

Es ist über zwei Jahre her, seit ich an dieser Stelle die wichtigsten Netztrends zusammengefasst habe. Zwei Jahre sind in der IT-Entwicklung lang. Es wird Zeit, dass ich, gestützt auf Erkenntnisse aus ComConsult-Projekten, die wichtigsten aktuellen Netztrends zusammenfasse.

RZ als Besonderheit

Das LAN im Rechenzentrum (RZ) unterliegt eigenen Trends. Nicht zuletzt aufgrund der zunehmenden Sicherheitsvorfälle ist die von Firewalls bewachte Trennung zwischen Rechenzentren und der Außenwelt zum Standardfall geworden. Je stärker diese Trennung wird, desto geringer ist der Grad der Integration des Netzes im RZ in die Infrastrukturen außerhalb des Rechenzentrums, weshalb man die Netze für die beiden Bereiche (RZ und die Außenwelt) gesondert behandeln muss.

Trotz des anhaltenden Cloud-Trends kenne ich kaum ein Unternehmens-RZ, das in den letzten zwei Jahren wesentlich weniger virtuelle Maschinen beherbergt hat als vor 2024. In vielen Rechenzentren sind die Server mit einer Virtualisierungsplattform das Herzstück. Die Bitraten der Server-LAN-Adapter steigen mit jeder neuen Server-Generation. Die Server werden mit zwei- bis dreistelligen Gigabit-Raten an das LAN angebunden. Zwischen den RZ-Switches werden 100G-Leitungen und bald auch leistungsfähigere Links genutzt. Storage, sofern ein dediziertes Speichersystem und nicht Storage in den Servern genutzt wird, nutzt ähnliche Anbindungen wie die Server.

Die physische RZ-Netzstruktur sieht überall ähnlich aus. Die logische LAN-Segmentierung im RZ unterscheidet sich jedoch von Umgebung zu Umgebung.

Zero Trust als bestimmender Trend

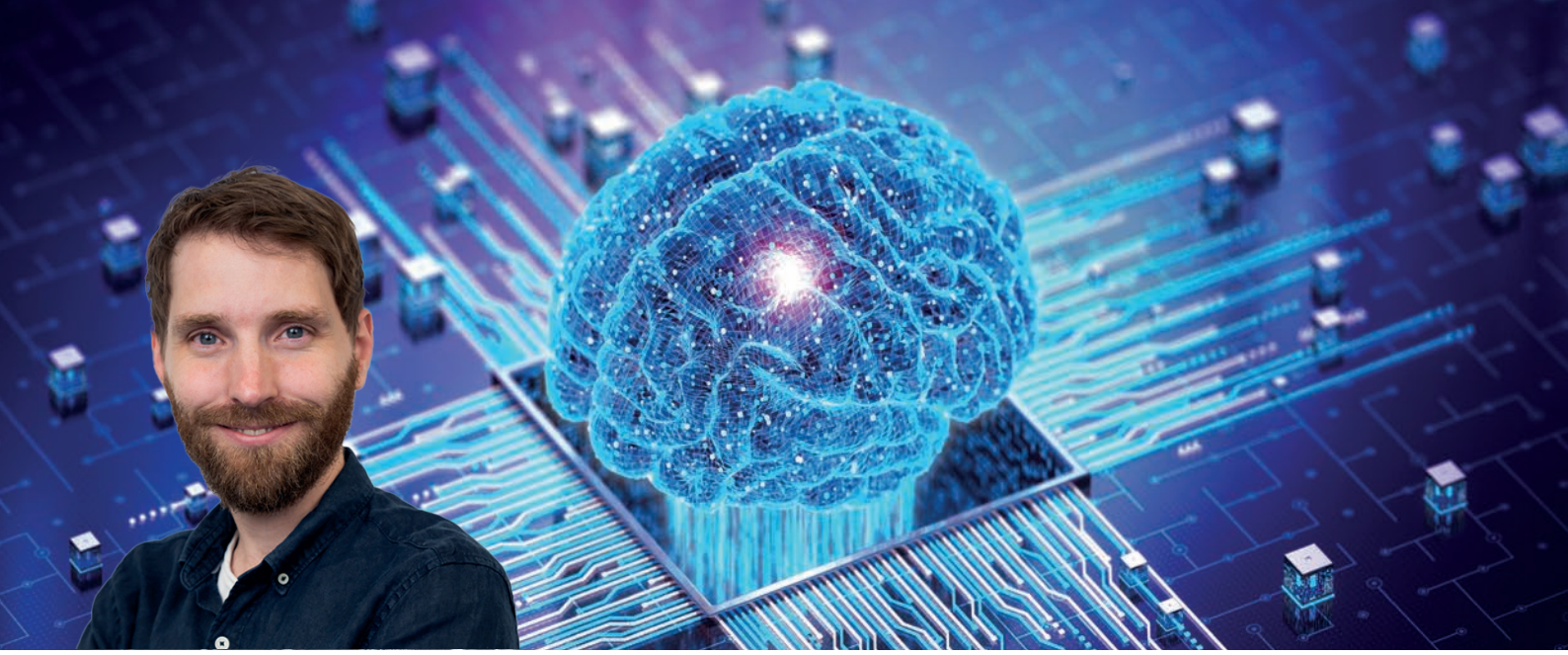
In den letzten Jahren bin ich an dieser Stelle wiederholt auf Zero Trust als den bestimmenden Trend bei der Gestaltung von IT-Infrastrukturen eingegangen. Viele RZ-Betreiber leiten von der Orientierung an Zero Trust (nie vertrauen, immer verifizieren) die Mikrosegmentierung ab. Die Idee dabei: die Verteidigungslinie immer weiter in Richtung der zu schützenden Ressource rücken. Am Ende dieser Entwicklung haben wir es dann mit Ressourcen zu tun, die der Außenwelt überhaupt nicht mehr vertrauen und jede Kommunikationsbeziehung verifizieren. Ein solches System verhält sich so, als ob es an das unsicherste aller Netze, das Internet, angeschlossen wäre.

Wir kommen somit von völlig offenen Netzen und werden künftig wieder alle Netze als unsicher behandeln. Der Ausgangspunkt und das Ziel der Entwicklung der Netze sind identisch.

Die Reise geht jedoch über Zwischenstationen. Kaum ein Unternehmen legt den Hebel einfach auf die letzte Stufe der von Zero Trust bestimmten Entwicklung um. In der Praxis sieht es so aus, dass ein RZ-Betreiber, häufig getrieben von Audits und Compliance, als unverzichtbaren Schritt zunächst das RZ-Netz von der Außenwelt trennen und die Kommunikation dazwischen über Firewalls leiten muss. Danach macht man sich, wiederum vorgegeben durch übergeordnete Richtlinien, an die Makrosegmentierung, d.h. die Bildung von Zonen im RZ. Und ab hier unterscheiden sich die Entwicklungen in den verschiedenen Rechenzentren.

Verschiedene Verfahren der Netzsegmentierung im RZ

Das logische Design des RZ-Netzes muss sich an dem Verfahren orientieren, das bei der Netzsegmentierung im RZ angewandt wird. Geht man den Weg, die zunehmende Anzahl der RZ-LAN-Segmente über dedizierte Firewalls zu koppeln, braucht man keine komplexen Sicherheitsmechanismen auf den RZ-Switches. Diese müssen nur die virtuelle Segmentie-



Die hybride Zukunft der IT-Landschaft mit Quantencomputern

von Dr. Philipp Rüßmann

Quantencomputer bergen immenses Potenzial für neue Anwendungen und gefährden die heutige allgegenwärtige asymmetrische Verschlüsselung. Der Q-Day, an dem Quantencomputer unsere Verschlüsselung bedrohen, könnte bereits 2030 bevorstehen [1]. Doch wie werden sich Quantencomputer in unsere IT-Landschaft integrieren? Welche Anforderungen bringen sie mit sich und wie kann man sie heute schon nutzen?

Chancen durch Quantencomputer

„Quantencomputing wird die IT-Welt grundlegend verändern“ hat meine Kollegin Lea Joosten Anfang 2024 in ihrem Blog-Artikel prognostiziert [2]. Der Auslöser für diese Aussage war das beachtliche Medienecho um die Vorstellung des Google-Willow-Quantenprozessors kurz zuvor. Seitdem hat sich auf dem Feld der Quantentechnologien noch mehr getan, was auch immer wieder zu Berichten in der Fachpresse führt. Einen Einblick in die Entwicklungen haben wir auf den Treffen der IBM Quantum Community bekommen [5].

Das vergangene Jahr stand insgesamt ganz im Zeichen der Quantenphysik. Anlässlich des 100-jährigen Bestehens der Formulierung der Quantentheorie war 2025 durch die UNESCO zum internationalen Jahr der Quantenwissenschaft und Quantentechnologien ausgerufen worden [3]. Zwar besitzt Quantencomputing noch nicht die Marktreife für die breite Produktion; allerdings haben Quantencomputer durchaus das Potenzial, nach dem aktuellen KI-Hype das nächste große Ding zu werden. Nach den aktuellen Rekordinvestitionen in KI-Infrastruktur [4], könnte durch Quantencomputing die nächste große Investitionswelle in die RZ-Infrastruktur der Zukunft heranrollen.

Das Geheimnis von Quantencomputern liegt dabei in ihrer grundlegend unterschiedlichen Bauweise gegenüber herkömmlichen Computern – und den damit verbundenen neuen Möglichkeiten für Berechnungen. Statt klassischer Bits, die die Zustände 0 und 1 annehmen können, verwenden Quantencomputer Quantenbits (auch Qubits genannt, siehe Infobox). Qubits können mehr als herkömmliche Bits. Sie können alle Überlagerungen von 0 und 1 gleichzeitig annehmen. Dadurch verfügen Quantenalgorithmen über eine eingebaute Parallelität. Diese Komplexität des Rechenraums lässt sich für gewisse Probleme nutzen, darunter solche, die für klassische Computer praktisch unlösbar sind. Und darin liegt das große Interesse an Quantencomputern.

Quantencomputer versprechen revolutionäre Durchbrüche in der Informationstechnologie. Sie eignen sich insbesondere dazu, die Lösung folgender Problemklassen gegenüber klassischen (Super-)Computern deutlich zu beschleunigen:

- **Intrinsisch quantenmechanische Probleme**: Beispielsweise können Quantencomputer für Simulationen in den Materialwissenschaften wie der Erforschung von Katalysatoren, Energiespeichern, Düngern oder neuer Medikamente eingesetzt werden. Bei diesen Problemen spielen quantenmechanische

IT Service Desk auf Erfolgskurs: klug strukturiert, umsichtig gesteuert

von Petra Kallisch

Der IT Service Desk ist die zentrale Schnittstelle zwischen Anwendern und IT – und damit maßgeblich für die Wahrnehmung der gesamten IT Organisation. Klar strukturiert und professionell gesteuert, erreicht er eine hohe Servicequalität, sorgt für schnelle Störungsbehebung und trägt nachhaltig zur Zufriedenheit der Kunden bei. Dieser Artikel zeigt praxisnahe Maßnahmen, mit denen Verantwortliche ihren Service Desk ausrichten, operativ stabilisieren und messbar optimieren können.

Bedeutung des IT Service Desk im Unternehmen

Der IT Service Desk ist weit mehr als eine Supporteinheit: Er ist Aushängeschild, Qualitätsindikator und zentraler Anlaufpunkt der IT.

Ein effizient arbeitender Service Desk sorgt dafür, dass:

- Anwender schnell Unterstützung erhalten,
- Störungen professionell erfasst und priorisiert werden,
- Tickets korrekte Weiterleitung und möglichst rasche Lösung erfahren und
- das Business störungsarm und produktiv arbeiten kann.

In der Praxis stehen Service-Desk-Teams jedoch häufig unter Druck: hohe Ticketvolumina, spontane Zusatzaufgaben, Projektlast und Major Incidents erschweren eine stabile Leistungserbringung. Umso wichtiger sind klare Strukturen, definierte Prozesse und eine konsequente Steuerung.

Erfolgsfaktor: Klares Zielbild

Ein häufiges Problem: Es existiert kein klares Zielbild für den IT Service Desk und den IT-Support. Ohne definierte Erwartungen bleibt unklar, worauf das Team hinarbeiten soll. Dabei spielt es eine große Rolle, welcher Weg eingeschlagen wird.

Typische Zielvarianten sind beispielsweise:

- Qualitätsfokus: perfekte Ticketbearbeitung, auch bei längerer Bearbeitungszeit
- Effizienzfokus: hoher Durchsatz, auch wenn die Tiefe der Bearbeitung variiert
- Balanced Approach: Orientierung an KPIs, Service Levels und Rahmenbedingungen

Empfehlung: Um das passende Zielbild für die Ausrichtung des Service Desk und IT-Supports zu zeichnen, sollte im Management ein einheitliches Verständnis hergestellt werden. Hierbei ist natürlich die IT-Strategie und der zentrale Business Need zu berücksichtigen. Das Zielbild darf der gesamten IT-Organisation erläutert werden, denn auch die nächstliegenden Supporteinheiten tragen wesentlich zum Erfolg der IT-Supportorganisation inklusive Service Desk bei.

Das Management von Sicherheitsvorfällen – ein Klassiker bekommt durch NIS-2 neue Brisanz

von Dr. Simon Hoff, Gaby van Laak, Dr. Kathrin Stollenwerk

Sicherheitsvorfälle, die eine Organisation unvorbereitet treffen, richten in der Regel bedeutenden Schaden an. Um diese Vorfälle effektiv zu erkennen, auf sie reagieren und sie bewältigen zu können und auch um potenzielle Schäden möglichst gering zu halten, bedarf es eines zuverlässigen Managements von Sicherheitsvorfällen, auch als Sicherheitsvorfallmanagement (SVM) oder im Englischen als Security Incident Management bezeichnet. Hier werden Prozesse definiert und Organisationsstrukturen gebildet, um Sicherheitsvorfälle frühzeitig zu erkennen und zu behandeln. So werden ihre Auswirkungen minimiert und die Widerstandsfähigkeit des Unternehmens gegen diese Vorfälle gestärkt.

Mit der Behandlung und speziell dem Management von Sicherheitsvorfällen sollten sich alle Organisationen befassen, denn jede IT-Infrastruktur kann von einem Sicherheitsvorfall betroffen sein. Betreibt eine Organisation jedoch ein Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001 oder nach BSI-IT-Grundschutz, besitzt das Management von Sicherheitsvorfällen automatisch eine besondere Bedeutung. Ist eine Organisation eine wichtige oder besonders wichtige Einrichtung oder gar Betreiber einer kritischen Infrastruktur im Sinne des BSI-Gesetzes vom Dezember 2025 [1], nimmt das Management von Sicherheitsvorfällen eine noch exponiertere Rolle ein.

Spätestens jetzt ist es an der Zeit, sich mit dem Thema Management von Sicherheitsvorfällen in der eigenen Organisation auseinanderzusetzen. Als Denkanstoß kann der vorliegende Artikel dienen: Er beschreibt alle wesentlichen Aspekte des Sicherheitsvorfallmanagements, erläutert Prozess-Strukturen und betrachtet Schnittstellen zwischen Prozessen. Regulative Grundlagen werden diskutiert und Werkzeuge und Methoden für das SVM vorgestellt.

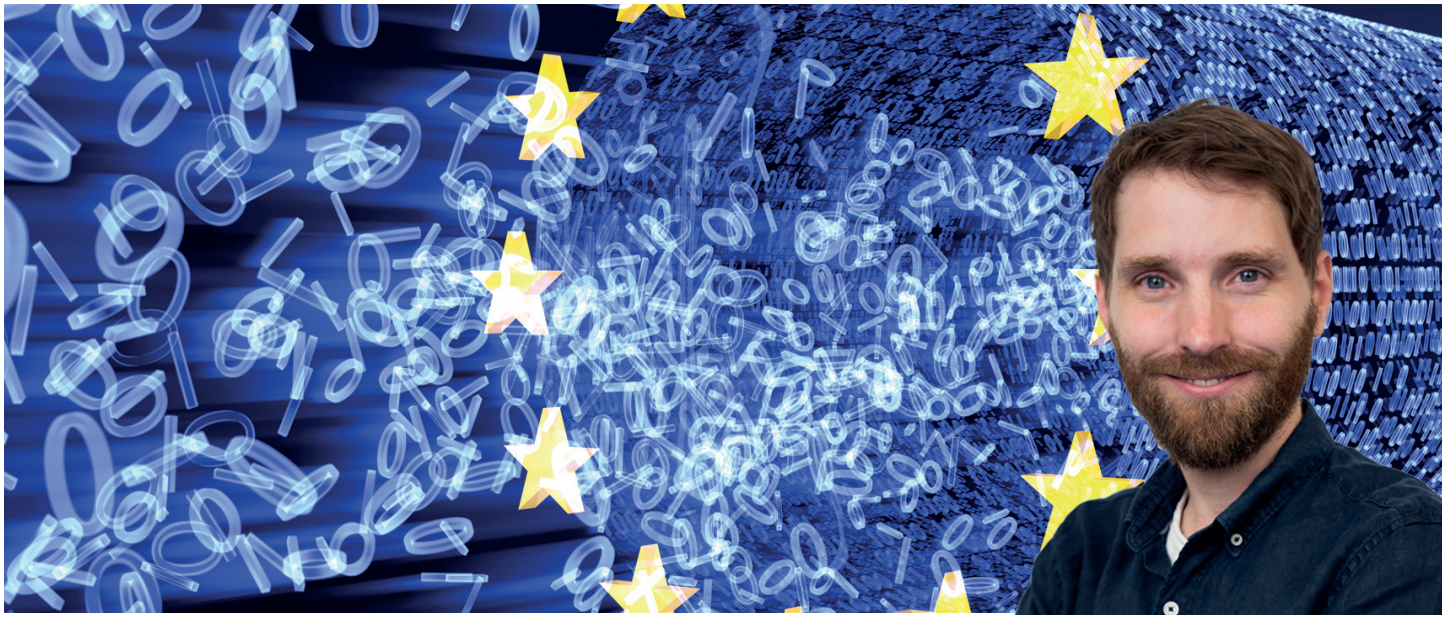
Auswirkungen von NIS-2 auf das SVM

Mit dem Anfang Dezember 2025 in Kraft getretenen BSI-Gesetz (BSIG, [1]) erfolgt die Umsetzung der NIS-2-Richtlinie der EU [2] in deutsches Recht. Durch dieses Gesetz bekommt ein angemessenes Management von Sicherheitsvorfällen eine herausgehobene Bedeutung, denn es verpflichtet wichtige und besonders wichtige Einrichtungen sowie Betreiber kritischer Infrastrukturen dazu, angemessene Maßnahmen zur Bewältigung von Sicherheitsvorfällen zu ergreifen, und verlangt zudem eine Meldung von erheblichen Sicherheitsvorfällen.

Als erheblich gilt im Sinne des §2 Nr.11 BSIG ein Sicherheitsvorfall, der

Der Deutschland-Stack: der nächste Schritt auf dem Weg zur digitalen Souveränität?

von Dr. Philipp Rüßmann



Die Aufregung um Grönland und die damit verbundenen Zollandrohungen gegen Dänemark und weitere Unterstützer haben es wieder einmal gezeigt: Eine zu starke Abhängigkeit von den USA macht angreifbar, wenn nicht sogar erpressbar. Dabei ist die Abhängigkeit in der IT besonders stark ausgeprägt. Da ist es höchste Zeit, das Thema digitale Souveränität wieder hoch auf die Agenda zu setzen. Dies gilt insbesondere für den öffentlichen Sektor.

Digitale Souveränität im öffentlichen Sektor

Auch die öffentliche Verwaltung hat erkannt, dass das Thema der digitalen Souveränität wichtiger und drängender ist denn je. Doch damit Worten auch Taten folgen können, braucht es Entschlossenheit und vor allem Investments. Eine Abkehr von Microsoft und Co. bedeutet Know-how-Aufbau und anschließend die Migration des Technologie-Stacks und der damit verbundenen digitalisierten Prozesse. Nicht zuletzt ist ein gutes Change Management essenziell, um die zahlreichen User in den öffentlichen Verwaltungen und auch deren Kunden auf dem Weg nicht zu verprellen und erfolgreich mitzunehmen.

Die viel beachtete Umstellung auf mehr Open-Source-Software in Schleswig-Holstein hat gezeigt, dass dieser Prozess gelingen kann [1]. Zwar gab es auch dort Startschwierigkeiten, doch ist die Praxistauglichkeit von Open-Source-Software inzwischen anerkannt [2].

Was ist der Deutschland-Stack?

Auf Bundesebene ist der Deutschland-Stack eine vom Bundesministerium für Digitales und Staatsmodernisierung ins Leben gerufene Technologie-Plattform für die öffentliche Verwaltung in Deutschland [3]. Für die großen Digitalvorhaben des Landes soll der Deutschland-Stack einen einheitlichen strategischen Rahmen vorgeben und eine souveräne nationale Plattform bieten. Bis 2028 sollen damit iterativ konkrete Angebote für Bund, Länder und Kommunen entstehen – für solch ein großes Vorhaben ein durchaus ambitionierter Zeitplan.

Nach dem etwas holprigen Start des Deutschland-Stacks im Herbst 2025, mit berechtigter Kritik am Erstentwurf aus der ersten Konsultationsrunde, wurde nun die nächste Version mit einigen Schärfungen im Gesamtkonzept veröffentlicht [4]. Neu an Bord sind jetzt mit KI-Agenten ein ganz aktuelles Hype-Thema und dazu ein stärkerer Fokus auf Open-Source-Entwicklungen [5]. Künstliche Intelligenz soll dabei als „Enabler“ für Automatisierung dienen.

Das Thema digitale Souveränität wird in der Strategie des Deutschland-Stacks besonders hervorgehoben: Lösungen